Multi-Domain Locational Risk Models for Critical Infrastructure: Influence via Real Estate Transactions

Christopher Dietz, Hayden Town,
Gabriel A. Weaver, Mary Klett, Robert Edsall
Infrastructure Resilience and Security
Idaho National Laboratory
Idaho Falls, USA

***Abstract*— Critical infrastructure owners and operators face a myriad of threats posed by sabotage, cyber intrusion, and supply chain disruptions. *Locational risk*---the role of proximity on the ability to implement adversarial tactics---is an increasingly important aspect of risk for the Energy Sector to assess. Real Estate ownership and associated property rights can support adversarial interests with multiple, legal avenues to access, develop, control, or monitor critical infrastructure. This paper provides three contributions to motivate a methodology to assess locational risk. First, this paper catalogs property rights and their potential for adversarial tactics as attested to by historical incidents and legislation. Second, we survey methods from spatial statistics and social network analysis to measure locational risk in geospatial and organizational domains. Finally, we present initial results of case studies in Texas and Hawaii to illustrate how organizational influence varies with geospatial extent.**

***Index Terms*—business organization, risk analysis, supply chain management, critical infrastructure, energy resources**

I. INTRODUCTION

Most of the critical infrastructure throughout the United States is privately owned, often with complex organizational structures for both the individual facilities and their parent companies. Although the security and resilience of critical infrastructure traditionally focused on physical, cyber, and supply chain considerations, *organizational risk* represents a vital, additional element to consider for infrastructure security. Organizational risk encompasses the potential threats and vulnerabilities from ownership interests, business affiliations, and relationships – both direct and indirect – that can influence and impact infrastructure operations. This includes how entities can exert control or leverage over critical assets, such as electric utility transmission and distribution infrastructure, affecting functionality, maintenance, and operational integrity.

Real estate represents a unique space for organizational risk to occur, tying organizational and social structures to tangible assets. Although important, the implications of real estate ownership and associated property rights on critical infrastructure security remain largely unexplored. Parties holding legal interests in land can use those rights in ways that present unanticipated risks to critical infrastructure. Beyond outright ownership, property interests such as commercial leases, mineral rights, easements, and rights-of-way serve as legal avenues for adversarial entities to obtain use and/or control over land. Land may be co-located with, or nearby, critical infrastructure. Foreign investment in agricultural land near U.S. military installations, for example, has become a well-known national security concern, at least partly due to the implicit threats it can pose to critical infrastructure [1].

The complexity of real estate interests can drastically compound risk to critical infrastructure facilities. Avenues of influence include the ownership of the property on which the infrastructure resides, adjacent properties, mineral rights, easements, rights-of-way, and potentially other types of interests that intersect with the infrastructure property. Each additional layer of ownership, control, and/or influence adds to the intricacy, greatly increasing the challenges in managing and securing critical infrastructure. As mentioned earlier, such issues have garnered national attention in recent years, including a landmark incident in North Dakota that resulted in sweeping legislation at the federal level to safeguard military installations from real estate developments and transactions within close proximity to certain military assets.

This paper provides three main contributions to develop a methodology to measure locational risk, risk faced by critical infrastructure assets due to their position. Although potentially applicable to a variety of domains, Section II illustrates how historical incidents and existing legislation attest to unexpected, adversarial use of property rights granted through ownership. Section III briefly surveys methods from spatial statistics and social network analysis to understand specific adversarial tactics enabled through position, as expressed in the geospatial and organizational domains. Finally, Section IV applies some of the surveyed methods from spatial statistics and social network analysis to demonstrate how organizational influence varies with geospatial extent.

Research was sponsored by the Energy Cyber Sense (ECS) program and was accomplished under the direction of Stephanie H. Johnson, Ph.D. and Jennifer Cooke, Program Lead for Supply Chain Cybersecurity at the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

979-8-3315-8138-1

II. Historical Incidents

Recent incidents demonstrate the need to characterize property rights obtained via real-estate transactions through the lens of critical infrastructure protection. Real estate ownership can directly influence critical infrastructure at the time of development and beyond. The U.S. Department of Agriculture (USDA)'s data on foreign investment in domestic agricultural land suggest that critical infrastructure development motivated many acquisitions. In fact, 88.5% of cropland and 84.1% of pastureland acreage acquisitions in 2020 were done by entities with 'solar' or 'wind' in their registered names. It is noteworthy that 54% of foreign holdings are for types of interest other than direct ownership, such as long-term leases [1]. This helps to underscore the need to consider a broad range of property rights. We now consider various property rights and how they have historically introduced risks of adversarial behavior worthy of mitigation by the Committee of Foreign Investment in the United States (CFIUS).

A. Geospatial Domain

Owning land close to where infrastructure is being developed can provide the landowner with persistent, physical access to sites nearby critical facilities. For example, a subsidiary of a Foreign Entity of Concern (FEOC) recently purchased land in New Hampshire at a price quadruple its market value. The property was within 10 miles of a Space Force Station and within 50 miles of other critical water and transportation infrastructure [2]. Such access, reported in 2025 by a U.S. Congressperson to the U.S. Department of the Treasury, demonstrates the acknowledged potential for adversarial persistence enabled through ownership rights such as physical access.

Real estate ownership can also impact the security of critical infrastructure, even when the owned property is miles away, by enabling data collection and monitoring. In 2024, a U.S. senator from Texas furnished a letter of concern to the U.S. Department of Defense after reports surfaced that a FEOC had purchased over 15,000 acres within 40 miles of Laughlin Airforce base in Val Verde County, Texas. Specifically, congress members cited concerns that the planned, 700-foot tall wind turbines, could be used to conduct surveillance on base operations or potentially interfere with the state's electric grid [4]. Another incident occurred in 2023 when the U.S. Airforce raised concerns over a FEOC purchasing 300 acres for a proposed cornmill less than 13 miles from Grand Forks Air Force Base (GFAFB) in North Dakota. As a result, the U.S. Department of Treasury revised CFIUS' jurisdiction from within a 1-mile radius of a sensitive facility, to a 99-mile radius.

Rights-of-way (ROW) and easements can also create critical infrastructure risk by giving private parties a legally enforceable chokepoint to pause development through litigation. In ETC Tiger Pipeline LLC v. DT Midstream, a dispute that began in Fall 2022, stopped DT Midstream's proposed pipeline crossing until the Louisiana Second Circuit reversed it in Spring 2024, a roughly 1.5-year delay [8]. A law firm analysis notes that "exclusive" ROW/easement language can become high-impact control points, reinforcing that corridor rights--even seen as routine real estate related instruments--can be leveraged to delay or constrain energy infrastructure buildouts [12].

These historical incidents illustrate the potential for *dual-use property rights* in which a land owner can pursue infrastructure development, or other legitimate uses, but with an optional platform for adversarial behavior. Methods to assess locational risk are necessary to balance between international investment and partnerships to encourage economic prosperity and long-term critical infrastructure protection. This need is underscored by a broader pattern highlighted by the USDA's data. From 2013 to 2023, foreign ownership in U.S. cropland increased by 146%, from roughly 5.4 million to 13.2 million acres; pastureland increased by 32%, from approximately 5.8 million to nearly 7.7 million acres [3]. The changes in cropland and pasture are largely due to foreign-owned wind companies signing and terminating long-term leases on large acreages.

B. Organizational Domain

Critical infrastructure facilities also face locational risk in the organizational domain. Throughout their lifecycle, infrastructure systems depend upon business relationships in order to function. While supply chain risk management recognizes the network of supplier relationships upon which an infrastructure site may depend, the function of critical infrastructure systems depends upon a broader range of business relationships such as parent companies, beneficial ownership, investors, and board membership. As with real-estate transactions and property rights, business relationships and their associated operational and information rights provide a legal, long-term potential for adversarial tactics.

TABLE I. Locational Risks to Critical Infrastructure via Tactics in Organizational and Geospatial Domains

Adversarial Tactic	**Domain**	**Property Rights or Business Transaction**	**Known Incidents**	**Analytic Methods**
Persistence	Geospatial	Physical Access	Nashua, NH, 2025 [2]	Neighborhood Analysis
	Organizational	Maintenance and Operations	Sandia report on DER, 2017 [3]	Graph Neighborhood Analysis
Data Collection	Geospatial	Improve/develop;attach structures	Laughlin AFB, 2022 [4]	Location Quotient [5]
	Organizational	Investment	ODNI Report, 2022 [6]	Centrality Measures for Corporate Interlock [7]
Impact: Denial of Control	Geospatial	Easement/ROW rights	ETC Tiger Pipeline LLC v. DT Midstream, 2022 [8]	Location Quotient, Getis-Ord Gi* [9]
Impact: Loss of Control	Geospatial	Surface-use rights (mineral)	Texas Supreme Court, Getty Oil Co. v. Jones, 1971	Neighborhood Analysis
	Organizational	Merger and Acquisition	Minnesota Power, 2025 [10]	Centrality Measures [11], Temporal network Analysis

Third-party maintenance and operations contracts provide Original Equipment Manufacturers (OEMs) with legitimate, persistent access to critical infrastructure facilities. For example, many Distributed Energy Resource (DER) systems have a design-level dependency on telemetry and monitoring services that suppliers can naturally provide following an installation. Moreover, a 2017 report from Sandia noted that "remote access to DER equipment from foreign companies is permitted" [3]. As such, third-party maintenance contracts between OEMs and asset owners can impact a facility's attack surface exposure [13].

Information rights gained by investors in emerging technology companies also provide a legal, long-term mechanism for persistence and data collection, with the potential for control. As noted in a report by the U.S. National Counterintelligence and Security Center (NCSC), investment in early-stage emerging technology companies provides the ability to "insert board members, secure voting rights, and/or access sensitive corporate data" [6]. As a result, domestic economic prosperity enabled by emerging technologies may inadvertently align with long-term adversarial objectives via FEOC.

Finally, mergers and acquisitions of companies in the critical infrastructure business ecosystem have the potential to consolidate control over regional operations while excluding competition. For example, the Canada Pension Plan Investment Board and Global Infrastructure Partners, a subsidiary of Blackrock, recently purchased the parent company of Minnesota Power, the second largest utility in the state. On the one hand, ownership by an equity firm in general means that profit, not necessarily grid reliability are top business drivers, though regulatory reliability requirements still apply [10]. On the other hand, private companies are renowned for efficiencies that often elude the public sector.

III. METHODS

Recent incidents from around the United States underscore the need for a methodology by which locational risk can be assessed. Therefore, this section surveys a handful of methods to measure locational risk within the geospatial and organizational domains. In addition, we discuss criteria by which such methods might be evaluated in the future.

A. Geospatial

In geographic terms, a critical infrastructure facility of concern and the parcels of land that are part of the real-estate transactions are polygons. The field of spatial statistics has provided several methods and indices that allow quantification of locational risk.

1) Neighborhood Analysis Metrics

Various neighborhood analysis metrics allow one to examine trends and correlations based on some reference distances. This approach is consistent with previously-mentioned policies that define the jurisdiction of CFIUS based on distance bands from a facility of interest (e.g. 1 mile, 10 miles, 99 miles). In this approach, various distances loosely align with adversarial tactics with data collection and monitoring possible from remote locations and constraining access from closer locations. One potential measure of a neighborhood-based risk measure is the *gravitational index*, which models the decrease of risk as one moves away from a sensitive facility analogous to the decay in gravitational pull as one moves away from a celestial body [14].

Spatial patterns may appear random or clustered at one scale, but dispersed at a different scale. Statistics such as the nearest neighbor index (NNI) allow examination of these variations by adjustment of the *kernel*, the area used to aggregate values to create the NNI. Such approaches allow adjustment of the spatial statistic based on the presumed threat and its scale.

2) Methods for Concentration of Ownership

Methods to measure concentrations of ownership nearby critical infrastructure facilities enable analysts to identify regional data collection risks. For example the *location quotient (LQ)*, helps an analyst to determine whether the number (or acreage) of foreign-influenced parcels in a region (e.g. a county containing a critical facility) is disproportionate relative to the rest of the county, state, or other region. The location quotient simply compares the proportion of the quantity under study in a region with the proportion of the quantity at a larger scale [5].

Analysts may want to identify 'hot spots' where there is a relatively high intensity of an activity versus that which would be attributed to a random distribution. The *Getis-Ord Gi** method examines whether a polygon has a high value of some quantity and is also surrounded by (or nearby to) other polygons with relatively high quantities (thus creating a hot spot) [9].

Finally, temporal considerations are important as well; a recent increase in a certain activity (such as purchase of property by a foreign-controlled investor) in a region can be flagged as significant: the Mann-Kendall trend test can be performed with the Getis-Ord Gi* (or other purely spatial statistic) to examine the sequence of clustering in the time dimension.

B. Organizational

Locational risk of a critical infrastructure facility, expressed in the organizational domain, is determined by the business relationships upon which that facility depends, throughout its lifecycle. Given an organizational network that relates critical infrastructure assets to its owners, operators, parent companies, third-party suppliers, investors and board members (to name a few), we consider several methods from the field of social network analysis with specific applications to fraud detection and white-collar crime.

1) Neighborhood Analysis Metrics

Social network analysis, as with the geospatial domain, allows one to consider organizations and people that are *close* to an organization of interest (e.g. asset owner and operator). In contrast to the geospatial domain, in which neighborhood analysis is based on geographic distance, such analysis is based on topological distance (e.g. the number of edges between two vertices). Specifically, the *graph neighborhood* of a vertex v is the set of all vertices that are adjacent to that vertex via an edge. In general, the i^{th} *neighborhood* of a

vertex *v*, is the set of all vertices for which a path of length *i* to/from *v* exists. An open research question is whether there is a maximum path length at which certain types of adversarial tactics cease to have impact on critical infrastructure owners and operators.

2) Centrality Measures

Centrality measures have been used in applications of social network analysis to organized crime. Specifically Bichler et al. studied corporate interlock by constructing affiliation networks of people and organizations to understand informal social circles that span multiple organiztaions. By applying betweenness centrality, the authors were able to identify information brokers within such networks [7]. Similarly, other research has applied closeness centrality in order to identify actors that are important to quickly spread or transfer resources and which, if removed, would destabilize the network [15].

IV. Case Study

This section presents initial results of a case study to demonstrate methods to evaluate locational risk to generation plants in Houston County, Texas and BESS in Hawaii. Our intent is to use some of the previously-described methods to explore how organizational influence over regional critical infrastructure facilities vary with geospatial extent. Data sources employed include information about generation assets reported via the Energy Information Administration (EIA) 860 form, real-estate parcel ownership information from the Texas Geographic Information Office (TXGIO), and information on upstream owners from OpenCorporates.

A. Owners and Operator Profile

First, we construct a baseline organizational profile for generation owners and operators within Houston County, Texas. Houston County has 42 generation plants with a total nameplate capacity of 3807 MW. These plants are owned and operated by 21 and 23 entities respectively with 17 of these entities serving as both owner and operator. Figure Fig. **1** illustrates owners and operators with more than 100 MW aggregate capacity in the region.

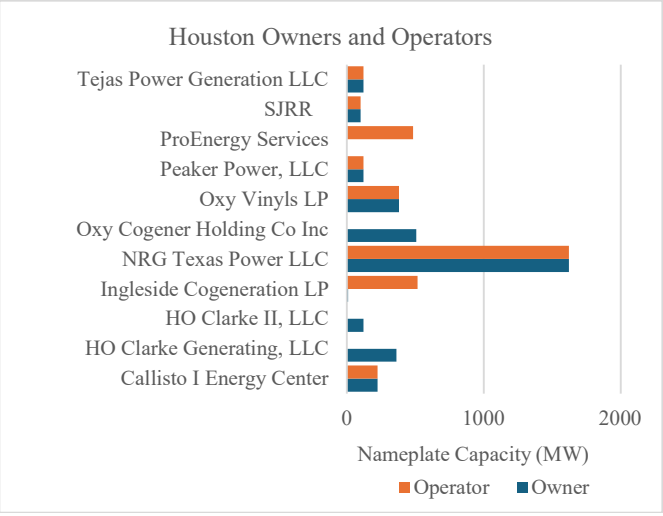

Fig. 1 Aggregate nameplate capacity of generators owned and operated within Houston County.

B. Neighborhood Analysis of Parcel Owners

Motivated by historical events surrounding real-estate acquisitions nearby sensitive facilities, we employ neighborhood analysis to examine trends in real-estate parcel ownership based on distance bands from these generation facilities. Table II illustrates the number of parcel owners within various distance bands (in miles) of generation plants.

TABLE II. Number of Parcel Owners By Generation Plants

0	1	5	10	25	50
33	54	112	149	209	311

Figure 2 illustrates *consolidation of influence through the geospatial domain* by Centerpoint Energy; we note that companies that accumulate a larger percentage of regional aggregate nameplate capacity, at lower distance thresholds, indicate geospatial consolidation. As a result, Centerpoint Energy has the ability to data collection and monitoring on or even deny access, given that they own land within 5 miles of generation sites with over 50% of county-wide nameplate capacity and within 10 miles of 57% of that capacity. Centerpoint is a Transmission and Distribution System owner.

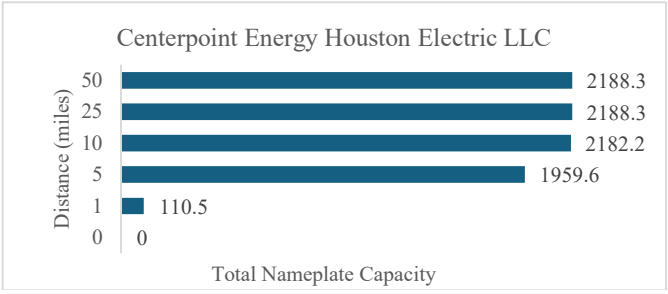

Fig. 2: Aggregate nameplate capacity within varying distance bands of real-estate parcels owned by Centerpoint Energy.

C. Neighborhood Analysis of Asset Owners

Given a list of owners/operators, we can construct an ASTN to consider consolidation of influence across real-estate parcel owners, as well as asset owners and operators. Figure 3 illustrates the ability to use betweenness centrality as a measure of *regional consolidation of influence through upstream ownership*. The 1-neighborhood of BESS (purple vertices) shows utilities and owners via green and light-blue edges respectively. Two and three-neighborhoods of BESS show parent companies and ultimate beneficial owners, indicated by darker blue edges.

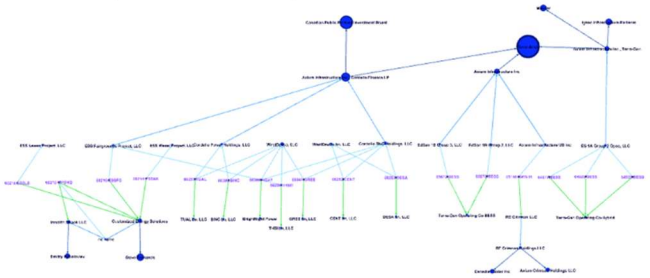

Fig. 3 Illustration of consolidation of influence via ultimate beneficial ownership for some BESS in Hawaii. Node size reflects entities with a high degree of influence, as measured by betweenness centrality.

V. Related Work

This paper motivates organizational influence enabled through locational risk as a vital element to consider for critical infrastructure protection. Our paper's first contribution describes how a wide variety of real-estate transactions, define a rich problem space in which to consider threat models for locational risk. Methods to quantify locational risk in the geospatial domain build upon spatial proximity analysis [16].

Previous work by Ouyang considers spatially-localized disruptions and models their impact on flows through regional electrical power and gas infrastructure [17]. More generally, the literature for interconnected critical infrastructures (ICI) and critical infrastructure resilience provide further context for network and grid-based representations of critical infrastructure and potential cascading disruptions. Grid-based approaches, such as that used by the HARmonized grids of Critical Infrastructures in Europe (HARCI-EU), can be used to identify regions where multiple infrastructure assets are concentrated [18]. Rinaldi et al. noted the need to consider a wide variety of dependencies, including geospatial, cyber, and others, early on in the infrastructure dependency research [19].

Spatial social network analysis (SSNA) is an emerging area of research that considers interpersonal and interorganizational relationships within a defined geographic region [20]. Our research considers such methods, but applies them to emergent threat models for critical infrastructure systems. and organizational influence. Multilayer networks point to the potential for using a network-based formalism to model cascading disruptions across layers of infrastructure systems. As mentioned earlier, multi-layered approaches to risk assessment may offset limitations of single-layer and aggregate models [21].

VI. Conclusion

Locational risk--the role of position on the ability to implement adversarial tactics--is an increasingly relevant aspect of risk for critical energy infrastructure protection. Property rights, enabled through real-estate transactions and business relationships in general provide mechanisms by which adversaries can express tactics that include loss of control, data collection, and persistence. This paper seeks to motivate and describe initial results to develop a rigorous methodology to assess locational risk within a geospatial region of interest. In so doing, we hope to provide a more holistic approach to evaluate multi-domain risks to regional critical infrastructure assets.

References

[1] K. M. Gianopoulos, Steve, "Foreign Investments in U.S. Agricultural Land," U.S. Government Accountability Office (GAO), January 18, 2024 2024. [Online]. Available: https://www.gao.gov/products/gao-24-106337

[2] M. Goodlander, "Letter to Treasury Secretary Scott Bessent re: CFIUS Nashua review," August 5, 2025. [Online]. Available: https://goodlander.house.gov/wp-content/uploads/2025/08/2025-0805-Rep.-Goodlander-Letter-to-Treasury-Secretary-Re-CFIUS-Nashua-Review-.pdf

[3] J. T. Johnson, "Roadmap for photovoltaic cyber security," Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), 2017.

[4] J. Cornyn "Termination or Suspension of Mitigation Agreement for Blue Hills Wind Project," July 10, 2024. [Online]. Available: https://www.cornyn.senate.gov/wp-content/uploads/2024/07/Letter-re-Blue-Hills-Wind-Project.pdf?utm_source=chatgpt.com

[5] M. M. Miller, L. J. Gibson, and N. G. Wright, "Location quotient: A basic tool for economic development analysis," *Economic development review,* vol. 9, no. 2, p. 65, 1991.

[6] "When the Invisible Hand turns into a Sleight of Hand: Understanding How Venture Capital is used to Create Vulnerabilities in the Supply Chain," National Counterintelligence and Security Center, 2020. Accessed: March 1, 2026. [Online]. Available: https://www.odni.gov/files/NCSC/documents/supplychain/Final%20VC.pdf

[7] G. Bichler, A. Schoepfer, and S. Bush, "White collars and black ties: Interlocking social circles of elite corporate offenders," *Journal of Contemporary Criminal Justice,* vol. 31, no. 3, pp. 279-296, 2015.

[8] "ETC Tiger Pipeline, LLC v DT Midstream, Inc. and DTM Louisiana Gathering LLC," ed: LA Ct. App., 2nd Circuit, 2024.

[9] J. K. Ord and A. Getis, "Local spatial autocorrelation statistics: distributional issues and an application," *Geographical analysis,* vol. 27, no. 4, pp. 286-306, 1995.

[10] J. Tomich, "Minnesota greens split over BlackRock's planned $6.2B utility buyout," *E&E News*, August 12, 2025. [Online]. Available: https://www.eenews.net/articles/minnesota-greens-split-over-blackrocks-planned-6-2b-utility-buyout/

[11] A. Landherr, B. Friedl, and J. Heidemann, "A critical review of centrality measures in social networks," *Business & Information Systems Engineering,* vol. 2, no. 6, pp. 371-385, 2010.

[12] A. D. Carna, Mitchell; Gann, Andrew; Indest Miles, "Louisiana Case Clarifies That Some "Exclusive" Pipeline Servitudes May Not Be All That Exclusive," April 17, 2024. [Online]. Available: https://www.mcguirewoods.com/client-resources/alerts/2024/4/louisiana-case-clarifies-that-some-exclusive-pipeline-servitudes-may-not-be-all-that-exclusive/?utm_source=chatgpt.com

[13] G. Weaver, M. Culler, and E. M. Stewart, "Organizational Influence on Supply Chain for Digital Energy Infrastructure: Business Models, and Policy Landscape," in *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 2024: IEEE, pp. 524-530.

[14] F. D. Stacey, "Gravity," *Science Progress (1933-),* pp. 1-17, 1984.

[15] R. C. Van der Hulst, "Introduction to Social Network Analysis (SNA) as an investigative tool," *Trends in Organized Crime,* vol. 12, no. 2, pp. 101-121, 2009.

[16] J. Brennan and E. Martin, "Spatial proximity is more than just a distance measure," *International journal of human-computer studies,* vol. 70, no. 1, pp. 88-106, 2012.

[17] M. Ouyang, "Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks," *Reliability Engineering & System Safety,* vol. 154, pp. 106-116, 2016.

[18] F. Batista e Silva, G. Forzieri, M. A. Marin Herrera, A. Bianchi, C. Lavalle, and L. Feyen, "HARCI-EU, a harmonized gridded dataset of critical infrastructures in Europe for large-scale risk assessments," *Scientific data,* vol. 6, no. 1, p. 126, 2019.

[19] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE control systems magazine,* vol. 21, no. 6, pp. 11-25, 2001.

[20] S. Jin, A. Endert, and C. Andris, "SNoMaN: a visual analytic tool for spatial social network mapping and analysis," *Cartography and Geographic Information Science,* vol. 52, no. 4, pp. 441-459, 2025.

[21] S. Poledna, J. L. Molina-Borboa, S. Martínez-Jaramillo, M. Van Der Leij, and S. Thurner, "The multi-layer network nature of systemic risk and its implications for the costs of financial crises," *Journal of Financial Stability,* vol. 20, pp. 70-81, 2015.