GeoJournal (2013) 78:287–301
DOI 10.1007/s10708-011-9411-0

A typological framework for categorizing infrastructure vulnerability

Tony H. Grubesic · Timothy C. Matisziw

Published online: 3 May 2011

Abstract The concept of vulnerability is increasingly important in engineering and the socio-economic planning sciences, particularly given the enormous costs associated with addressing it. The ability to identify and mitigate vulnerabilities is extremely challenging because it is influenced by a complex and dynamic set of interacting factors that can compromise social, economic and infrastructure systems. Where the latter is concerned, the ability to assess infrastructure vulnerability involves the consideration of a range of physical, operational, geographical and socio-economic characteristics. In this paper, significant elements of infrastructure vulnerability are identified and discussed with a focus on their intrinsic spatial nature and their propensity to interact across space. Further, the developed typology of vulnerability outlined in this paper emphasizes the need to ensure that policy, planning and disaster mitigation efforts are strongly integrated at global, regional and local levels.

Keywords Critical infrastructure · Networks · Interdependency · Interdiction · Disaster mitigation · Spatial analysis · Public policy

Introduction

In the United States, there is a growing interest in both social vulnerability (Cutter and Finch 2008; Borden et al. 2007) and the vulnerability of infrastructure systems, both of which are intimately related (NRC 2006; White House 2003). Moreover, during the past two decades, both the executive and legislative branches of the U.S. government have made concerted efforts at better defining what systems and assets are most important to the day-to-day functioning of the nation, giving rise to what is now termed *critical infrastructure* (Sec. 1016[e]). Critical infrastructure and assets include transportation systems, telecommunication networks, the electrical grid, banking networks, reservoirs, natural gas distribution systems, and many other interdependent infrastructures, vital to the day-to-day functioning of social, economic and physical systems in the United States (Lewis 2006; Murray and Grubesic 2007). Although, the importance of such infrastructure is obvious, how to most appropriately describe sources of vulnerability is not, particularly given the sheer

T. H. Grubesic (✉)
College of Information Science and Technology, Drexel University, Philadelphia, PA 19104, USA
e-mail: grubesic@drexel.edu

T. C. Matisziw
Department of Geography, University of Missouri, Columbia, MO 65211, USA

T. C. Matisziw
Department of Civil and Environmental Engineering, University of Missouri, Columbia, MO 65211, USA

variety of critical assets and systems. Compounding matters is the range and level of services that infrastructure systems provide, their interdependencies, and potential threats, all of which can vary significantly across time and space.

The purpose of this paper is to develop a typological framework for categorizing infrastructure vulnerability. While complimentary to the work on social vulnerability, which focuses on the sensitivity of populations to hazards and their ability to respond to/recover from the impacts of an extreme event (Cutter 2006), the analysis of infrastructure vulnerability is primarily concerned with the physical, operational, and geographic characteristics of infrastructure elements, their fragility to threats, their role in the system(s) with which they interact, as well as the potential implications of disruptive events. While many factors influence vulnerability, this paper primarily focuses on their spatial facets, which are often the most difficult features to characterize. It is also important to note that the development of a typology concerning the spatial facets of critical infrastructure vulnerability, is largely absent in the existing literature. While multiple facets of infrastructure vulnerability are certainly addressed in other work (ASCE 2005; Pederson et al. 2006; Murray and Grubesic 2007), the failure to provide an overarching framework for categorizing these facets is a major oversight. Given the geographic emphasis of the taxonomy developed in this paper, it is hoped that this will serve as a useful multiscalar (i.e. global, regional and local) framework for developing more effective and holistic policy, planning and disaster mitigation efforts.

In the next section, a brief review of the vocabulary, terms and literature that examines the spatial and temporal context of infrastructure vulnerability is provided. This is followed by the introduction of a typological framework for categorizing infrastructure vulnerability. This paper is concluded with a brief discussion and provide a roadmap for future research.

Vulnerability vocabulary

The concept of vulnerability is multifaceted (Adger 2006). By definition, vulnerability means susceptibility to injury or attack (MW 2008a). However, there are a number of pre-conditions that are required for an entity to be vulnerable. In this context, the concept of risk is an important one. Kaplan and Garrick (1981) summarize risk as a simple function of three factors: (1) what can go wrong; (2) what is the probability of it going wrong; (3) what are the consequences if it does go wrong. For example consider the impacts of a hurricane making landfall in a populated area. The loss of human life, economic disruption and the environmental/physical damage caused by high winds, rain, storm surge and flooding are certainly negative outcomes. However, when efforts are made to mitigate risk, levels of exposure may not change, but the degree to which an area, population or system is vulnerable can be altered. For instance, by developing and implementing a comprehensive hurricane evacuation plan, one does not decrease the probability that a hurricane will hit communities along a coastal region, but it can reduce the *vulnerability* of populations within the region. There are also elements of uncertainty associated with vulnerability. In many situations it is difficult to ascertain the specific threats or events which may generate negative outcomes for a population or infrastructure system (Sage and White 1980). Again, knowledge (or lack thereof) of these threats does not decrease exposure (Holton 2004), but a systematic understanding of, and planning for potential threats can help reduce vulnerability.

Although the fundamental concept of vulnerability is related to the susceptibility of people, places and infrastructure to disruptive events, there are elements of uncertainty associated with how, when and where these events will occur. For example, although the timing of earthquakes has proven exceedingly difficult to predict, the scientific community has developed a relatively good understanding of which areas are vulnerable to major seismic events (USGS 2008).

It is also important to acknowledge that vulnerability comprises elements of sensitivity and response. For instance, some infrastructure systems are more resilient (i.e. able to recover or respond quickly) to disruptions than others. Portions of this resilience can often be attributed to careful planning (e.g. organized evacuations, availability of shelter, water, food and medical supplies) and through good infrastructure design (e.g. retrofitted buildings, redundant and diverse supply and distribution systems, etc.). From a social perspective, Cutter and Finch (2008: 2301) note that response is also a multidimensional construct and is not easily captured within a single variable. As a result, elements of race, age, socioeconomic class, gender and housing tenure impact the ability of social groups to respond and recover from extreme events. A similar argument can be made for the economic impacts of infrastructure failure (Richardson et al. 2006), where many dimensions need to be considered.

Regardless of the type of vulnerability in question (e.g. social, economic or infrastructural) both the timing and location of disruptive events can influence their overall impact. For example, while the loss of electricity for several days or even a week would have minimal impact on rural villages in developing countries where the power grid is thin, that same loss would have catastrophic impacts to New York City, where electrical power is crucial for the day-to-day operations of transportation systems, telecommunication networks, water distribution pumps, computers, etc. In fact, this is exactly what happened in August 2003, when a series of infrastructure-related failures generated a massive blackout in the Northeastern U.S. and portions of Canada (Minkel 2008). In this scenario, while the type of failure is identical (i.e. loss of electricity), the vulnerability of these two locations is dramatically different.

Perhaps the most significant concern relating to the vulnerability of social or infrastructural systems is potential for *failure*. Specifically, where infrastructure is concerned, the concept of failure does not necessarily imply uniform levels of service disruption within a system. In many cases, critical infrastructures have back-up facilities or services that ensure operational continuity. For example, most hospitals maintain some type of back-up electrical system if the main power grid fails. However, vulnerabilities do increase the risk of failures because systematic weaknesses increase the likelihood of system disruptions when exposed to extreme events. Not surprisingly, disruptions can lead to different types of failures given the dependencies among system components as well as interdependencies between systems (Rinaldi et al. 2001; McDaniels et al. 2007).

The spatial and temporal aspects of vulnerability

Given the complex interplay of vulnerability and failure, it is also important to note that the demand for certain services (e.g. broadband, electricity, rail service, etc.) are spatially and temporally heterogeneous. As a result, the impacts of infrastructure failures and associated losses can vary dramatically.

Spatial

As noted previously, the spatial vulnerability of infrastructure systems is multifaceted. In a highly generalized context, the locations where infrastructure is placed, along with the relative locations of failures within or between systems, is extremely important when evaluating spatial vulnerability. For example, Grubesic et al. (2008) illustrate that depending on the spatial configuration of telecommunication nodes in network, a variety of scenarios of infrastructure damage exist, each having a differential impact on infrastructure performance—both in terms of magnitude and geographic scale. Further, the disruptive potential of each scenario can be measured in numerous ways, such as the impact to system capacity, cost, connectivity, demand/provision, and redundancy. As a result, decline in system connectivity may not be particularly problematic if connectivity among vital supply and demand nodes is still available, but the delays or re-routing costs associated with delivering a good or service may be crippling.

Again, this hints to the mutuality of infrastructure, social vulnerability and failure. For example, as noted by Cutter and Finch (2008), locations increasing in social vulnerability between 1960 and 2000 often did so because of extreme population growth and lack of corresponding infrastructure support. In this case, the authors cite Orange County, California as a location that was determined to be moderately vulnerable in 1960, but due to a nearly 300% growth in population (among other things) is now considered one of the most socially vulnerable location in the United States. Population growth generates greater demands for all resources and services. In areas where system capacities and use are near maximum levels, vulnerability increases and any type of disruption or failure can intensify the social or systemic impacts.

Temporal

In addition to the spatial implications of infrastructure vulnerability and failure, systems and their use are rarely static—requiring the acknowledgement of temporal dimensions of vulnerability. Similar to the overly generalized statement for spatial vulnerability provided previously, the "when" of potential infrastructure disruptions is equally as important as the "where". For example, if we revisit the impacts of electrical disruptions, the temporal variations associated with outages can be quite pronounced. Because the use of electricity often spikes both during the winter (heating) and summer months (cooling) in temperate, mid-latitude climates (Willis 2002), the loss of electricity during these periods may be more problematic than during milder spring and autumn months when climate related health problems (e.g. heat stroke or hypothermia) may be less of a concern. Switching sectors for a moment, temporal variations can also be examined at a much smaller scale. Consider the loss of telecommunications services to a residential household at 3 a.m. versus 7 p.m. The impacts of the 3 a.m. loss are likely less problematic than the same loss at 7 p.m., when the demand and use of broadband services is highest. It is also important to note that larger temporal windows (e.g. decadal or multi-decadal) also impact vulnerability of populations and infrastructure. The duration of a disruption is also relevant. As evident from the 9/11 attacks, although backup systems (e.g. emergency power supply) can provide a short-term bridge for operational continuity, they are not viable long-term substitutes (Grubesic and Murray 2006), frequently failing prior to initialization or simply running out of alternative energy supplies (i.e. diesel).

Regardless of how one conceptualizes vulnerability in time and space, infrastructures maintain a range complex relationships (amongst and between each other) and characteristics that contribute to their vulnerability. As a result, efforts directed at maintaining the operational continuity of critical infrastructure systems must be driven by a broader understanding of vulnerability. In the next section, a typological framework for categorizing infrastructure vulnerability is proposed to address these issues.

A typology of infrastructure vulnerability

Every 2–3 years, the American Society for Civil Engineers (ASCE) releases a report card that summarizes U.S. infrastructure on the basis of condition, performance, capacity and funding. The results of the most recent (2009) evaluation are sobering. Aviation, dams, drinking water, energy, hazardous waste, inland waterways, levees, roads, schools, transit, and wastewater all received grades of D+, D or D− (ASCE 2009). Essentially, a "D" quality level in the ASCE report means that the infrastructures are not functioning in a safe and reliable manner, teetering on collapse. The question is, why? More importantly, how do these conditions contribute to infrastructure vulnerability?

As discussed in the previous sections, vulnerability manifests in a variety of ways. Both spatial and temporal aspects of the level of demand for a service are of obvious importance.

However, other dimensions of vulnerability do exist for critical infrastructures. In this section, we will introduce these additional considerations and propose a typological framework for better understanding their contributions to vulnerability. Figure 1 presents a depiction of our typological framework and displays eight distinct facets of infrastructure vulnerability, including *condition, capacity and use, obsolescence, location and topology, interdependencies, disruptive threats, policy and political environment, and safeguards*. While this is not an exhaustive list, largely ignoring issues related to economic and social vulnerability, we believe it captures the bulk of those factors underlying the geographic aspects of infrastructure systems. Individually, each of these

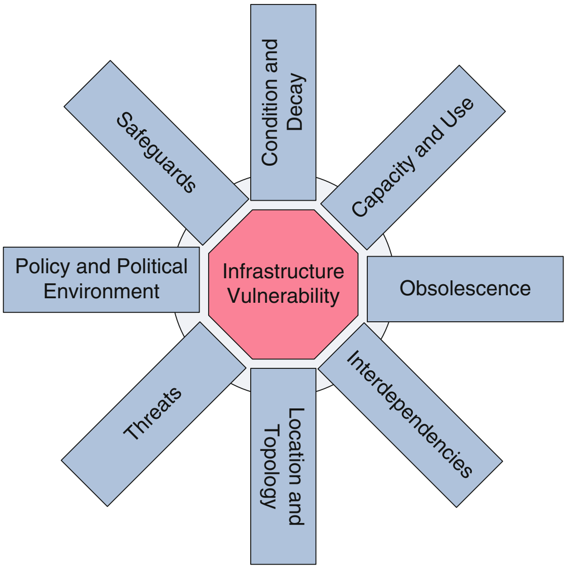

Fig. 1 Eight facets of critical infrastructure vulnerability

eight aspects has the potential to contribute to infrastructure disruptions. It is important to note, however, that most infrastructure systems are simultaneously influenced by a multiple facets, any of which can contribute to systemic disruption. Moreover, while we have endeavored to ensure that each category is relatively exclusive, some overlap is unavoidable.

Condition and decay

By definition, decay refers to a decline from a sound or prosperous condition or, destruction by decomposition (MW 2008b). The sources of infrastructure decay vary widely, but dams provide a particularly interesting case-study for considering this process. Decay, through erosion, corrosion, weathering or other atmospheric and geologic forces strongly contribute to both decomposition and dam failure. Further, many problems in the condition and structural integrity of dams can be attributed to the movement and/or failure of the foundation supporting the dam and inadequate maintenance and upkeep (FEMA 2008). According to the 2009 ASCE report, there are 15,237 high hazard dams in the United States, an increase of nearly 3,300 since 2007.[1] Interestingly, there were 67 dam incidents were reported between 2003 and 2005. While this figure may seem relatively low, particularly considering that there are over 80,000 dams in the U.S., these incidents only hint to the breadth of the problem. For instance, current estimates suggest more than 3,500 dams have deficiencies severe enough to leave them susceptible to failure. Further, it is estimated that $36 billion will be needed over the next decade to rehabilitate and repair the most critical structures (Reid 2008).

Decaying infrastructure also impacts other critical assets, particularly bridges. As recounted by Lichtenstein (1993), one of the worst bridge disasters in U.S. history occurred because of a corroded eyebar suspension system on the Silver Bridge, which linked Point Pleasant, West Virginia and Gallipolis, Ohio. The bridge collapse killed 46 people and motivated the establishment of the National Bridge Inspection Program, which requires that every bridge longer than twenty feet be inspected every 2 years (Reid 2008). In this context, because decay compromises the structural integrity of critical infrastructure and assets, decay contributes to the vulnerability of these systems. It is also important to note that the "trigger" for condition-related failures need not be an extreme event as they can also occur under normal use.

Finally, condition and decay can also impact federal, state and local highway and road systems in more mundane ways. Environmental conditions combined with car and truck traffic eventually degrade the quality and condition of both concrete and asphalt road systems. Decay, in the form of potholes or worn surfaces increases both accident frequency and municipal liability (Tighe et al. 2000). Furthermore, maintenance needed to mitigate the effects of decay and maintain suitable infrastructure condition can require significant expenditures, detracting resources from other areas of need.

Capacity and use

As alluded to in the previous sections, the availability of infrastructure is a major concern in many regions. For example, estimates suggest that the world's infrastructure stock is valued at approximately $15 trillion, but only 13% of this stock is located in low income countries (Fay and Yepes 2003). The problem is particularly acute in Africa, where populations in many of the least developed countries, such as Niger and Chad, lack access to electricity, telephones and other relatively standard physical infrastructure systems (Borgatti 2005). In other cases, access to infrastructure may not be a problem, but the availability of infrastructure that can handle all of the demand placed upon it, can be.

The definition of capacity is the maximum amount or number that can be contained or accommodated (MW 2008c). For infrastructure systems, this might represent bandwidth availability on a fiber-optic backbone, or the volume of car and truck activity a highway can accommodate. Increasingly, infrastructure systems in the United States and abroad lack the capacity to meet user demand. For example, consider

[1] According to the ASCE (2009), A dam's "hazard potential" is classified on the basis of the anticipated consequences of failure, not the condition of the dam. The classifications include "high hazard potential" (anticipated loss of life in the case of failure), "significant hazard potential" (anticipated damage to buildings and important infrastructure), and "low hazard potential" (anticipated loss of the dam or damage to the floodplain, but no expected loss of life).

the commercial air traffic system in the United States. In a recent report by the Federal Aviation Administration (2007), estimates suggest that 18 airports and seven metropolitan areas will need additional runway and/or service capacity by 2015 to keep air traffic flowing smoothly and to meet projected consumer demand. However, simply meeting the growing physical infrastructure needs for this sector and the needed improvements will require $41.2 billion in investment (FAA 2007). With passenger counts projected to exceed 1 billion by 2015, ensuring that sufficient capacity exists in this system is critical. According to the ASCE (2005), failure to allocate "significant infrastructure investment", aviation delays are expected to cost the U.S. economy $170 billion between 2000 and 2012.

In this type of operating environment, capacity induced vulnerability manifests in different ways. For instance, if we revisit the capacity constraints associated with airports, many major U.S. hubs lack the capacity to handle traffic during peak periods. According to Forrey (2007), president of the National Air Traffic Controllers Association, while 57 flights were scheduled to depart from Newark Liberty International Airport between 9:00 and 10:00 a.m. on September 5, 2007, only 45 flights could be accommodated. Two days later, a similar situation occurred in Chicago at O'Hare International. The lack of capacity makes airports vulnerable because significant ground control delays prohibits the efficient functioning of both airlines and creates delays for passengers. In other infrastructure systems, a lack of capacity has similar impacts. For example, when disrupted systems are unable to reroute traffic due to a lack of capacity, the ability for a system to recover and readjust after a disruption is compromised. In telecommunications systems, the phenomenon of congestion collapse is particularly troublesome (Nagle 1984; Albuquerque et al. 2004). For instance, with the loss of high bandwidth lines, lower bandwidth connections are forced to carry the data packets. If the remaining lower bandwidth lines are overloaded with transmission requests, latency increases in the system and congestion collapse becomes a possibility (Johari and Tan 2001; Albuquerque et al. (2004).[2]

Infrastructure obsolescence

Although there is no universally accepted definition of infrastructure obsolescence, any element of a system that suffers from poor design, is based on outdated engineering or design components, can no longer meet current safety standards or lacks the ability to handle new applications, can be considered obsolete. That said, it is important to note the differences between obsolescence and infrastructure condition/decay. Specifically, while obsolete infrastructure can be in poor condition or a decayed state, this is not always the case. Simply put, brand new components can be obsolete, particularly if they do not meet current application standards.[3] Obviously, things get more complex when engineered systems and critical infrastructure are examined for both obsolescence and condition. As noted by the ASCE (2009), while many infrastructure *systems* are in extremely poor condition, it is extremely difficult to say if one or more *parts* are obsolete. Analysis at this minute scale is time consuming, costly and requires a significant investment of human resources.

Unfortunately, it is all too frequent that one of the *parts* of an infrastructure system is linked to a catastrophic system malfunction. For example, one of the most high-profile infrastructure failures in the last 25 years was the collapse of the Interstate 35 W Bridge in Minneapolis, Minnesota in August 2007. Killing 13 people and injuring nearly 100 more, the National Transportation and Safety Board (NTSB 2008) investigation revealed several problems associated with bridge design and its structural conditions. Post-collapse analysis indicates that the bridge was constructed with gusset plates that were too thin for connecting steel beams in the truss bridge. In fact, the gusset plates were about 50% too thin for this particular application, resulting in sixteen plates

[2] Congestion collapse occurs when an overloaded network has settled into a stable state, where traffic demand is high, but

Footnote 2 continued
little throughput is available in the system. As a result, high levels of latency, packet delay and loss emerges (Johari and Tan 2001).

[3] A good analogy here is the eight-track audio cartridge. While it is possible to design, produce and use a brand new eight-track cartridge today, the technology is obsolete and the sound quality, relative to digital audio technologies (e.g. compact disc) is poor.

being fractured prior to the collapse (NTSB 2008). In addition, because the bridge was designed and fabricated in the 1960s, it included antiquated, "fracture critical" design components—where the failure of a fracture critical member (FCM) is expected to result in the collapse of the bridge (TRB 2005).

One of the major problems with FCM bridges is the lack of redundancy for the structure and substructures. In this context, redundancy is defined as "the quality of a bridge that enables it to perform its design function in the damaged state" (AASHTO LRFD 2004). In a recent report regarding the inspection and maintenance of FCM bridges, the Transportation Research Board (2005) notes that during the late 1970s, materials, design and the fabrication of steel bridge components improved dramatically, resulting in fewer instances of fatigue and fracture. However, while these adjustments improved bridges erected after the new standards were implemented, 76% of the bridges with FCMs in the United States were fabricated before 1978. In fact, national statistics reveal that approximately 11% of all steel bridges in the U.S. have FCMs (TRB 2005).

Obviously, there are other examples of obsolescent infrastructure and related failures, such as the steam pipe explosion in New York City during July 2007 (Barron 2007) and problems with water storage tanks and low-pressure water distribution lines in Pittsburgh, Pennsylvania (PIIA, 2007). Many of these older pipeline infrastructures still use cast iron components. Therefore, in addition to rust and decay (i.e. condition), cast iron systems are far last resistant to geological events such as earthquakes—particularly when compared to newer steel or polymer structures.

Clearly, in all of the examples illustrated above, infrastructure longevity, system age, design and the diminished ability of these infrastructures to cope with increased demands make them highly vulnerable. As noted by Marland and Weinberg (1988), infrastructure systems do have limited life-spans, even if the exact duration of their functionality is difficult to precisely predict. Simply put, devices and structures wear out, operation and maintenance can become too expensive and competing systems and technologies become available—offering improved functionality at less cost.

Interdependencies

A fourth aspect to vulnerability is the degree to which an infrastructure system is reliant or dependent upon another infrastructure system for operation. While this seems to be a relatively simple concept, it is important to note that there is a difference between *dependency* and *interdependency*. Rinaldi et al. (2001, 14) define dependency as, "a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of another". This suggests a unidirectional relationship between systems, where one relies on the other for functionality. Conversely, they define interdependency as "a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other". In this instance, the infrastructures are co-dependent on each other for operation. Pederson et al. (2006) formalize infrastructure interdependency as a network as follows:

1. An infrastructure network, I, is a set of nodes related to each other by a common function. The network can be connected or disjoint. It may be directional, bi-directional or have elements of both. Internal relationships/dependencies within I are represented by edge (a, b) with $a, b \in I$.
2. Given I_i and I_j are infrastructure networks, $i \neq j$, $a \in I_i$ and $b \in I_j$, an interdependency is defined as a relationship between infrastructures and represented as the edge (a, b) which implies that node b is dependent upon node a. The nature of this relationship may also be reflexive in that $(a, b) \rightarrow (b, a)$.

Taxonomies for interdependencies have also been developed. For example, Rinaldi et al. (2001) differentiate between four basic types of interdependencies. The first, *physical*, is the reliance on material flow from one infrastructure to another. *Cyber* interdependencies are largely related to computer control systems or a reliance on computerized information transfer between infrastructure systems. If changes in the local spatial environment can affect components across multiple infrastructure systems due to physical proximity, a degree of *geographic* interdependence is in place. Finally, *logical* interdependencies reflect linkages in human decision making, are bidirectional and do not necessarily depend on any physical, spatial or cyber connection. While space limitations prevent us from detailing all of the nuances associated with infrastructure interdependencies, particularly those detailing infrastructure as complex adaptive systems (Axelrod and Cohen 1999), additional details can be found in the review provided by Rinaldi et al. (2001). In sum, there are numerous examples in recent years that highlight why infrastructure interdependencies exacerbate vulnerabilities. Obviously, the example discussed earlier regarding the August 2003 blackout provides an excellent case study in how interdependent infrastructures fail after an initial shock to a single system (i.e. electrical). For more details, see Grubesic and Murray (2006), Minkel (2008) or USCPSOTF (2004).

When one begins examining the interdependencies between more than two or three systems, the resulting matrix of interactions becomes extremely complex. Complicating matters is the notion of *coupling* between systems. Tightly coupled systems have no slack or buffer in their operational requirements. They are time dependent, goods services and information are continually moving, sequences in the process are invariant, and reactions to changes to the system are almost instantaneous (Perrow 1999). Conversely, *loosely coupled* systems are more tolerant of processing delays, sequencing can be changed, alternative methods may be available or used if necessary, and reactions to changes to the system are not immediate. For more details, see Perrow (1999).

Location and topology

As noted in the introductory section, the geographic location of critical infrastructure systems or their components plays an important role in understanding system vulnerability. Regardless of location, all systems maintain some degree of exposure to risk. Again, while there is uncertainty associated with the specifics of where, when and why disruptions may occur, the geographic locations of the majority of critical infrastructure systems do contribute to their vulnerability.

It is important to note that because critical infrastructure varies in form and function, as does the demand for services provided by these systems, their locational attributes are also varied. For example, while telecommunications backbones are the lifeblood of many information intensive businesses throughout the United States (Mack and Grubesic 2009), the geographic footprint of most backbone systems includes extremely large continental transects through the most sparsely populated regions in the United States (Fig. 2). The same can be said for most large networked infrastructures in the U.S., including gas pipelines (Fig. 3). This makes the geographic location of network components and their ambient environment important factors when evaluating the vulnerability of infrastructure systems. Consider, for instance, the differential in time and effort associated with transporting equipment and crews for repairing supervisory control and data acquisition (SCADA) devices or other network elements to geographically remote or inaccessible locations versus more central, urbanized locales. For example, Gothenburg, Nebraska is located along Interstate 80, a major corridor for fiber optic backbones in the United States. Gothenburg is also located at least 250 miles away from any major city (e.g. Denver or Omaha) and most likely lacks the resources, equipment and technical expertise to mount an effective local response to heavy fiber backbone damage. Conversely, support crews and equipment located in Chicago could respond to a major disruption on a fiber backbone (or any infrastructure-related problem) in the city within minutes.

Similarly, some areas of the United States are more prone to natural disasters, such as wildfires, floods, hurricanes, tornadoes, etc. As a result, the ambient local environment often influences the overall vulnerability of infrastructure systems, particularly if they are exposed to extreme events. Consider, for example, the geographic distribution of interstate gas pipelines displayed in Fig. 3. Extremely high densities of pipelines exist along the Gulf Coast region (e.g. Louisiana) and portions of Oklahoma. Both locales, incidentally, are subject to extreme weather, with hurricanes along the Gulf of Mexico and coastal Louisiana and tornadoes in Oklahoma.[4]

Another aspect to consider is the spatial scale associated with geographic vulnerability. As noted

[4] While a significant portion of pipeline infrastructure is subterranean, a tornado recently hit a natural gas pumping station in Tennessee (AP 2008), generating a massive fire.

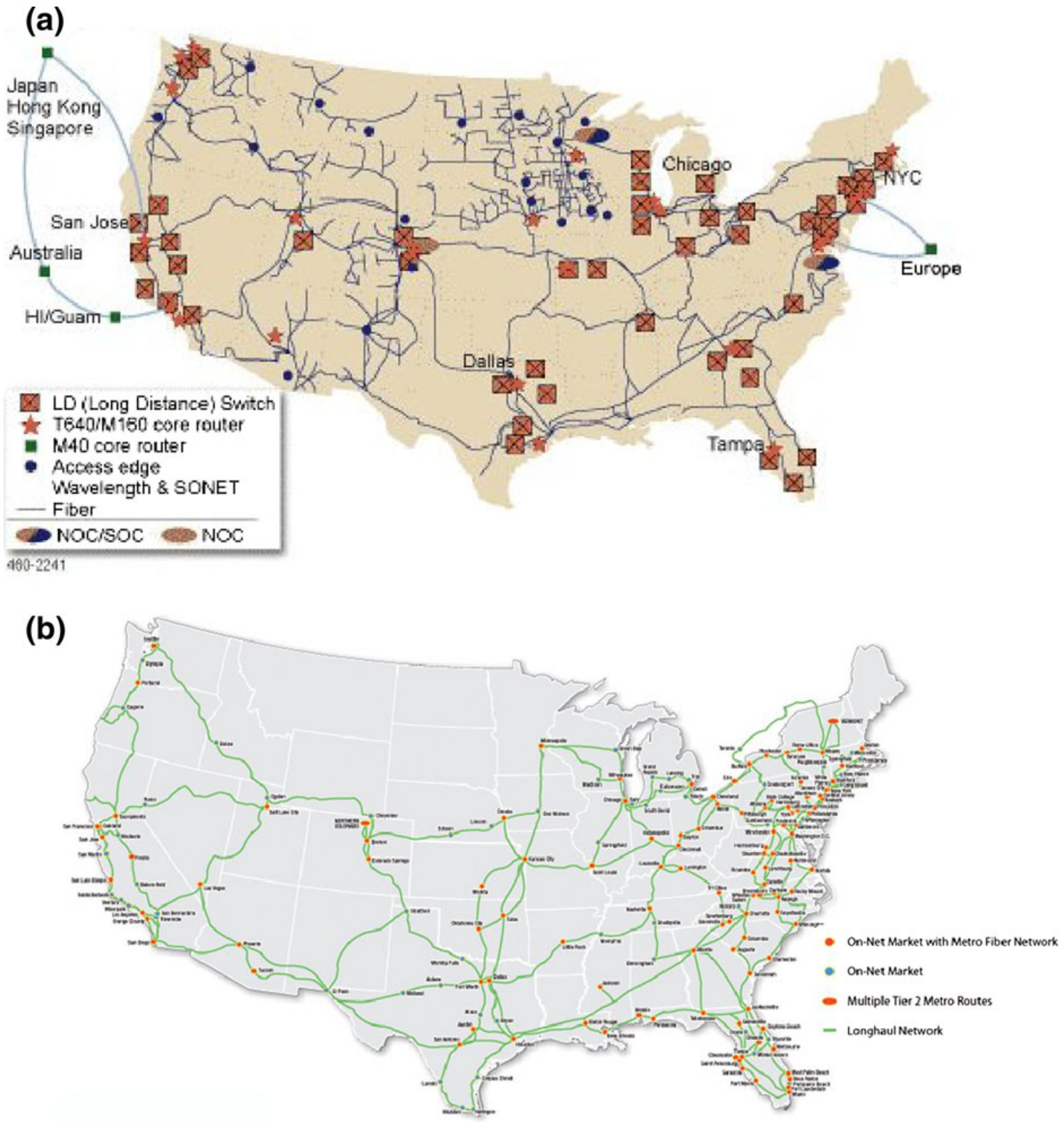

Fig. 2 **a** Qwest nationwide converged backbone. **b** Protocall nationwide backbone

previously, the form and function of infrastructures in the United States vary tremendously. While some critical systems have geographic footprints spanning multiple continents, others are limited to regions, cities or even a single building. As a result, when considering vulnerability, geographic scale matters. Finally, the topological structure of critical infrastructure systems is an important consideration. Typically, the most efficient networks, such as those using a directed link, star, bus or hub-and-spoke topology are the most vulnerable to disruption. In many instances, the loss of a single switching node or link in these systems creates a disconnection in the network. For more details on the relationship between system topology and vulnerability, see Murray and Grubesic (2007).

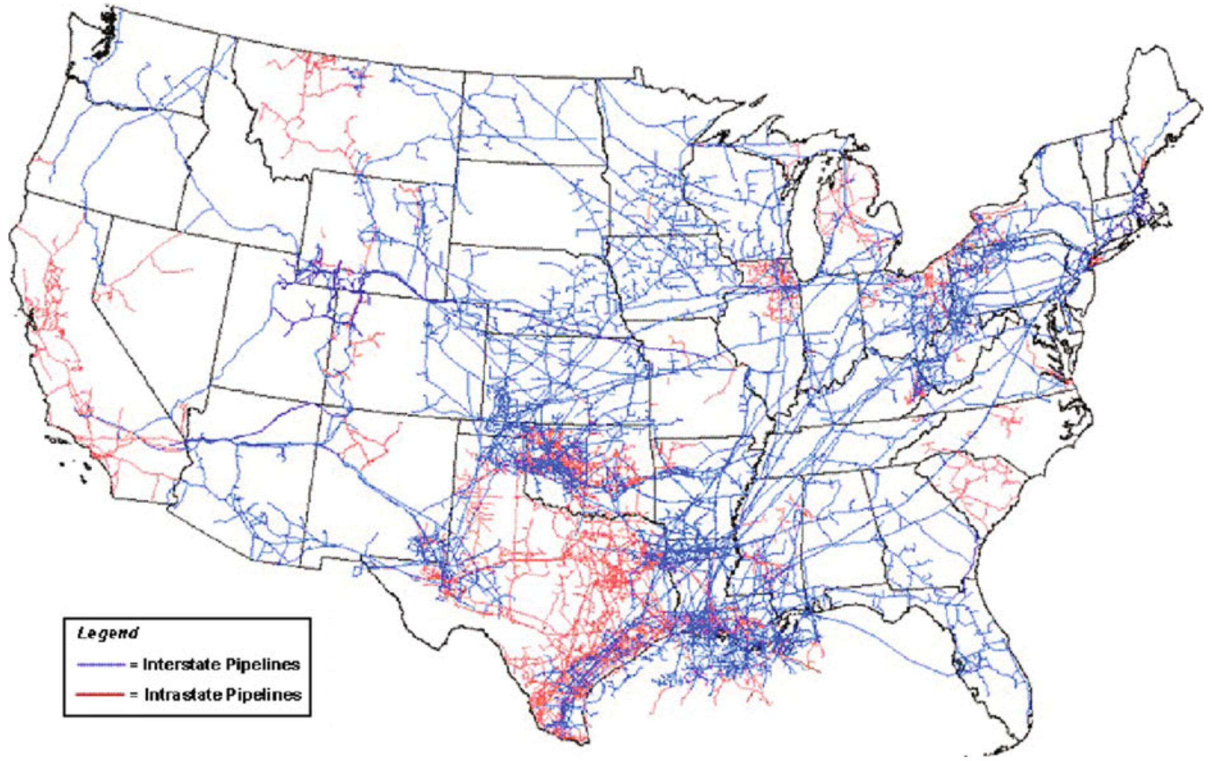

Fig. 3 United States natural gas pipelines. *Source* Energy Information Administration, Office of Oil and Gas, Natural Gas Division

Disruptive threats

The set of potential threats to critical infrastructure is highly diverse, ranging from natural and technological disasters to sabotage. Consider, for example, the overall spatial distribution of natural disasters in the United States. Schmidtlein et al. (2008) highlight clusters of environmental threats in the upper Great Plains (tornadoes and flooding), the Gulf Coast (hurricanes and tropical storms) and southern California (wildfires and earthquakes). This is not to say that other regions are devoid of threats, but between 1965 and 2004 natural disasters were most frequent in the previously identified areas (Schmidtlein et al. 2008).

The now classic example of a major natural disaster, Hurricane Katrina, exemplifies how environmental threats and the interplay of water, wind and storm surge wreaked havoc on critical infrastructure systems at local and regional levels. For example, in the report *A Failure of Initiative* issued by the U.S. House of Representatives in 2006, a brief inventory of damage to the information and communications infrastructure is provided. In addition to the loss of three million telephone lines in the region (Louisiana, Mississippi and Alabama), thirty eight 911 call centers, 2,000 cellular towers, and many of the most important fiber-optic backbones were lost to flooding and/or wind damage (U.S. House 2006). Ironically, even the small subset of systems that managed to maintain functionality had problems. In most instances, these communication lines were overwhelmed by the heavy traffic emanating from the response effort (U.S. House 2006). Combine these telecommunication losses with the damage done to transportation infrastructure, levees, the electrical system, hospitals and most governmental buildings in New Orleans, the severity of this natural disaster at the local and regional level is apparent.

While Katrina was an extreme event that garnered national attention, there are also many smaller-scale environmental and technological threats that occur on a weekly, monthly or yearly basis in the United States that do not generate significant, long-term attention although they can be similarly damaging to specific infrastructure sectors. Winter storm related losses in the Northeastern U.S. exceeded $45 million between 1971 and 2007 Changnon (2008). Similarly, technological threats, such as the Baltimore Freight Rail Crash of 2001 which generated a chemical fire that burned for nearly a week, ruptured a water main that caused streets to flood, disrupted East Coast rail service and slowed the Internet are also extremely disruptive to a wide variety of sectors (NTSB 2004).

While natural and technological disasters are unintended, Sabotage and terrorist attacks are acts of subversion with the direct intent to inflict physical and emotional damage to people, property and critical infrastructure. Although the terrorist attacks of September 11, 2001 provide the most horrific example of such events, there are many others. For example, during the initial stages of the U.S. war in Iraq, acts of sabotage crippled critical infrastructure systems throughout the country. Glanz (2004) notes that over 100 electrical backbone lines were cut between 2003 and 2004, with 1,200 transmission towers toppled. Even after President Bush declared the end of major hostilities in Iraq (April 2003), over 200 oil pipeline attacks occurred (April 2003 through December 2004), primarily along the 600-mile, 40-inch Kirkuk-Ceyhan pipeline (Luft 2005).

Interestingly, sabotage is not always committed by outside threats such as terrorists or guerilla armies. In many instances, acts of sabotage are committed by "insiders". As noted by Keeney (2005), these are typically individuals who were authorized to use infrastructure or its associated support systems (e.g. SCADA) that eventually leveraged this access to perpetrate a destructive act. Results of this detailed study also reveal that 59% of the saboteurs were former employees or contractors while 41% were currently engaged with the victimized company. The vast majority of the insiders were employed in technical positions and 96% were male. In addition to citing odd pre-attack behavior around the office by the saboteurs, it was determined that the majority of perpetrated attacks were accomplished using company computer equipment (Keeney 2005).

Policy and political environment

From a political and policy perspective, vulnerability is somewhat more difficult to define than many of the other facets of previously discussed. For example, Sarewitz et al. (2003) explore six different "assertions" associated with both vulnerability and risk in the context of policy, ranging from the need for acquiring accurate probabilistic information about extreme events to understanding that such events are context driven. Consider, for example, the impacts of political and economic rows between countries (or corporations) on the operational continuity of critical infrastructure systems. In 2008, Gazprom, headquartered in Russia and one of the largest oil and natural gas companies in the world claimed that Ukrainian held gas company, Naftogaz Ukrainy, owed it more than $2 billion in missed payments and fines. Naftogaz Urkainy countered that they had paid the bill and that Gazprom was trying to force a new price for gas which it could not afford. In a response to this disagreement, Gazprom completely shut down its supply pipelines to the Ukraine (Kramer 2009). While this may appear to be a relatively isolated geographic incident, it is important to note that Austria, Turkey, the Czech Republic, Germany and Greece were impacted by the shutdown, forcing these nations to seek alternate supply sources for nearly a week. As a result of this crisis, the Nabucco Pipeline project was developed, seeking to route alternative supplies of natural gas to Europe via Turkey (Lyons 2010)—lessening Europe's dependence on Russian supplies and its politically vulnerable distribution system.

In a similar vein, geopolitical context also impacts homeland security policy in the United States. With the recent failures of command and control infrastructures in the U.S. due to extreme events such as the September 11th attacks and Hurricane Katrina, homeland security policy and vulnerability planning is slowly moving to a more regionalized structure. For example, Caruson and MacManus (2007) argue that strongly integrated regional systems help overcome the multiplicity of state agencies and local governments during disasters, facilitating stronger vertical (e.g. federal-state-local) and horizontal (local–local) networks. In essence, these stronger and better-integrated networks allow state and local governments to "harness the collective benefits of shared resources and information: (Caruson and MacManus 2007, 1)".

Safeguards

A final influence on infrastructure vulnerability is the presence and effectiveness of safeguards. In general, safeguards refer to any actions that are taken to detect/identify and plan for potential threats to infrastructure operation. Such efforts include asset tracking, identification of vulnerabilities, development of disaster response/restoration plans, surveillance of infrastructure, protection, and infrastructure hardening (Church and Scaparra 2007; Murray et al. 2007; Matisziw et al. 2008, 2010) . In this context, better implementation of safeguards is assumed to result in enhanced proactive and reactive targeting, response, and reduction of vulnerabilities. For example, given the application of various network analysis methodologies, worst-case scenarios of network damage (and associated components) can be identified. Based on these insights, vulnerable network components can then be more effectively targeted for protection, thereby reducing/eliminating worst-case vulnerabilities (Matisziw et al. 2008).

Given that resources for applying infrastructure safeguards are limited, it is essential to obtain an accurate characterization of exactly how the application of safeguards may result in vulnerability reduction. Of course, the ability to accomplish this is reliant on how well other elements of the vulnerability matrix are understood. For instance, developing a protection plan for one infrastructure might require addressing interdependencies and hardening components of another.

Discussion and conclusion

Given the preceding narrative on the different facets of vulnerability, it is possible to more concretely define a matrix of vulnerability for individual infrastructure systems. Specifically, the vulnerabilities of a particular infrastructure, V_i, can be thought of as a function of a complex and diverse set of features, roughly corresponding to the outlined facets. Consider the following notation, where each variable represents a range of potential vulnerabilities:

δ	condition and decay
χ	capacity and use
α	obsolescence
ι	interdependencies
λ	location and topology
ν	disruptive threats
π	policy and political environment
ς	safeguards

When evaluating the vulnerabilities of different critical infrastructure systems, one can more simply represent these complexities as a function, using various combinations of the outlined facets. Further, if feasible, one can also assign either positive (+) or negative (−) factors to each facet. In many instances, the positive and negative factors for each facet are mutable. For example, newer systems that are in good condition and exhibit no decay would receive a positive factor for δ. Conversely, if elements of the system are decayed or in poor condition, δ might receive a negative factor. Consider, for instance, the vulnerability of telecommunications infrastructure (V_i^T), which is a function of capacity and use, obsolescence, interdependencies, location and topology, disruptive threats and safeguards. More simply, $V_i^T = f(\chi^+, \alpha^-, \iota^-, \lambda^+, \nu^-, \varsigma^+)$. In this instance, negative factors are assigned to obsolescence, interdependencies and disruptive threats. However, if there are no safeguards in place, network capacities are running at a maximum level and the network displays a sparse typology, it is possible to assign negative factors to χ, λ and ς. The reverse, for obsolescence, interdependencies and disruptive threats may also be true. Given the facets of vulnerability outlined above, the exact contribution of each of these variables to characterizations of vulnerability will be context dependent, varying between infrastructure types and locations.

Table 1 provides a snapshot of how the different facets of this typology may interact or display some level of simultaneity. It is important to note that this matrix does not represent a definitive categorization of interactions between facets. Instead, it represents a very broad, context-dependent, view of how they might interact simultaneously across systems. What holds true for telecommunications systems may not be applicable to the national air transportation system. That said, it is clear that these facets are not mutually exclusive. For example, as noted previously, although condition and obsolescence are unique, both facets have the potential to interact within a single system (e.g. the I-35W bridge).

Finally, given this paper's focus on the geographic nature of infrastructure vulnerability, it is important to highlight some potential geographic strategies to reduce infrastructure vulnerability. While it is clear that infrastructure systems must be designed to meet

Table 1 Vulnerability matrix

	Condition	Capacity and use	Obsolescence	Location and typology	Interdependencies	Disruptive threats	Policy and political environment	Safeguards
Condition	–	▲	▲					
Capacity and use	▲	–	▲	▲	▲		▲	▲
Obsolescence	▲	▲	–					
Location and typology		▲		–	▲	▲	▲	▲
Interdependencies		▲		▲	–		▲	▲
Disruptive threats				▲	▲	–	▲	▲
Policy and political environment				▲	▲	▲	–	
Safeguards		▲		▲	▲	▲		–

▲ Facets are interrelated or display some level of simultaneity

user demand, this can be a difficult task when simultaneously attempting to reduce vulnerabilities. Users must be able to access the system somewhere, even if this access increases systematic exposure to risk. Not surprisingly, the need to serve infrastructure demand often results in relatively “problematic” clusters or agglomerations of critical infrastructure in certain locations (Parfomak 2005). For example, considering that over 45% of U.S. securities are traded in the American Stock Exchange and New York Stock Exchange in lower Manhattan, A targeted strike to this area, much like the events of September 11th, 2001, could yield massive disruptions to the global marketplace. The question is, how can such vulnerabilities be mitigated?

Again, while there is no single ‘best’ strategy, a variety of approaches have been recommended. For example, during the Cold War era, the Long Lines Division of AT&T was particularly concerned with the vulnerability of critical telecommunications infrastructure in both the military and civilian sectors to nuclear attack. In an effort to mitigate the vulnerability of these systems, AT&T recommended a series of geographic strategies, including network diversification, separation, avoidance and hardening to minimize the impacts of a nuclear detonation on their telecommunication equipment. For more details on these strategies, see Grubesic and Murray (2005).

Obviously, these types of strategies are not always possible; particularly if there are geographic constraints (e.g. immobility) associated with critical infrastructure systems (e.g. oil refining capacity clustered along the Gulf Coast). However, there are operational strategies for critical infrastructure systems with more locational flexibility such as critical stockpiles of emergency supplies (Church and Scaparra 2007). These can be moved, albeit with some effort, to both minimize vulnerability and maximize accessibility.

In sum, regardless of the functional representation of vulnerability, or the selection of strategies for vulnerability mitigation, it is clear that the acquisition, analysis and synthesis of data from a wide variety of sources is needed to determine the specific nature of vulnerability for infrastructure systems. More importantly, understanding both *where* and *when* systems may be vulnerable to disruption is important for developing disaster mitigation plans and policies structured to minimize systemic weaknesses. Further, as outlined by Murray et al. (2008), the ability to utilize multiple methods for better identification and understanding vulnerability is essential—ranging from strategy-specific, simulation-based and mathematical modeling assessments.

In conclusion, while the presented typological framework for categorizing infrastructure vulnerability is both complex and multifaceted, significant work is still required to capture the many nuances of vulnerability through space and time and across and between systems. As suggested by Sarewitz et al. (2003), extreme events are created by context—and context is highly dynamic. So, while it may be nearly impossible to concretely identify every conceivable vulnerability within an infrastructure system, this does not absolve policy makers and analysts of their responsibility to explore the complex mesh of potential vulnerabilities, nor their charge in formulating mitigation strategies and associated public policies for minimizing the impacts of extreme events to critical systems and society. As the discussion in this paper highlights, these are not easy tasks, but they are clearly essential ones.

References

Adger, N. (2006). Vulnerability. *Global Environmental Change, 16*(3), 268–281.

Albuquerque, C., Vickers, B. J., & Suda, T. S. (2004). Network border patrol: Preventing congestion collapse and promoting fairness in the Internet. *IEEE/ACM Transactions on Networking, 12*(1), 173–186.

American Association of State and Highway Transportation Officials (AASHTO) (2004). LRFD-US-3. Bridge design specifications.

American Society for Civil Engineers (ASCE) (2005). Report card for America's infrastructure. URL: http://www.asce.org/reportcard/2005/index.cfm.

American Society for Civil Engineers (ASCE) (2009). Report card for America's Infrastructure. URL: http://www.infrastructurereportcard.org/sites/default/files/RC2009_full_report.pdf.

Associated Press (AP) (2008). Firefighters contain massive gas fire in Tenn. URL: http://www.msnbc.msn.com/id/23023302/.

Axelrod, R., & Cohen, M. D. (1999). *Harnessing complexity: Organization implications of a scientific frontier*. New York: Free Press.

Barron, J. (2007). Steam blast Jolts Midtown, killing one. *New York Times*. URL: http://www.nytimes.com/2007/07/19/nyregion/19explode.html.

Borden, K. A., Schmidtlein, M. C., Emrich, C. T., Piegorsch, W. W., & Cutter, S. L. (2007). Vulnerability of U.S. cities to environmental hazards. *Journal of Homeland Security and Emergency Management*, *4*(2).

Borgatti, L. (2005). Status of infrastructure in the LDCs: A cluster analysis. Background paper prepared for the least developed countries report 2006, UNCTAD, Geneva.

Caruson, K., & MacManus, S. A. (2007). Designing homeland security polity within a regional structure: A needs assessment of local security concerns. *Journal of Homeland Security and Emergency Management, 4*(2), 7.

Changnon, S. A. (2008). Losses from sleet storms in the United States. *Natural Hazards, 47*, 465–470.

Church, R. L., & Scaparra, M. P. (2007). Protecting critical assets: The r-interdiction median problem with fortification. *Geographical Analysis, 39*(2), 129–149.

Cutter, S. L. (2006). *Hazards, vulnerability and environmental justice*. London: Earthscan Publications.

Cutter, S. L., & Finch, C. (2008). Temporal and spatial changes in social vulnerability to natural hazards. *Proceedings of the National Academy of Sciences, 108*(7), 2301–2306.

Fay, M., & Yepes, T. (2003). Investing in infrastructure: What is needed from 2000 to 2010? *World Bank*. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=636464.

Federal Aviation Administration (FAA) (2007). Capacity needs in the National Airspace System. URL: http://tinyurl.com/24attx.

Federal Emergency Management Administration (FEMA) (2008). Why dams fail. URL: http://www.fema.gov/hazard/damfailure/why.shtm.

Forrey, P. (2007). Airline delays and consumer issues. Testimony before the house transportation and infrastructure subcommittee on aviation. URL: http://tinyurl.com/5jftzn.

Glanz, J. (2004). Sabotage taking toll on Iraq's power lines. *New York Times*. June 11.

Grubesic, T. H., Matisziw, T. C., Murray, A. T., & Snedicker, D. (2008). Comparative approaches for assessing network vulnerability. *International Regional Science Review, 31*(1), 88–112.

Grubesic, T. H., & Murray, A. T. (2005). Spatial-historical landscapes of telecommunication network survivability. *Telecommunications Policy, 29*(11), 801–820.

Grubesic, T. H., & Murray, A. T. (2006). Vital nodes, interconnected infrastructures and the geographies of network survivability. *Annals of the Association of American Geographers, 96*(1), 64–83.

Grubesic, T. H., Murray, A. T., & Mefford, J. N. (2007). Continuity in critical network infrastructures: Accounting for nodal disruptions. In A. T. Murray & T. H. Grubesic (Eds.), *Critical infrastructure: Reliability and vulnerability*. Berlin: Springer.

Holton, G. A. (2004). Defining risk. *Financial Analysts Journal, 60*(6), 19–25.

Johari, R., & Tan, D. K. H. (2001). End-to-end congestion control for the Internet: Delays and stability. *IEEE/ACM Transactions on Networking, 9*(6), 818–832.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1), 11–27.

Keeney, M. (2005). *Computer system sabotage in critical infrastructure sectors*. U.S. Secret Service and CERT Coordination Center/SEA, Washington, D.C.

Kramer, A. E. (2009). Gazprom shuts off gas links to Ukraine. *New York Times*. URL: http://tinyurl.com/3mb24nh.

Lewis, T. G. (2006). *Critical infrastructure protection in homeland security*. New York: Wiley.

Lichtenstein, A. G. (1993). The Silver Bridge collapse recounted. *Journal of Performance of Constructed Facilities, 7*(4), 249–261.

Luft, G. (2005). Pipeline sabotage is terrorist's weapon of choice. *Energy Security*. URL: http://www.iags.org/n0328051.htm.

Lyons, W. (2010). Nabucco at center of gas politics. *Wall Street Journal*. URL: http://tinyurl.com/yehbd9g.

Mack, E. A., & Grubesic, T. H. (2009). Broadband provision and firm location in Ohio: An exploratory spatial analysis. *Tijdschrift voor Economische en Sociale Geografie, 100*(3), 298–315.

Marland, G., & Weinberg, A. M. (1988). Longevity of infrastructure. In J. H. Ausubel & R. Herman (Eds.), *Cities and their vital systems*. Washington, DC: National Academy Press.

Matisziw, T. C., Murray, A. T., & Grubesic, T. H. (2008). Exploring the vulnerability of network infrastructure to disruption. *Annals of Regional Science*. doi:10.1007/s00168-008-0235-x.

Matisziw, T. C., Murray, A. T., & Grubesic, T. H. (2010). Strategic network restoration. *Networks and Spatial Economics, 10*(3), 345–361.

McDaniels, T., Chang, S., Peterson, K., Mikawoz, J., & Reed, D. (2007). Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems, 13*(3), 175–184.

Merriam-Webster Dictionary (MW). (2008a). Vulnerability. URL: http://www.merriam-webster.com/.

Merriam-Webster Dictionary (MW). (2008b). Decay. URL: http://www.merriam-webster.com/.

Merriam-Webster Dictionary (MW). (2008c). Capacity. URL: http://www.merriam-webster.com/.

Minkel, J. R. (2008). The 2003 Northeast blackout—Five years later. *Scientific American*. URL: http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

Murray, A. T., & Grubesic, T. H. (2007). *Critical infrastructure: Reliability and vulnerability*. Berlin: Springer.

Murray, A. T., Matisziw, T. C., & Grubesic, T. H. (2007). Critical network infrastructure analysis: Interdiction and system flow. *Journal of Geographical Systems, 9*(2), 103–117.

Murray, A. T., Matisziw, T. C., & Grubesic, T. H. (2008). A methodological overview of network vulnerability analysis. *Growth and Change, 39*(4), 573–592.

Murray, C. J. (2007). Fatigue could loom large in bridge collapse. *Design News*. URL: http://tinyurl.com/5jclc8.

Nagle, J. (1984). Congestion control in IP/TCP internetworks. *Computer Communication Review, 14*(4), 61–65.

National Research Council. (2006). *Terrorism and the chemical infrastructure: Protecting people and reducing vulnerabilities*. Washington, DC: National Academies Press.

National Transportation Safety Board. (2004). CSX freight train derailment and subsequent fire in the Howard street tunnel in Baltimore, Maryland, on July 18, 2001. URL: http://www.ntsb.gov/publictn/2004/RAB0408.htm.

National Transportation Safety Board. (2008). Transportation for tomorrow: Report of the National Surface Transportation Policy and Revenue Study Commission. URL: http://www.transportationfortomorrow.org/final_report/.

Parfomak, P. W. (2005). Vulnerability of concentrated infrastructure: Background and policy options. CRS Report for Congress. URL: http://www.hsdl.org/?view&doc=55205&coll=limited.

Pederson, P., Dudenhoeffer, D., Hartley, S., & Permann, M. (2006). Critical infrastructure interdependency modeling: A survey of U.S. and international research. Idaho National Laboratory. URL: http://tinyurl.com/6fzweo.

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. Princeton, NJ: Princeton University Press.

Reid, R. L. (2008). The infrastructure crisis. *Civil Engineering*. January.

Richardson, H. W., Gordon, P., & Moore II, J. E. (2006). *The economic impacts of terrorist attacks*. Northampton, MA: Edward Elgar.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. December 11–25.

Sage, A. P., & White, E. B. (1980). Methodologies for risk and hazard assessment: A survey and status report. *IEEE Transactions on Systems, Man and Cybernetics, 10*(8), 425–446.

Sarewitz, D., Pielke, R., & Keykhah, M. (2003). Vulnerability and risk: Some thoughts from a political and policy perspective. *Risk Analysis, 23*(4), 805–810.

Schmidtlein, M. C., Deutsch, R. C., Piegorsch, W. W., & Cutter, S. L. (2008). A sensitivity analysis of the social vulnerability index. *Risk Analysis, 28*(4), 1099–1114.

Tighe, S., Li, N., Falls, L. C., & Haas, R. (2000). Incorporating road safety into pavement management. *Transportation Research Record, 1699*, 1–10. doi:10.3141/1699-01.

Transportation Research Board. (2005). Inspection and management of bridges with fracture-critical details. URL: http://onlinepubs.trb.org/Onlinepubs/nchrp/nchrp_syn_354.pdf.

U.S.-Canada Power System Outage Task Force (USCPSOTF). (2004). URL: https://reports.energy.gov/.

United States Geological Survey (USGS). (2008). URL: http://earthquake.usgs.gov/.

United States House of Representatives. (2006). A failure of initiative: The final report of the select Bipartisan Committee to investigate the preparation for and response to Hurricane Katrina. URL: http://katrina.house.gov/full_katrina_report.htm.

White House. (2003). The national strategy for the physical protection of critical infrastructures and key assets. URL: http://www.whitehouse.gov/pcipb/physical.html.

Willis, H. L. (2002). *Spatial electric load forecasting*. New York: CRC Press.