INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

Understanding Critical Infrastructure as Systems and Networks

Mark Scott

Understanding Critical Infrastructure as Systems and Networks

Mark Scott

Critical Infrastructure Consultant

July, 2025

Abstract

Critical infrastructure provides services that are essential to community health, safety, and well-being. Infrastructure assets, systems, and networks are characterized by their connections with other infrastructure, increasing the likelihood of cascading effects if they are disrupted, but analysis of these dependencies is not often integrated into emergency planning. This paper is intended to help private and public sector critical infrastructure protection practitioners expand their awareness of how infrastructure is connected, so they can use that knowledge to more effectively assess and mitigate risk to critical facilities. It achieves this purpose by applying network and systems science principles to explore the dependencies between infrastructure assets, examining how these connections change the risk profile of critical facilities, and suggesting actions for enhancing risk management approaches. Case studies of recent emergency events affecting Texas and other parts of the U.S. are included to demonstrate the importance of this approach. Users will be able to apply this knowledge across individual assets, sectors, and geographic scales based on available resources.

Keywords: cascading impacts; critical infrastructure; dependencies; network theory; systems thinking

Section 1: Introduction

Critical infrastructure delivers essential services to communities

"Infrastructure" is broadly understood to mean human-designed spaces that make up communities, often referred to as the Built Environment. The term "critical infrastructure" was first widely used in the United States during the 1990s in the context of national security, following concerns about vulnerabilities in essential systems. Today, critical infrastructures are considered to be engineered systems that are designed, built and managed to deliver basic and vital services. They are the backbone of modern economies and essential for community health, safety, and well-being. Many are privately owned and operated; others are managed by government, quasi-government authorities, and private-public partnerships.

Current U.S. national policy defines critical infrastructure as *physical and virtual assets, systems, and networks so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety*.[1] Each of the categories identified in this definition has unique characteristics:

- **Assets** are individual facilities with specific addresses and defined footprints. Security considerations are focused on a single location and designed to prevent intrusions in the operating systems or otherwise affect functions at that site. Assets usually have a single owner/manager, although occasionally this is shared between two or more organizations.
- **Systems** are made up of separate and distinct infrastructure assets that work together to deliver a service. Examples include natural gas supply and distribution, and food supply chains. For this type of critical infrastructure, risk is multiplied and spread across several assets, and a disruption anywhere in the system can have cascading effects. Critical infrastructure systems introduce a more complex risk picture due to their expanded threat surface and diversity of components.
- **Networks** are larger, interconnected webs of infrastructure systems providing similar functions and connected through geographic linkages. Examples include power grids, water pipelines, transportation routes, communication networks, and internet infrastructure. Like systems, networks have an expanded threat surface due to their interconnections that needs to be considered when managing risk.

The U.S Department of Homeland Security (DHS) categorizes the nation's critical infrastructure in 16 distinct sectors, based on the services they provide.[2] This

[1] National Infrastructure Protection Plan (NIPP) 2013; "National Security Memorandum on Critical Infrastructure Security and Resilience" (NSM-22), April 2024. This definition has been widely adapted for use by state and local jurisdictions across the country.

[2] The 16 critical infrastructure sectors are codified in Presidential Policy Directive 21 (PPD-21) issued in 2013. This directive establishes the framework for securing the nation's critical infrastructure and assigns responsibilities to

categorization has also been used by countries around the world who have made critical infrastructure a national priority.[3] Recently, DHS expanded the sector framework to identify "National Critical Functions" in recognition of the interconnectedness of individual sectors for service delivery.[4]

Protecting critical infrastructure has become a business imperative and public policy goal

Critical infrastructures are vulnerable to damage or failure from natural hazards, component aging, human error, and physical and cyberattacks. Disruption of infrastructure services can result in both **direct impacts** from the failure of individual components such as roads, railways, transmission infrastructure, buildings and other assets; and **indirect impacts** such as loss of income, disruption of supply chains, and injuries and fatalities. Because critical infrastructure services are vital for social and economic well-being, deliberate action by infrastructure owners and governments is needed to prevent or minimize these impacts and ensure they return to operational capability quickly if disrupted.

The current national goal for addressing infrastructure risk in the U.S. is enhanced security and resilience through implementation of focused risk management activities within and across sectors and levels of government. Key actions include identifying vulnerabilities, implementing security measures, developing response plans, and raising awareness among stakeholders to maintain resilience in the face of potential disruptions.[5]

Critical infrastructures are interconnected, which increases risk

An important characteristic shared by all categories of infrastructure is that they provide services through core elements that rely on other systems to function. These dependencies occur through linkages between components, by interconnecting different services, and from connections to larger regional, national, and even international networks. The resulting interconnected systems are complex, non-linear, and often geographically dispersed. While critical infrastructures have largely been developed and managed in isolation, economic and technological developments and the global context in which infrastructure operates have increased the connections between individual assets and systems.

Dependencies can strongly affect delivery of infrastructure services, such that failure of one infrastructure system or component can have cascading effects on other systems. For example, a power outage can disrupt transportation systems, leading to gridlock and delays; a water supply disruption can lead to sanitation problems and public health emergencies; and interruptions to communication networks can cripple financial

---

various federal agencies. Additionally, these sectors are referenced in the Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018 and the National Infrastructure Protection Plan.

[3] Weber, et al. (2023)

[4] U.S. Department of Homeland Security/CISA: National Critical Functions. See also Prier, et al. (2023)

[5] NIPP 2013 Supplement: Executing a CI Risk Management Approach

systems and economic activity. Cascading impacts also delay the rate of service restoration following a disruption, reducing resilience in coping with hazardous events.

Since 1997, a substantial body of empirical and predictive research has been devoted to identifying and analyzing infrastructure dependency-related risk.[6] Increasingly, techniques from the study of complex adaptive systems have been used to help understand networked infrastructure systems. Several models have also been developed to simulate dependencies across infrastructure systems and how they perform under various failure scenarios.[7]

As infrastructures become more interconnected, it is not enough to assess their individual components in isolation to evaluate risk. An incomplete understanding of these connections and the scale and scope of potential cascading failures limits the ability to prepare and adapt to disruptive events. Government officials responsible for protecting infrastructure within their jurisdictions need to understand how dependencies increase risk to critical systems and what steps are needed to mitigate these risks. Infrastructure owners and operators need to know the likely impact of disruptions from other infrastructures on their services, so they can develop business continuity and emergency operations plans and make more focused investments in resilience.[8]

> *"The essence of protecting these systems and ensuring their resilience during any crisis lies in our collective ability to develop and sustain a thorough understanding of the relationships among them. Infrastructure assets, clusters, systems, and networks are bound together through a series of complex dependencies and interdependencies. The failure of any single component in these networks can lead to a series of direct and indirect impacts and cascading failures."*
>
> TEXAS HOMELAND SECURITY STRATEGIC PLAN 2021-2025

For both government and business, using dependency analysis to more fully incorporate security and resilience thinking into decision making offers multiple benefits: it provides a better understanding of vulnerabilities, impacts on other infrastructure, and consequences when things do go wrong; it presents an opportunity for effective and proportionate mitigation action to ensure operational continuity following hazard events; and it enables more effective response to disruptions or system failures, and more timely recovery of services.

Infrastructure dependencies have not been integrated into business continuity and emergency planning

Managing critical infrastructure risk has traditionally focused on protecting individual assets, with only limited consideration of dependencies. Although dependency relationships can significantly disrupt infrastructure performance, these connections

[6] Gong, et al. (2023)
[7] Sun, et al. (2021)
[8] Bloomfield, et al. (2017)

have not been significantly integrated into operational, business continuity, and emergency preparedness plans.[9] There are several reasons why:

1. Dependency relationships are increasingly complex

   Recognizing and managing dependency-related risk is complicated by an ever-evolving threat environment -- including more frequent extreme weather conditions, changes in terrorism patterns, rapid development and urbanization, and shifts in demand patterns --which multiplies the likelihood of cascading impacts across networked systems. The convergence of information technology (IT) and operational technology (OT) has also created many new dependencies and significantly increased the complexity and vulnerability of infrastructure systems, making cyber-physical systems attractive targets for cyberattacks. Similarly, many supply chains increasingly rely on a small number of third-party service suppliers, such that any disruption to those suppliers can affect several infrastructure systems with cascading impacts across multiple communities.[10]

2. Assessment tools don't fully illustrate dependencies

   Existing methods of classifying dependencies are fragmented and lack a comprehensive, universally accepted framework.[11] There is also no clear or consistent way to identify and assess interdependencies.[12] With few exceptions, even quantifying the linkages between infrastructures, their dependencies, and failure mechanisms, is rarely done.[13] The assessment approaches which do describe mutual dependencies across sectors don't completely capture the systemic nature and dynamic behavior of connected infrastructure systems.[14] Where assessment methodologies have been developed, most have not been significantly socialized and adopted for regular use across the potential user community.[15]

   Moreover, it is difficult to accurately model the behavior of interactions within a single system, let alone across a wider network. Some risk prediction models have been developed for infrastructure systems such as electrical power grids, water networks, traffic flow, and rail systems. Yet few models tie connected infrastructures together in a form that represents their actual operation. Where such models do exist,

[9] Sonesson, et al. (2021); personal communications with Mike George, Clint Ladd and David Garcia, Texas Department of Public Safety, February 25, 2025; Alexandra Lampson, DC Homeland Security and Emergency Management Agency, March 6, 2025, and Justen Noakes, KTLO Solutions, May 1, 2025.
[10] Setola (2025)
[11] Dasuni, et al. (2024)
[12] Sonesson, et al. (2021)
[13] Schweikert, et al. (2021)
[14] Rathnayaka, et al. (2025)
[15] Personal communications with Leslie-Anne Levy, Argonne National Laboratory, April 22, 2025; William McNamara, DHS/CISA Region 3, March 28, 2025; and Edwin Otten, DHS/CISA Region 6, April 23, 2025.

problems of inconsistent usage and lack of technical guidance hinder their practical application.[16]

Decision support systems have been built in recent years to support risk management decision-making. These software systems can help assess risks to critical infrastructure by combining real-time data analysis with threat modeling to suggest mitigation strategies and provide guidance during crises and emergencies. Some decision support systems are starting to incorporate dependencies, but still struggle to fully capture the complex relationships between sectors.[17] This leads to incomplete risk assessments and less effective mitigation strategies.

3. Gathering, sharing, and maintaining dependency information is challenging

   Assessing dependencies requires large amounts of high-quality data from multiple sources to realistically represent infrastructure topology, behavior, and failure consequences. Many states, localities, and stakeholder organizations lack the staffing, funds, and technical expertise to support the extensive data collection and detailed modeling needed to conduct complete dependency assessments.

   Information security and competitive business concerns, along with a reluctance to reveal points of operational weakness, can also hinder the sharing of infrastructure data between sectors and with government, limiting the accuracy of modeling and other dependency analyses. Related issues include lack of technical tools to efficiently exchange and maintain confidential and security-sensitive information, and knowing at what point non-sensitive information becomes sensitive when aggregated.

4. Effective collaboration mechanisms are lacking

   Stakeholder engagement is needed to ensure a more complete understanding and response to dependency-related risk. However, effective and sustainable methods for collaborating across infrastructure sectors and between infrastructure owners/operators and public agencies are often hampered by unclear delineations of risk ownership and control, lack of trust between parties in protecting information, and priority on internal core business or mission needs at the expense of cross-sector and private/public collaboration. The absence of incentives for working together to conduct dependency analyses limits understanding of these interconnections and perpetuates a silo approach to risk management.

[16] Sun, et al. (2021) and Rathnayaka, et al. (2025)
[17] Hajializadeha & Imani (2021)

Purpose of this paper

This paper offers a pathway for wider application of dependency-related risk information across the critical infrastructure community. It is directed primarily to infrastructure owners/operators and to government agencies with a critical infrastructure protection mission, recognizing that resources and capabilities vary widely within both groups.

Given the importance of understanding infrastructure connections, along with the challenges in knowing and using that information, this paper considers three questions: (1) what do we need to understand about how critical infrastructures are connected? (2) what can systems and network science tell us about dependency-related risk? and (3) what are key actions available to all infrastructure partners for applying this information to strengthen protection and resilience?

A Word on Terminology

For simplicity and brevity, this paper uses the terms **dependency** and **dependency-related risk** to refer to both one-way dependencies and two-way interdependencies, which are defined in Section 2.

Section 2: What do we need to understand about infrastructure dependencies?

There are multiple dimensions of infrastructure dependency

Prior research has conceptualized four types of infrastructure dependency[18] that are commonly recognized today:

- *Physical*, where infrastructure assets are dependent upon other services to continue functioning. Example: a water treatment facility relies on chemicals and electricity produced by external providers.
- *Geographic*, where physical components or activities of two or more infrastructures are co-located within a prescribed geographical area. Geographical dependencies often highlight clusters of infrastructure and local single points of failure which more than one infrastructure site may depend. Examples: (1) gas, electric, and water lines may share a right of way and can all be disrupted simultaneously; (2) two adjacent chemical processing plants may both depend on a local electricity substation, communications exchange or access road.
- *Cyber*, where the state of one infrastructure system is dependent on data transmitted via information technology systems to support operations. Example: a bulk petroleum fuel terminal relies on information technology and communication systems to operate accounting and billing systems to distribute fuel.
- *Logical*, where operations rely on other systems due to economic, policy, or human factors, and are not the result of physical or cyber processes. Example: travel restrictions in one region impact cross-region transportation of goods.

Connections between infrastructure and its users may be either direct or indirect, and either dependent or interdependent, as shown in Figure 1.

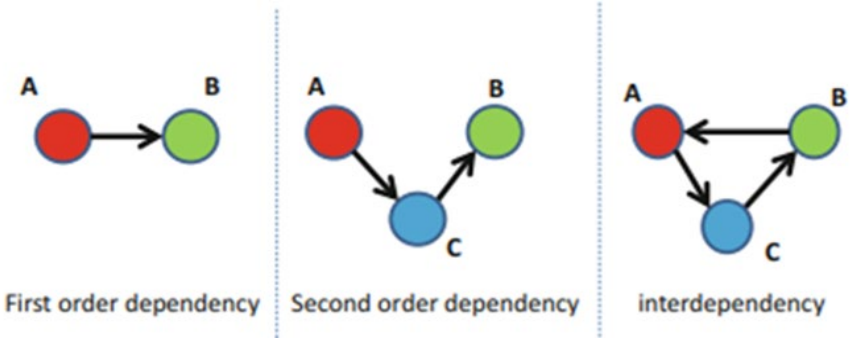


Figure 1: Types of infrastructure dependencies[19]

[18] Rinaldi, et al. (2001)

[19] Setola & Theocharidou (2017)

A “first-order” dependency is a relationship in which an infrastructure asset provides a direct service or resource to a user. This occurs through a specific connection for delivering the service or resource, and by which the operation of the upstream infrastructure asset has an immediate impact on downstream users.

A “second-order” dependency is a relationship in which an infrastructure asset indirectly supports a downstream entity. These include upstream interactions between interdependent infrastructure assets that are critical for the operation of one or more assets that ultimately provide direct services or resources to a user. Additional order levels of dependency can exist depending on the extent of the system or network.

Infrastructures can also be “interdependent”, where dependencies between two assets exist in both directions and rely on each other to operate. Interdependencies can be physical, geographic, or cyber. Examples include:

- *Electricity and water*: Water is needed as a coolant for many power plants, and water treatment plants need electric power to operate.
- *Energy and manufacturing*: Energy is used to run manufacturing facilities, and manufacturing facilities produce components for energy systems.
- *Communications and energy*: telecoms infrastructure is dependent on the power network, which is in turn dependent on telecoms to monitor and control the system.

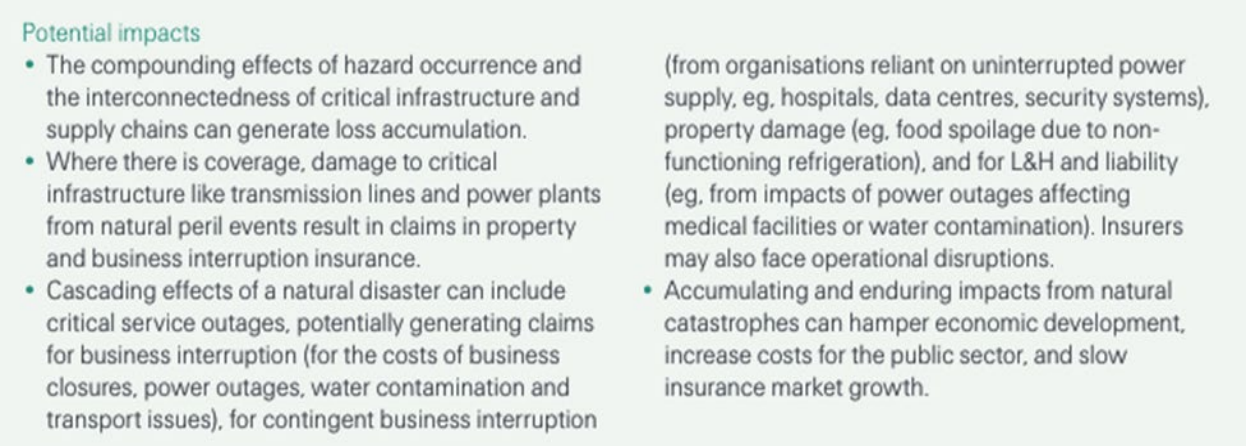
Dependency relationships increase infrastructure risk

Under normal operating conditions, dependencies improve the reliability and efficiency of infrastructure services. However, reliance on connectivity means that a local service disruption caused by a natural disaster, human-caused threat, or unforeseen failure mode could spread to other infrastructure components, leading to cascading failures across the system.

Impacts from one infrastructure disruption may also extend well beyond the individual system directly affected by an event, creating cascading and escalating failures across other dependent infrastructure systems and jurisdictional boundaries and causing significant economic and physical damage on a citywide, regional, or even national or international scale. Because of infrastructure dependencies, such cascading disasters have become more common.[20]

[20] Lewis & Petit (2019)

Increasingly, the insurance industry is assigning higher risk ratings to cascading impacts from infrastructure dependencies, reflecting the increased cost of service disruption. Figure 2 show how these risks are recognized by insurance company Swiss Re:[21]



Potential impacts

- The compounding effects of hazard occurrence and the interconnectedness of critical infrastructure and supply chains can generate loss accumulation.
- Where there is coverage, damage to critical infrastructure like transmission lines and power plants from natural peril events result in claims in property and business interruption insurance.
- Cascading effects of a natural disaster can include critical service outages, potentially generating claims for business interruption (for the costs of business closures, power outages, water contamination and transport issues), for contingent business interruption (from organisations reliant on uninterrupted power supply, eg, hospitals, data centres, security systems), property damage (eg, food spoilage due to non-functioning refrigeration), and for L&H and liability (eg, from impacts of power outages affecting medical facilities or water contamination). Insurers may also face operational disruptions.
- Accumulating and enduring impacts from natural catastrophes can hamper economic development, increase costs for the public sector, and slow insurance market growth.

Figure 2: Cascading impacts present increased insurance risk

Several high-profile disasters since 2001 – among them the World Trade Center terrorist attack (2001), Northeast U.S./Canada power outage (2003), Hurricane Katrina (2005), Iceland volcanic eruption (2010), and the worldwide Covid-19 pandemic (2020) -- have illustrated the extent of cascading failure impacts due to critical infrastructure dependencies.[22] More recent events such as the December 2020 Nashville bombing, February 2021 Winter Storm Uri, May 2021 Colonial Pipeline cyberattack, and July 2024 global internet outage highlight the continued nature of dependency risk; case studies of these cascading impact events are included in Appendix A.

Duration of infrastructure failure is the primary factor for determining impacts from a cascading event and what is needed to fully recover system operations. Duration will vary depending on specific disruption scenarios and the temporal or spatial locations of the system components affected. The extent of impacts also depends on the size of the disruption, strength of the dependencies, and the ability of the infrastructure to adapt.[23]

Studies exploring dependencies, using both empirical approaches and predictive research, have concluded that:[24]

[21] Swiss Re SONAR New emerging risk insights. Swiss Re Institute, June 2024

[22] A summary of the cascading events, pathways, and types of dependencies for these and other global disasters can be found at Gong, et al. (2023).

[23] For example, if a storm event or accident causes significant damage to a major bridge or roadway, and alternative transport options are limited, this can impact commuters, freight traffic and emergency services. See May 2021 Mississippi bridge closure, June 2023 Philadelphia interstate collapse

[24] Li, et al. (2022)

- The most common dependency type among critical infrastructures is physical, followed by geographic, and more than 79% of infrastructure interaction behaviors are highly interdependent.
- Almost all cascading effects across critical infrastructure propagate within first and second-order ranges, accounting for 80.4% and 17.9%, respectively.
- The most frequently cascading behaviors occur between power systems and transportation, critical manufacturing, water supply, and healthcare sectors.[25]

[25] In the aftermath of Hurricane Beryl in 2024 impacting Texas, it was noted that "When a power outage hits a city, some services immediately disappear. After Hurricane Beryl, stoplights ceased working; some gas stations, which provided critical services to anyone running a generator, lost power themselves and closed. Cell towers not equipped with their own backup power went down, severing thousands of people from communication with the outside world." Washington Post, *The disaster no major U.S. city is prepared for*. September 13, 2024.

Section 3: What can network and systems theories reveal about dependencies?

The nature of infrastructure dependencies and how they impact risk can best be understood by applying network and system theory principles. In both areas of study, connectivity is the primary area of focus. Instead of viewing a problem in terms of single, discrete entities, these disciplines describe interconnections that exist and how they facilitate the flow of information, resources, and other concepts.

Network theory described

Network theory provides a framework for analyzing how objects interact in a system and how those connections influence system behavior. It uses graphs to represent systems, with **nodes** (system components) representing discrete objects and **edges** (connections between components) representing interactions between them, as shown in Figure 3.[26]

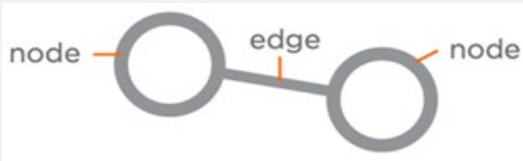


Figure 3: Networks are represented by nodes and edges

The basic node-edge construction of networks provides a useful model to understand how complex systems are structured and how interactions occur. It helps predict how a system will behave under various scenarios, considering the key properties of the network:[27]

- Decentralization – is the network centralized or decentralized?
- Centrality – which are the most important nodes?
- Diffusion – how will something spread across the network?
- Dynamics – how is the network growing?
- Degree distribution – how evenly distributed are the connections?
- Resilience – how easily can the network components adapt to changes?

Systems follow this construct because the interactions between individual nodes "add up" to become the large-scale behavior of the system, including the ability to self-organize and adapt to changing conditions following a disruption. This can reveal critical points of failure within the system and ultimately lead to improved system performance.[28]

[26] Cabrera & Cabrera (2020)
[27] Ibid.
[28] Cheng, et al. Task allocation in manufacturing: A review and Kizhakkedath & Tai, (2021)

Systems theory described[29]

Systems theory, also known as systems thinking, is a conceptual framework for understanding complex systems by examining their components, interactions, and relationships, and then using that knowledge to improve management of the system. Its core principle is that elements in a system influence and rely on each other.

In systems theory, interactions between elements can be both direct and indirect. Direct interactions involve immediate exchanges of information, resources, or energy between elements. Indirect interactions occur when changes in one element have indirect effects on other elements through a chain of interconnections. Systems theory recognizes that changes in one part of a system can have ripple effects throughout the entire system.

Systems analysis is the technique used to break down a system into its individual components to understand how they interact and work together, and how they evolve and adapt over time. Doing this helps identify problems, potential improvements, and solutions to optimize performance and achieve desired goals.

"Systems thinking is a discipline for seeing wholes. It is a framework for seeing interrelationships rather than things, for seeing patterns of change rather than static snapshots."

Peter Senge, American systems scientist and senior lecturer at the MIT Sloan School of Management

How network and systems theories help understand dependency-based infrastructure risk

Network theory shows how individual components in an infrastructure system are connected and how they interact. Systems theory shows how those components work together to produce a good or service, and how they may evolve and adapt in response to disruptive events or changes in the operating environment. Together, they help practitioners better assess risk and plan accordingly.

Network theory is used to depict an infrastructure system as a mathematical graph containing nodes, links, and a map showing connections between nodes, as illustrated in Figure 4.[30] This allows decision-makers to anticipate and mitigate dependency-related risk in several ways:

[29] Systems Thinking: A Holistic Approach to Solving Complex Problems; Senge, P. "The Fifth Discipline: The Art and Practice of the Learning Organization: First edition" (2010).

[30] Transportgeography.org

- *Identifying critical points*: by defining how the system is structured, network theory identifies which nodes are highly connected and considered critical points within the system, meaning their failure could have cascading effects.
- *Identifying vulnerabilities*: knowing the number of connections a node has, and how important a node is in connecting other nodes, will help identify the components that, if disrupted, could cause large-scale cascading failures.

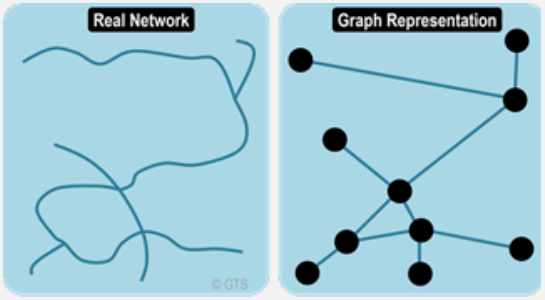


Figure 4: Infrastructure systems can be mapped using graph theory

- *Informing resilient design*: network theory will reveal options for improving system resilience, such as increasing the number of alternative paths and components within the network to reduce the risk of single points of failure and create multiple layers of protection; reducing reliance on high-centrality nodes by distributing network functions and resources more evenly; and developing mechanisms to monitor network health and detect potential disruptions before they escalate.

With this base understanding of a network's structure, systems analysis can then be used to address dependency-related risk by (1) determining which systems are most "critical" based on their impact on public safety, economic stability, and national security; (2) understanding how different infrastructure systems rely on each other, identifying potential cascading effects if one system fails;[31] (3) analyzing the full range of potential threats to system components and evaluating the likelihood and severity of their impact; (4) examining potential vulnerabilities in physical security, cyber defenses, and operational procedures; and (5) developing actions to reduce risk, and establishing metrics to measure overall risk reduction from such actions.

[31] Node failure in critical infrastructure networks can be triggered either in a random event (e.g. natural hazard, technical failure) or in an intentional manner (e.g. terrorist attack). When a random event occurs in a network, a number of its nodes are randomly removed from the network; while in a targeted attack, the nodes are systematically broken down. Different triggers of node failures may result in different levels of failure consequences. Kizhakkadeth & Tai (2021)

Examples of how network and systems theories can address infrastructure risk:

Power grid vulnerability analysis: (1) identifying critical substations and transmission lines by analyzing their network connectivity and potential cascading effects due to disruptions; (2) analyzing grid components as a network to understand potential blackouts resulting from cascading failures.

Water system resilience assessment: (1) studying the resilience of a distribution system by analyzing how disruptions at a treatment plant might impact other areas and potential recovery pathways; (2) modeling treatment plants and pipelines to identify contamination risks and optimize water flow.

Transportation network disruption analysis: (1) identifying critical transportation hubs in a network and assessing impact of disruptions on overall traffic flow; (2) studying road connections to identify traffic bottlenecks and assess the impact of disruptions like road closures.

Telecommunication networks: (1) analyzing connectivity of cell towers and fiber optic cables to understand potential disruptions in communication; (2) identifying the topology of regional communications systems to identify critical links supporting 911 centers.

Section 4: How can this knowledge be put into practice?

Dependency analysis is a necessary input for managing critical infrastructure risk. Insights provided by network science and systems thinking will expand awareness of connections and potential cascading failures. This in turn can help design and implement strategies to reduce risk. Decision-makers should plan emergency response from a systems perspective, considering potential threat scenarios, and then conduct targeted preparedness and mitigation efforts.

For critical infrastructure owners/operators, decision support for business continuity and operational resilience needs to include awareness of the external linkages that affect their service delivery. This knowledge can help guide design, operations, and managerial strategies to improve resilience and sustainability of the underlying infrastructures.[32] Governments should use understanding of infrastructure dependencies to meet their public safety responsibilities and work productively with infrastructure owners/operators in mitigating the potential for cascading impacts from a disruptive event.

This section identifies three broad strategies for developing and using dependency-related risk analysis to enhance critical infrastructure protection and resilience: (1) map and analyze dependency relationships; (2) build and manage new partnerships; and (3) incorporate dependency analyses into emergency planning. Each strategy can be conducted at a baseline level and scaled up as resources are available. Together, these actions will significantly improve an organization's ability to prepare for, respond to, and recover more quickly from the cascading effects of an infrastructure disruption.

Strategy 1: Map and analyze dependency relationships

Operational resilience is the ability to deliver services through disruption from any hazard. But it is not possible to know if an infrastructure asset is resilient without first understanding what goes into its operations. Dependency mapping does this by identifying and documenting all the activities involved in delivering critical services.

Mapping dependencies involves systematically identifying and documenting connections between different infrastructure systems. Dependency mapping enables users to identify vulnerabilities such as single points of failure, better plan exercises around potential disruptions, and test possible remediations if disruptions were to occur.

Dependency mapping also helps better mitigate risk. Organizations with strong dependency mapping practices will be better positioned to prioritize and optimize incident response and recovery protocols to ensure as much uptime as possible. By recognizing potential vulnerabilities in delivering core products and services, asset owners can better manage operational risk. Governments can use this knowledge to better target response and recovery resources. Both can use mapping to support resilience investment decisions.

[32] Valinejad & Mili (2023)

Dependency mapping includes these steps:

- Identify the services that support the infrastructure assets, systems, and networks of concern, including their locations and operational details.
- Gather data from multiple sources including interviews with infrastructure operators and experts; technical documentation such as system diagrams, operational manuals, and technical specifications; and on-site inspections to observe physical connections and operational processes.
- Analyze the direct physical connections between system components, data flows between systems, and operational dependencies, to show how disruptions in one system could impact the functionality of other systems.
- Use visualization techniques such as **geospatial mapping** to illustrate time and space factors affecting dependency relationships; **flowcharts** to illustrate the sequence of operations and data flows between different critical infrastructure assets; **network diagrams** to visually represent the physical connections between infrastructure components; and **dependency matrices** to show the impact of disruptions in one system on other related systems.[33]

Figures 5, 6, and 7 show how dependencies can be visualized at different levels:

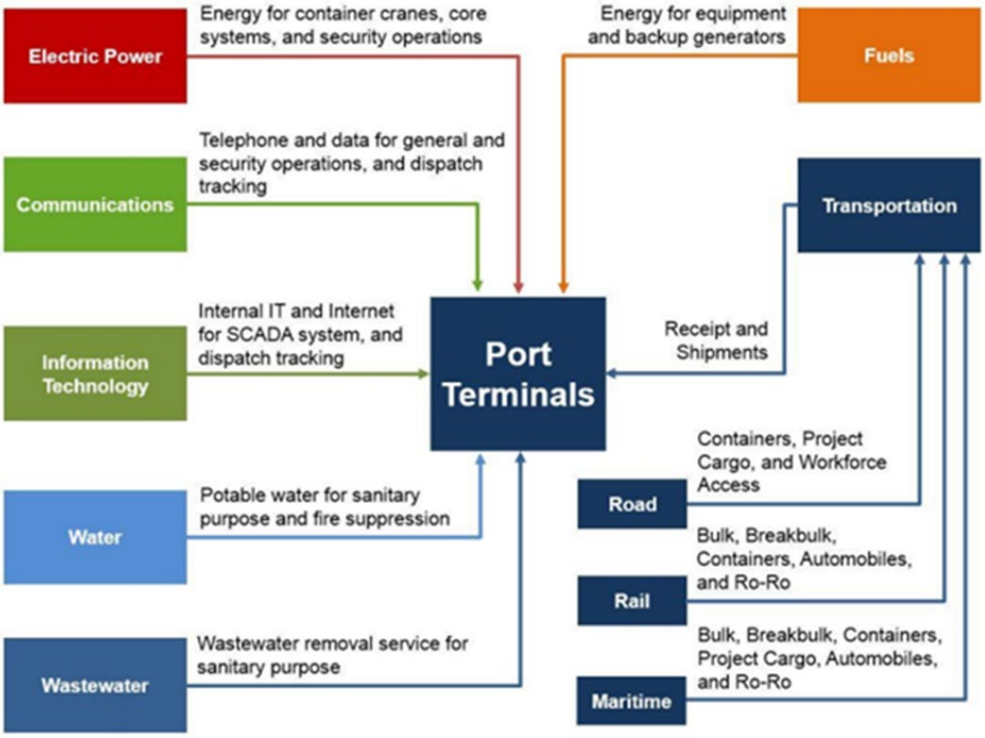


Figure 5: Asset-level mapping showing dependencies

[33] Macaulay (n.d.)

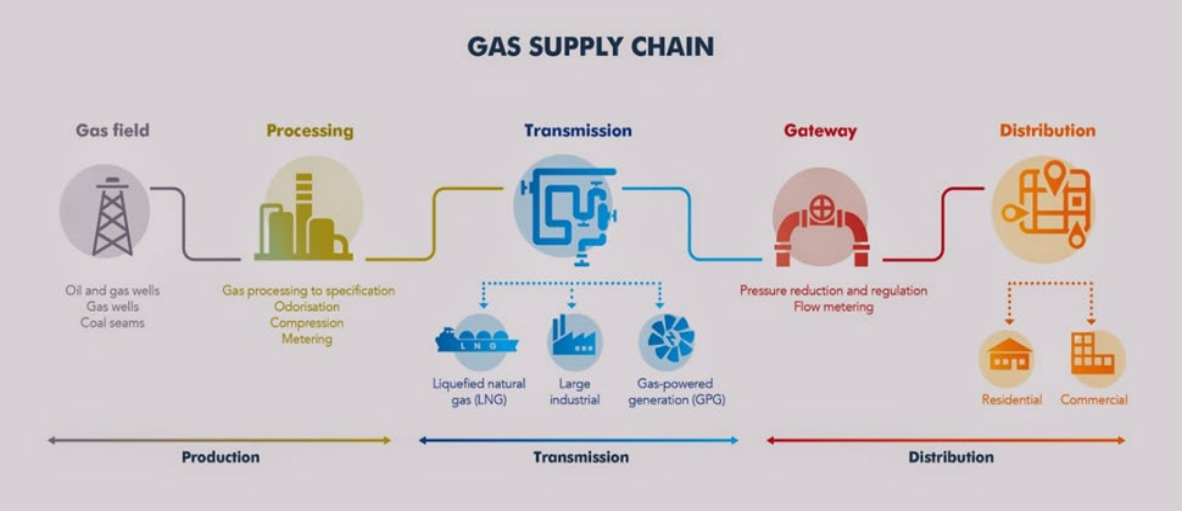


Figure 6: Sector-level mapping showing dependencies between system components[34]

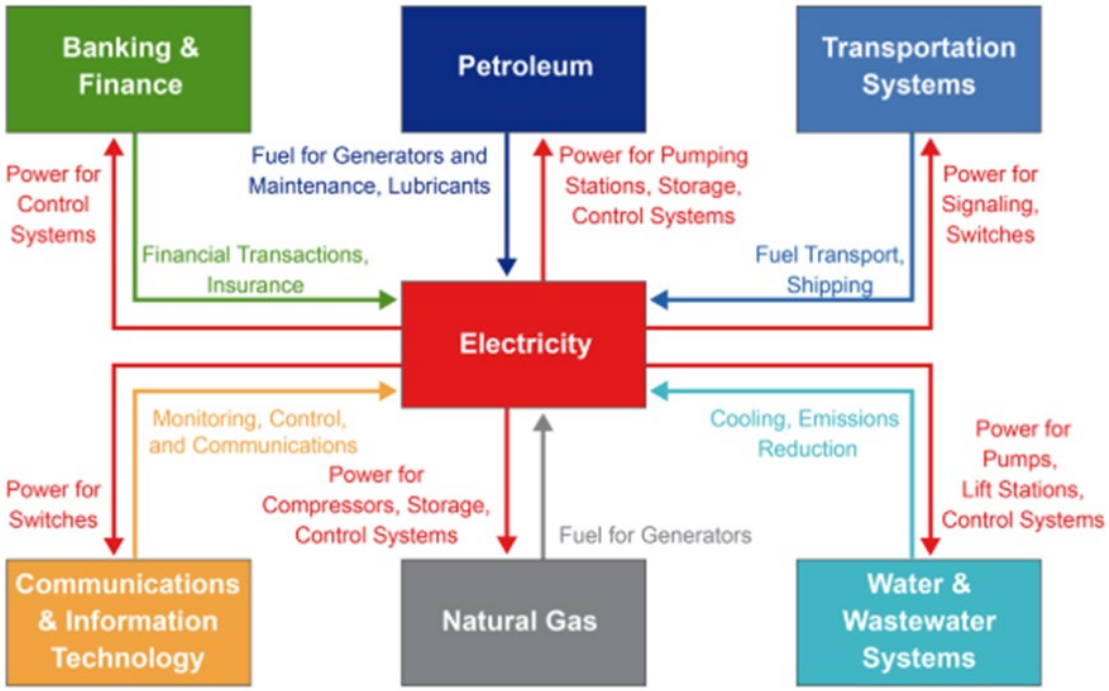


Figure 7: Sector-level mapping showing dependencies and interdependencies[35]

[34] Texas Oil and Gas Association

[35] *Impacts, Risks, and Adaptation in the United States: The Fourth National Climate Assessment, Volume II*

Strategy 2: Build and manage new partnerships

Each component of a critical infrastructure system plays a role in maintaining delivery of services from that system. Dependency mapping will identify the components that are most critical for system functioning and show who needs to be engaged before, during, and after a disruptive event. Knowing the operating procedures, contingency plans, and resilience protocols that guide each component's actions will help maintain system functions and ensure more coordinated response and recovery if disrupted.

Importantly, dependency mapping may reveal partners who have not been engaged in the past. For example, examining a supply chain for food, fuel, or healthcare supplies will identify multiple producers, suppliers, and transporters who must work together to ensure timely delivery of these essential commodities, but who may not have been previously known. Identifying all the partners needed to make a system work opens new possibilities for broader visibility, better situational awareness, and more rapid response and recovery.

For both infrastructure operators and government representatives, individual consultations with these component partners will clarify their ability to maintain operational capability during a cascading event. Key questions to ask include:

1. Are there redundancies in operations that will allow activity to continue during a disruption?
2. Have appropriate preparedness and response plans been developed to enable rapid restoration of service and reduce overall downtime?
3. Have systemic measures been adopted to improve recovery performance, such as regular maintenance, adequate response budgets, efficient organizational processes, and emergency training?

Once all critical partners are known, a shared understanding of collective risks within a jurisdiction or infrastructure system can be developed and used for coordination between organizations. With knowledge of dependencies, partners will be able to work together to gain clarity about the anticipated performance of infrastructure systems under various hazard scenarios, identify desired service restoration times, and develop short and long-term resilience goals to be pursued.

Multi-stakeholder workshops are a proven way to develop this shared understanding of dependencies. Such events enable partners to jointly discuss and map connections between operations, record which links are critical, and identify which failure points could lead to cascading consequences. Often these workshops include discussion-based exercises to consider cascading effects from different hazard scenarios. For some jurisdictions, establishing more formal private-public sector engagement mechanisms provides an effective way to continue this collaboration.

As with all stakeholder engagements, trust between parties is essential for successful outcomes. Open and honest dialogue, common understanding of issues, and clear

protocols for sharing and managing information will ensure more complete awareness of how infrastructure components are connected, what cascading impacts could occur, and how response and recovery could be coordinated. Non-disclosure agreements (NDAs) and data-sharing agreements can help meet the need for enhanced information sharing which may conflict with an organization's willingness to share or validate information due to competitive or legal liability concerns.

Partner engagement for dependency mapping in Dallas, TX

- As part of a city resilience workshop in 2015, the city of Dallas hosted a scenario-based session mapping cascading impacts for a number of climate change-related shocks and stresses.
- One of the fictional scenarios was related to drought or failure in long term water supply: *"Rapid population growth in the Dallas-Fort Worth-Arlington metropolitan area continues at record pace and forecasts outpace the region's long-term, water resource plan. This potential shortage is exacerbated by record drought conditions that strain current water supply. Lawsuits have limited the water authority's ability to develop additional lakes and reservoirs in East Texas and the region's long-term water supply is threatened. Business leaders warn local officials of plans to relocate manufacturing businesses and water-intensive industries out of the greater Dallas area unless solutions are reached quickly."*
- Participants identified shocks and stresses in this scenario, dependencies between sectors, and cascading impacts. They also discussed potential initiatives to strengthen the response to an event of this nature. The workshop aimed not only to map these dependencies and cascading impacts, but also to raise awareness about the repercussions of climate impacts across sectors.

Source: C40, "How to manage infrastructure interdependencies and cascading risk". March 2022.

Strategy 3: Incorporate dependency analyses into emergency planning

Identifying infrastructure dependencies and key partners are important steps toward more informed decision-making and better outcomes. To put this information to work, private and public sector partners should upgrade strategic and operational plans to identify dependencies and their potential impact on operations.

Dependency insights can be incorporated into risk assessments, hazard mitigation planning, community and environmental planning, capital improvement planning, emergency response planning, business continuity planning, and multiple types of regional planning. This can be done in several ways:

- Include a description of critical infrastructure systems and their associated dependencies in the community overview section of any plan.
- Use dependency awareness to prioritize critical infrastructures for mitigation, response and recovery.

- Apply dependency analysis to identify obstacles to resilience that need to be addressed and by whom.
- Identify new projects, policies, or procedures to mitigate dependency-related risks.
- Incorporate dependency considerations in any project cost-benefit analysis.
- Conduct stress test exercises and simulations between connected infrastructure sectors, which could illuminate areas for improvement and build resilience.
- Use dependency analysis to identify new Essential Elements of Information that can guide consequence management during emergency events.
- Review After Action Reports from past emergency events to identify dependency-related failures and cascading impacts, for use in future planning.
- Update risk assessments to include new mitigation and adaptation actions, and to ensure that any risks they might create are reflected in resilience plans.

Tools to Help Incorporate Dependency Risk in Planning

The DHS/CISA **Dependency Analysis Framework** and **Infrastructure Resilience Planning Framework** outline a consistent analytic approach used by CISA for evaluating infrastructure dependencies and provide a process for incorporating dependencies and other critical infrastructure resilience considerations into planning activities. CISA's **Infrastructure Survey Tool (IST)** and **Security Assessment at First Entry (SAFE)** tool include identification of dependencies for individual assets, and its **Regional Resilience Assessment Program (RRAP)** considers dependencies in systems and networks.

The National Institute for Standards and Testing (NIST) **Community Resilience Planning Guide** includes an overview of possible dependencies between social systems and buildings and infrastructure systems for consideration when setting performance goals for response and recovery times. Available tools for identifying dependencies, predicting impacts, and mitigating or managing dependencies are also presented.

The **All-Hazards Analysis (AHA)** methodology developed by Idaho National Laboratory models infrastructure systems as directed multidimensional graphs, enabling the evaluation of cross-sector dependencies before, during, and after disruptive events.

Applying these strategies at the asset, jurisdiction, and sector levels

Identifying dependency relationships at an asset level is best conducted by the asset owner. It involves identifying dependencies within the same sector as well as on assets from other infrastructure sectors. This helps inform strategic planning and capital investment decisions to improve long- term operational resilience.

The asset-level approach follows this process:

- Examine the asset to identify key dependency relationships within the sector and with other critical infrastructure sectors.
- Identify the most critical processes within the asset, and the services and providers which support these processes.
- Establish the impact of disruption through loss of the dependent relationships.
- Develop information sharing protocols and non-disclosure agreements to protect commercially sensitive information and facilitate partnership working and information sharing.
- Use GIS mapping to plot supply routes for the critical services into the asset.
- Use the mapping to identify any critical points where service routes overlap and present an additional vulnerability or single points of failure for critical processes within the asset.
- Conduct a table-top exercise involving potential disruptive scenarios, in order to test the asset's resilience.
- Work with the service providers to ensure that delivery processes for the services are robust and resilient.
- Use the findings of this work to update business continuity plans and identify investments to strengthen the resilience of the site.

Identifying dependency relationships at the community level is best led by local emergency management organizations. It involves looking at communities in a geographical area and determining the networks and critical infrastructure which provides essential services to those communities.

An important element of the community-level approach is that local emergency responders and infrastructure owners work together to ensure common understanding of critical systems and their dependencies. Their collective knowledge of operations and potential service disruptions can support specific planning assumptions needed for preparedness planning. For example, areas surrounding an industrial plant can be analyzed for other critical infrastructure that could be affected by an explosion at the site; or a geographical area can be analyzed for infrastructure that could be affected by a flood.

The community-level approach follows this process:

- Focus on a specific community (town/city/district/region/zone).
- Have members individually identify potential significant local infrastructure and known dependencies.

- Create a master list and map of significant local infrastructure for the community.
- Establish the consequences to the community of failure of the significant local infrastructure.
- Test community resilience through exercises, and identify vulnerabilities, capability gaps, and mitigation measures to improve resilience.
- Use the findings of this work and resulting recommendations to update community response and recovery plans.

Identifying dependency relationships at the sector level is generally best guided by the leading government departments, to get a fuller understanding of dependencies within and between sectors. The information can then contribute to policy and investment decisions and inform engagement with infrastructure operators.

The sector-level approach follows this process:

- Focus on each priority sector represented in the jurisdiction.
- Work with sector representatives to identify direct dependencies of key sector assets, systems, and networks with other sectors.
- Prepare a dependencies matrix to catalogue the key dependencies of the sector
- Determine vulnerabilities and identify capability gaps.
- Test sector resilience to disruptive events through exercises and identify risks, vulnerabilities, and capability gaps.
- Use the results in a sector workshop to identify a program of measures to raise the resilience of the sector.
- Apply this information to support security and resilience regulations, policies, plans, and investment strategies.

Section 5: A Way Forward

The impact of dependencies on infrastructure risk is clear. Complexity in critical infrastructure systems and networks leads to fragility and instability; the disruption of any one of the innumerable connected components can disrupt whole systems. As economic and technological advances continue to shrink geographies and more tightly bind systems together, the potential for cascading harm expands.

Knowing dependency risk and putting that information to work to ensure service delivery and strengthen community security and resilience is thus a business imperative for the owners and operators of infrastructure, and a mission imperative for the governments whose citizens depend on the essential services that infrastructure provides.

This paper seeks to offer a roadmap for both business and government to operationalize dependency analysis as they plan for, respond to, and recover from emergencies and disasters. Recognizing the challenges this task poses, the three strategies outlined above provide steps that can be conducted even when resources are limited. Doing so will help ensure more secure and resilient outcomes.

Appendix A: Cascading impact case studies

Case Study #1: Nashville bombing

On December 25, 2020, an individual detonated a vehicle-borne improvised explosive device in downtown Nashville, Tennessee in front of a commercial communications network facility. The explosion killed the attacker, injured eight others, and caused widespread damage to the network facility and surrounding buildings.

This attack disrupted about 170 public safety answering points (911 centers) in the immediate and neighboring areas, and as far away as Kentucky and Alabama. The outages impacted some 911 centers for over a week. Telephone, data, and internet outages were also seen as far as Atlanta, Georgia. Flights were grounded at the Nashville airport, and communications systems were disrupted for many law enforcement agencies and hospitals, including one Nashville hospital where doctors and other workers relied on phones using a different provider and slept in the hospital to maintain contact.

Source: CNN

Source: downdetector.com

Lessons learned:

- While investigators determined that the attacker's choice of location for the explosion was not motivated by any specific ideologies, the bombing showed the potential damage and cascading disruption across a wide geographic area from an attack targeting a single infrastructure asset.
- The resulting outages revealed systemic weakness of the connections that have become increasingly essential for communications systems. It also illustrates the extent to which communication networks, cloud computing services and the internet are interdependent, and the vulnerabilities this creates.

Sources: SAFECOM; downdetector.com

Case Study #2: Winter Storm Uri

In February 2021, severe winter weather conditions associated with Winter Storm Uri triggered an energy infrastructure failure in Texas. Most state residents lost electricity; some lost potable water, natural gas, and suffered other infrastructure-related service disruptions that had profound household consequences. According to a University of Houston study, 69% of Texans lost electrical power, and about half lost access to running water. Other infrastructure-related impacts of the storm include difficulty obtaining food or groceries, the loss of internet service, and difficulty obtaining bottled water.

The severe impacts during Uri occurred in part because the storm triggered an energy infrastructure failure. During this event, natural gas producers were shut off during blackouts, which led to freezing in pipes and a lack of supply to keep power plants going, which led to even more power outages. The winter weather conditions, infrastructure failures, increased energy demand, and fuel limitations during the storm, all led to deteriorated power grid conditions, causing load shedding and rolling blackouts across the Electric Reliability Council of Texas (ERCOT) service area. The power demand so greatly exceeded generation capacity that many Texans were without power for days at a time.

Source: DHS/CISA

Source: Fox 4 News Dallas-Fort Worth

Lessons learned:

- The storm caused outages in water, power, communication, and transportation infrastructure. The outages had cascading impacts on community, emergency, and medical services. These impacts had not previously been envisioned or accounted for in planning.
- Mapping the power grid and identifying the most important natural gas infrastructure required for deliveries to gas-dependent generating facilities is key to determining which upstream assets should be winterized to prevent future occurrences.

Sources: City of Austin and Travis County*;* Congressional Research Service; Energy Research and Social Science Journal; Journal of Critical Infrastructure Policy; KXAN News; Natural Hazards Journal; University of Houston, Hobby School of Public Affairs

Case Study #3: Colonial Pipeline cyberattack

On May 7, 2021, Colonial Pipeline Company, the largest pipeline in the U.S. for transporting refined petroleum products, experienced a ransomware attack that prompted a pre-emptive shutdown of their roughly 5,500 miles of pipelines between Texas and New Jersey. This pipeline system controls nearly half of the gasoline, jet fuel, and diesel flowing along the East Coast. The attack began when a hacker group accessed the Colonial Pipeline network and stole 100 gigabytes of data. Following the data theft, the attackers infected the Colonial Pipeline IT network with ransomware that affected many administrative systems, including billing and accounting. The company subsequently shut down the pipeline to prevent the ransomware from spreading.

Source: Canary Media

Source: Colonial Pipeline/Wall Street Journal

Pipeline operations were offline for approximately five days, causing localized shortages of gasoline, diesel fuel, and jet fuel. Panic-buying by consumers depleted gasoline supplies at some service stations on the East Coast while also driving up retail gasoline prices. CISA identified cascading impacts across multiple infrastructure sectors including transportation and emergency services and noted that, if fuel supply issues continued, the impact would be increasingly felt by National Critical Functions that rely heavily on just-in-time supplies and workers that are unable to perform their duties remotely.

Lessons learned:

- The attack highlighted significant regional dependencies on a single critical infrastructure system, which if disrupted could have far reaching impacts including cascading and escalating failures of interconnected critical infrastructure systems.
- A cyberattack can lead to disruption in operations, even if the operating technology is not specifically targeted.
- Understanding fuel dependencies and the consequence of disruption is essential for effective policy making, continuity of operation planning, community resilience planning, and emergency management and response.

Source: U.S. Department of Homeland Security/CISA; Cyber Defense Review

Case Study #4: Global internet outage

On July 19, 2024, a faulty section of code in a software update from CrowdStrike caused PCs running Microsoft's Windows operating system to crash, affecting 8.5 million Microsoft Windows devices worldwide. Many of the impacted organizations had thousands of them spread around the world's servers, and many PCs needed to be fixed manually. What has been described as the largest IT outage in history created global financial losses estimated to be around $15 billion.

Disruptions were widespread, with cascading failures affecting multiple sectors. Thousands of commercial flights were grounded, critical hospital care was interrupted, financial institutions were unable to service clients, some 911 operators could not respond to emergencies, and international shipping was disrupted. Companies across various sectors faced immediate disruptions, with many unable to access critical services. This led to significant productivity losses, revenue declines, and operational challenges. Retailers, for example, struggled with online transactions, while healthcare providers faced delays in accessing patient records.

Texas experienced significant impacts, including cancelled elective procedures at Harris Health System; flight delays at major airports like George Bush Intercontinental Airport and Dallas Love Field; widespread closure of driver's license offices and other disruptions in government services; and issues with online banking and transactions.

Source: Atlanta Constitution-Journal

Lessons learned:

- Increased reliance on cyber-physical infrastructure systems demonstrates continued vulnerability to technological failures. Unlike physical infrastructures, which are tangible and visible, Digital Public Infrastructures (DPI) such as Microsoft Windows are ubiquitous but also largely invisible, posing a significant challenge when it comes to managing risks associated with them. The potential risks posed by DPI failures from software bugs or cybersecurity breaches can have widespread cascading effects across multiple infrastructure systems.
- The global tech outage demonstrates why organizations must have reliable and redundant methods to communicate both internally and externally during a crisis, and also need to reassess IT systems and business continuity plans to ensure resilience against similar future disruptions.

Sources: Cyber Defense Magazine, World Economic Forum

Author Biography:

Mark Scott is an independent consultant and risk management specialist with over 40 years working in the public, private, and nonprofit sectors, including 25 years in critical infrastructure protection.

Prior to establishing his consulting practice, Mark designed and led a program for the District of Columbia's Homeland Security and Emergency Management Agency to strengthen protection and resilience of critical infrastructure in the Nation's capital against all hazards. More recently he consulted on critical infrastructure protection practices for countries in Central Asia and the Western Balkans through the Organization for Security and Cooperation in Europe. Mark has also served as member and past Vice-Chair of the U.S. Department of Homeland Security's State, Local, Tribal, and Territorial Government Coordinating Council.

Mark has lived and worked in the Washington D.C. area since 2008, having previously resided in Charleston, West Virginia and Pittsburgh, Pennsylvania. He holds a master's degree in urban and regional planning from the University of Pittsburgh.

Disclosure: The author reports there are no competing interests to declare.

Appendix B: References

Ahmad, I., Clark, A., Ali, M., Hansheng, L., Ferris, D. & Aved, A. Determining critical nodes in optimal cost attacks on networked infrastructures. *Discover Internet of Things* (2024) 4:2. https://doi.org/10.1007/s43926-023-00054-1

Akbarzadeh, A. & Katsikas, S. Identifying and Analyzing Dependencies in and among Complex Cyber Physical Systems. *Sensors,* 2021, 21, 1685. https://doi.org/10.3390/s21051685

Al Musawi, A.F., Satyaki, R. & Preetam, G. Examining indicators of complex network vulnerability across diverse attack scenarios. *Nature Scientific Reports*, (2023) 13:18208. https://doi.org/10.1038/s41598-023-45218-9

Bakhtiari, S. *Multi-Hazard Risk Assessment of the Interconnected Infrastructure Systems (2024).* Electronic Thesis and Dissertation Repository. 10494. https://ir.lib.uwo.ca/etd/10494

Beyza, J., Garcia-Paricio, E. & Yusta, J. Applying Complex Network Theory to the Vulnerability Assessment of Interdependent Energy Infrastructures*. Energies,* 2019, 12(3), 421; https://doi.org/10.3390/en12030421

Bloomfield, R., Popov, P., Salako, K., Stankovic, V. & Wright, D. Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering and System Safety* 167 (2017) 198–217. http://dx.doi.org/10.1016/j.ress.2017.05.030

Cabrera, Derek and Laura Cabrera. *Network Theory*. Cabrera Research Lab, April 2020. https://blog.cabreraresearch.org/network-theory

Chachra, Deb. *How Infrastructure Works: Inside the Systems that Shape Our World.* New York: Riverhead Books, 2023.

Chester, Mikhail and Braden Allenby. *The Rightful Place of Science: Infrastructure in the Anthropocene.* Tempe, AZ: Consortium for Science, Policy & Outcomes, Arizona State University, 2021.

Chief Risk Officers (CRO) Forum. *Breaking Point: Critical Infrastructures Disrupted*. November 2023. https://www.thecroforum.org/wp-content/uploads/2023/11/Breaking-Point_Critical-Infrastructure-Disrupted.pdf

Dasuni, K. A. L., Palliyaguru, R., Amaratunga, D., & Liyanawatta, T. N. (2024). Redefining 'dependencies/interdependencies' of critical infrastructure: a systematic review of the existing knowledgebase. *Sustainable and Resilient Infrastructure*, *10*(2), 202–222. https://doi.org/10.1080/23789689.2024.2403885

Davletshin, Marat. 7 Ways Network Theory Is Reshaping Supply Chains. University of Arkansas, Sam M. Walton School of Business, February 2020. https://walton.uark.edu/insights/network-theory.php

Devineni, P., Kay, B., Lu, H., Tabassum, A., Chintavali, S. & Lee, S. Toward Quantifying Vulnerabilities in Critical Infrastructure Systems. U.S. Department of Energy/Office of Scientific and Technical Information, 2020. https://www.osti.gov/servlets/purl/1779137

DiPietro, A., Calabrese, A., De Nicola, A., Ferneti, D., Franchina, L., Martì, J. & Ruocco, T. An Open-Data-Based Methodology for the Creation of a Graph of Critical Infrastructure Dependencies at an Urban Scale. *IntechOpen*, November 2023. https://www.intechopen.com/chapters/88622

Dunn, S., Fu, G., Wilkinson, S. & Dawson, R. Network Theory for Infrastructure Systems Modelling: Proceedings of the Institute of Civil Engineers: *Engineering Sustainability*, October 2013. https://www.icevirtuallibrary.com/doi/abs/10.1680/ensu.12.00039?journalCode=jensu

Dunn, S. & Holmes, M. Development of a hierarchical approach to analyse interdependent infrastructure system failures. *Reliability Engineering and System Safety*, 191 (2019) 106530. https://doi.org/10.1016/j.ress.2019.106530

Elkady, S., Hernantes, J. & Labaka, L. Decision-making for community resilience: A review of decision support systems and their applications. *Heliyon*, 10 (2024) e33116. https://doi.org/10.1016/j.heliyon.2024.e33116

Ferrario, E. & Zio, E. Resilience analysis framework for interconnected critical infrastructures. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B Mechanical Engineering.* January 2017. http://doi.org/10.1115/1.4035728

Gong, S., Ye, Y., Gao, X., Chen, L. & Wang, T. Empirical patterns of interdependencies among critical infrastructures in cascading disasters: Evidence from a comprehensive multi-case analysis. *International Journal of Disaster Risk Reduction*. 95 (2023) 103862. https://doi.org/10.1016/j.ijdrr.2023.103862

Grofe, C. A review of the foundations of systems, infrastructure and governance. *Safety Science* 160 (2023) 106060. https://doi.org/10.1016/j.ssci.2023.106060

Gupta, H. Strengthening the Backbone: Using Network Theory to Enhance Critical Infrastructure Resilience. University of Oklahoma, Industrial & Systems Engineering. April 10, 2023. https://www.linkedin.com/pulse/strengthening-backbone-using-network-theory-enhance-critical-gupta/

Hackl, J. Network Analysis of Systems of Systems Models for Complex Infrastructure Systems. *14th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP14*, Dublin, Ireland, July 9-13, 2023. https://cis.princeton.edu/sites/g/files/toruqf5856/files/documents/Hackl2023.pdf

Hajializadeha, D. & Imani, M. RV-DSS: Towards a resilience and vulnerability- informed decision support system framework for interdependent infrastructure systems. *Journal of Computers & Industrial Engineering*, Vol 156, June 2021, 107276. https://doi.org/10.1016/j.cie.2021.107276

Hruska, R., McGillivary, K. & Edsall, R. *A Functional All-Hazard Approach to Critical Infrastructure Dependency Analysis.* Idaho National Laboratory, February 2022. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_53240.pdf

Imani, M. & Hajializadeh, D. A resilience assessment framework for critical infrastructure networks' interdependencies. *Water Science & Technology*, 81.7 (2020). http://iwaponline.com/wst/article-pdf/81/7/1420/707279/wst081071420.pdf

Kane, B., Webber, S., Tucker, K., Wallace, S., Chang, J., McCarthy, D., Murphy, D., Egel, D. & Wingfield, T. *Defending the United States Against Critical Infrastructure Attacks: Exploring a Hypothetical Campaign of Cascading Impacts*. RAND, June 2024. https://www.rand.org/pubs/research_reports/RRA2397-3.html

Kizhakkedath, A. & Kai, T. Vulnerability analysis of critical infrastructure network. *International Journal of Critical Infrastructure Protection,* Volume 35, December 2021, 100472. https://doi.org/10.1016/j.ijcip.2021.100472

Kong, J., Simonovic, S. & Zhang, C. Resilience Assessment of Interdependent Infrastructure Systems: A Case Study Based on Different Response Strategies. *Sustainability* 2019, 11, 6552. http://doi.org/10.3390/su11236552

Lewis, L. & Petit, F. *Critical Infrastructure Interdependency Analysis: Operationalising Resilience Strategies.* Argonne National Laboratory, 2019. https://www.unisdr.org/files/66506_f415finallewisandpetitcriticalinfra.pdf

Li, N., Wang F., Magoua, J. & Fang, D. Interdependent effects of critical infrastructure systems under different types of disruptions. *International Journal of Disaster Risk Reduction*. Volume 81, 15 October 2022, 103266. https://doi.org/10.1016/j.ijdrr.2022.103266

Macaulay, T. *The Danger of Critical Infrastructure Interdependency.* Centre for International Governance Innovation (n.d.) https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency

McAllister, T. *Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume II, Special Publication (NIST SP).* National Institute of Standards and Technology, Gaithersburg, MD. (2015). https://doi.org/10.6028/NIST.SP.1190v2

Milanovic, J. & Zhu, W. Modelling of Interconnected Critical Infrastructure Systems Using Complex Network Theory. *IEEE Transactions on the Smart Grid*, vol. 9, no. 5, pp. 4637-4648, Sept. 2018. https://doi.org/10.1109/TSG.2017.2665646

National Academies of Sciences, Engineering, and Medicine. *Electricity System Operability and Reliability Under Increasing Complexity: Proceedings of a Workshop 2025*. Washington, DC: The National Academies Press. https://doi.org/10.17226/28541

National Association of State Energy Officials (NASEO). *Electricity-Water Critical Infrastructure Interdependencies: How States Can Enhance Resilience and Reduce Risks.* NASEO, December 2021. https://naseo.org/data/sites/1/documents/publications/NASEO%20Electricity-Water%20Critical%20Infrastructure%20Interdependencies%20December%202021%20FINAL.pdf

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J. & Peerenboom, J. *Analysis of Critical Infrastructure Dependencies and Interdependencies.* Argonne National Laboratory, ANL/GSS 15/4, June 2015. https://publications.anl.gov/anlpubs/2015/06/111906.pdf

Petit, F., Verner, D. & Levy, L-A. *Regional Resilience Assessment Program Dependency Analysis Framework*. Argonne National Laboratory, ANL/GSS 17/05, August 2017. https://publications.anl.gov/anlpubs/2018/04/137844.pdf

Pozo, A., Priesmeier, P., & Fekete, A. Measuring spatial accessibility to critical infrastructure: The Access Road Identification model. *International Journal of Critical Infrastructure Protection.* 49 (2025) 100760. https://doi.org/10.1016/j.ijcip.2025.100760

Prier, S., Strong, A. & Welburn, J. *Interdependence Across the National Critical Functions*. RAND, WR-A210-1 January 2023. https://www.rand.org/pubs/working_papers/WRA210-1.html#:~:text=The%20interdependence%20of%20NCFs%2C%20driven,to%20the%20risk%20analysis%20community

Rathnayaka, B., Robert, D., Adikariwattage, V., Siriwardana, C., Kuligowski, E., Setunge, S. & Amaratunga, D. Novel methodology for resilience assessment of critical infrastructure considering the interdependencies: A case study in water, transportation and electricity sector. *International Journal of Disaster Risk Reduction.* 19 (2025) 105271. https://doi.org/10.1016/j.ijdrr.2025.105271

Rinaldi, S., Peerenboom, J. & Kelly, T. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, Vol. 21, No. 6, pp. 11–25. (2001). https://doi.org/10.1109/37.969131

Sarkissian, R., Cariolet, J-M., Diab, Y. & Vuillet, M. Investigating the Importance of Critical Infrastructures' Interdependencies during Recovery; lessons from Hurricane Irma in Saint-Martin's Island. *International Journal of Disaster Risk Reduction*, Volume 67, January 2022, 102675. https://doi.org/10.1016/j.ijdrr.2021.102675

Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M. & Navaratnam, S. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures* 2022, 7, 67. https://doi.org/10.3390/infrastructures7050067

Schneider, M., Halekotte, L., Mentges, A. & Fiedrich, F. Dependent Infrastructure Service Disruption Mapping (DISruptionMap): A method to assess cascading service disruptions in disaster scenarios. *Sci Rep* **15**, 5736 (2025). https://doi.org/10.1038/s41598-025-89469-0

Schweikert, A., L'Her, G. & Deinert, M. Simple method for identifying interdependencies in service delivery in critical infrastructure networks. *Applied Network Science* (2021) 6:44. https://doi.org/10.1007/s41109-021-00385-4

Setola, R. Interdependencies and supply chain. *International Journal of Critical Infrastructure Protection.* 49 (2025) 100774. https://doi.org/10.1016/S1874-5482(25)00035-6

Setola, R. Interdependencies and third parties. *International Journal of Critical Infrastructure Protection.* 40 (2025) 100750. https://doi.org/10.1016/S1874-5482(25)00011-3

Setola, R., Rosato, V., Kyriakides, E. & Rome, E. (eds). Managing the Complexity of Critical Infrastructures. *Studies in Systems, Decision and Control*, vol 90. Springer, Cham. 2017. https://doi.org/10.1007/978-3-319-51043-9_2

Shapiro, D. *Networks are Everywhere: Understanding Systems Thinking*. Medium.com, September 8, 2023. https://medium.com/@dave-shap/networks-are-everywhere-understanding-systems-thinking-7ff37ebcf8c9

Skarvelis-Kazakos, S., Kiss, I., & Panteli, M. (2025). *Advanced resilience metrics for electricity networks adjacent to telecommunications networks, based on graph theory (Version 1).* University of Sussex. https://hdl.handle.net/10779/uos.28207988.v1

Sonesson, T., Johansson, J. & Cedergren, A. Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety Science* 142 (2021) 105383. https://doi.org/10.1016/j.ssci.2021.105383

Spizzirri, J. *Advanced tools reveal critical infrastructure connections and help mitigate disasters***.** Argonne National Laboratory, January 2021. https://www.anl.gov/article/advanced-tools-reveal-critical-infrastructure-connections-and-help-mitigate-disasters

Stergiopoulos, G., P. Theocharidou, M., Lykou, G. & Gritzalis, D. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *International Journal of Critical Infrastructure Protection* 12 (2016) 46-60. https://doi.org/10.1016/j.ijcip.2015.12.00

Sun, W., Bocchini, P. & Davison, B. Overview of Interdependency Models of Critical Infrastructure for Resilience Assessment. *Natural Hazards Review,* Vol 23, No 1, November 2021. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000535

Valinejad, J. & Mili, L. Cyber–Physical–Social Model of Community Resilience by Considering Critical Infrastructure Interdependencies. *IEEE Internet of Things Journal*, Vol. 10, No. 19, October 2023. https://doi.org/10.1109/JIOT.2023.3277450

Weber, V., Riera, M. & Laumann, E. *Mapping the World's Critical Infrastructure Sectors: DGAP Policy Brief 35 (2023)*. German Council on Foreign Relations. November 2023. https://doi.org/10.60823/DGAP-23-39548-en

Wells, E., Boden, M., Tseytlin,I. & Linkov, I. Modeling critical infrastructure resilience under compounding threats. *Progress in Disaster Science* 15 (2022) 100244. https://doi.org/10.1016/j.pdisas.2022.100244

Xie, B., Tian, X., Kong, L. & Chen, W. The Vulnerability of the Power Grid Structure: A System Analysis Based on Complex Network Theory. *Sensors* 2021, 21, 7097. https://doi.org/10.3390/s21217097

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Scott, M. (2025). Understanding Critical Infrastructure as Systems and Networks (Institute for Homeland Security Report No. 2025-1021). Institute for Homeland Security.

https://doi.org/10.17605/OSF.IO/G983Y