DISPATCHES 002 / POWER + INFRASTRUCTURE

The Systems Beneath the System

Power, Infrastructure, and Hidden Dependencies

August 25, 2026

Classification: Open Intelligence

khaosholdings.com\ siobhan@khaospartners.com

KHAOS HOLDINGS

Contents

1. Executive Summary

Modern civilization rests on a fragile and interwoven network of lifeline services—electricity, water, transportation, communications, healthcare, finance, and food supply. These critical infrastructures are not isolated silos but elements in a living, breathing, and highly dynamic system. Each service depends on others to function, often in hidden, nonlinear, and deeply complex ways. The more connected our world becomes, the more this interconnectedness becomes both a source of strength and a potential point of failure.

The next competitive advantage will belong to institutions that can see hidden physical, digital, financial, regulatory, and human dependencies before they become points of failure. The operational reality is clear: dependency chains create invisible failure points. Critical infrastructure behaves as a complex system, defined by networks of dependencies, feedback loops, and emergent behaviors. On the surface, the dependencies seem obvious: hospitals need electricity, telecommunications need the power grid, and water utilities require both power and data to operate. But deeper down, second-order and higher-order dependencies emerge—ones that even domain experts may not recognize until it's too late. For instance, a power outage in one region can cascade into a telecommunications failure, disabling remote control capabilities for other grids, leading to miscoordination in transportation or delayed emergency responses.

> **KEY ASSESSMENT:** The increasing interconnectedness of physical, digital, and financial infrastructure has created complex, hidden dependencies that pose systemic risks. Organizations that map and mitigate these vulnerabilities will gain a decisive competitive advantage, while those relying on traditional, siloed risk management face catastrophic, cascading failures during inevitable "poly-crises."

2. Current Landscape

2.1 Physical and Geographic Dependencies

Critical infrastructures are inherently complex systems because they integrate heterogeneous platforms, proprietary systems and protocols, and open communications networks. In addition, critical infrastructures are usually interconnected and interdependent with other critical infrastructures that belong to other sectors, such as energy, information and communications technology (ICT), and transportation. According to Rinaldi et al. [1], critical infrastructures may have physical, informational, and logical dependencies. Specifically, a failure in one infrastructure may affect the operation of other critical infrastructures as a result of their dependencies. In the case of a geographical dependency, seemingly independent critical infrastructures may be affected by a threat due to their physical proximity.

Furthermore, lifelines are critical infrastructure systems characterized by a high level of interdependency that can lead to cascading failures after any disaster [2]. The connections among different networks increase the probability of cascading failures and the risk of a tremendous amplification of the consequences. For this reason, it is essential to consider them in risk analysis and resilience assessment.

2.2 Digital and Informational Dependencies

The continued functioning of critical infrastructure is highly dependent on communication, which underpins everything from the logistics of order fulfillment to the financial transfers of funds and sharing of intellectual property. As a result, addressing threats to data exchanges between critical infrastructure sectors is important to their protection. Understanding the flows of data is a useful tool for identifying hidden risks. There are two basic varieties of threats to data flows: threats to availability affect whether the data can be accessed when it is needed; and threats to confidentiality and integrity concern data being disclosed or changed without the reliant party's knowledge or approval.

2.3 Financial and Supply Chain Dependencies

Business continuity often depends on more than the resilience of a company's own facilities. It also relies on suppliers, infrastructure, and logistics networks that keep supply chains moving. Yet many companies still assess physical risk too narrowly. An analysis of public corporate disclosures reveals that many business interruption exposures remain unmapped and potentially underestimated [3]. Just 7% of analysed companies

report extending physical risk assessments to their suppliers' facilities, and fewer than 2% disclose assessing the wider infrastructure they rely on. Within the analysed public corporate disclosures, this suggests a growing visibility gap in business continuity risk as climate risk, production concentration and interconnected infrastructure increase supply chain dependencies.

3. Exposure Matrix

Sector	Assessment of Own Facilities	Assessment of Supplier Facilities	Assessment of Infrastructure Dependencies	Key Vulnerabilities
Chemicals	86%	14%	<2%	Geographic concentration, hazardous material transport
Motor Vehicles	60%	19%	<2%	Just-in-time supply chains, microchip dependencies
Industrials	55%	16%	<2%	Energy intensive operations, raw material sourcing
Financials	30%	5%	<2%	Data availability, telecommunications networks
Healthcare	45%	10%	<2%	Power supply, specialized medical equipment

Table 1: Fortune 500 Europe physical risk disclosure by sector and assessment scope (estimated), along with key vulnerabilities.

4. Structural Failure or Governance Gap

4.1 The Anatomy of Cascading Failures

Disruptions or outages in critical infrastructures are usually categorized as cascading, escalating, or common-cause failures. A cascading failure occurs when an infrastructure A affects one or more components in another infrastructure B, which, in turn, leads to the partial or total unavailability of infrastructure B. An escalating failure occurs when a disruption in one infrastructure exacerbates an independent disruption in another infrastructure, usually by increasing the severity of the disruption and/or the time needed to recover from the second failure. A common-cause failure occurs when two or more infrastructures are disrupted at the same time; components within each infrastructure fail due to a common cause. This occurs when two infrastructures are co-located (geographic interdependency) or when the root cause of the failure is widespread (e.g., a natural or human-initiated disaster).

Cascading risk is the risk that one or more hazard event(s) may precipitate subsequent risks and events [4]. Cascading events occur when hazards or failures trigger chains of interrelated hazards or impacts. Essentially, cascading risk is the probability of a chain reaction resulting from a hazard or failure which triggers interconnected impacts that may escalate across systems and sectors. Cascading failures occur when the failure of a part in a system triggers the failure of successive parts, or when the disruption of one system component triggers failures in other interconnected systems, escalating rapidly if not contained.

To understand cascading failures, we must examine the mechanisms by which risk propagates through complex networks. As noted in recent research on critical infrastructure resilience, the Input-Output Inoperability Method (IIM) is often used to simulate the propagation of inoperability among infrastructures [2]. Inoperability is defined as the inability for a system to perform its intended function. Mathematically, it is quantified by a value between 0 and 1: when the inoperability of an element is 0, it means that it is working at full capacity,

when it is 1, it is completely inoperative. By applying temporal network approaches to the IIM, analysts can capture the dynamic evolution of systemic failure. Time-dependent analyses are required when temporal inhomogeneity matters and understanding the sequence of events is crucial. This is usually the case during the emergency response phase where response time should be as short as possible and a number of cascading events might occur.

The dynamic nature of cascading failures demands a shift from static risk assessments to continuous, system-wide monitoring. The threshold dividing a low-risk operational state from a high-risk cascading failure state must be calibrated according to the criticality of the system and the minimum acceptable performance. Through rigorous sensitivity analysis, organizations can evaluate the advantages of different interventions on the topology of the system, such as introducing redundancies or spin-offs to isolate critical components.

4.2 Managing Infrastructure Interdependencies

Managing interdependencies requires the involvement and cooperation of a wide range of public and private stakeholders—including many over which a single organization has no direct control. Organizations should seek to catalyse action and build support and capacity to respond to these risks across all critical infrastructure sectors [11]. Engaging a multi-sector group of stakeholders is essential, including government agencies, private sector operators, academic experts, and community organizations.

A critical step in managing these dependencies is conducting comprehensive climate and operational risk assessments. These assessments must incorporate information on asset characteristics such as usage, replacement cycle, sensitivity, and criticality to supporting the broader economy. By mapping the connections, dependencies, and interdependencies between organizations, assets, and operations, leaders can identify which links are critical and the directionality of potential failures. For example, solid waste management might depend on a functioning energy system, but not the other way around unless the city uses its waste to produce a significant portion of its energy.

Cities and organizations that successfully navigate these challenges often establish dedicated task forces or councils to facilitate regular, sustained cooperation and information sharing. Creating a safe space for stakeholders to be open about their practices, including providing privacy, legal, and reputational protection for shared sensitive information, is vital. This enables participants to discuss specific risks and collectively evaluate the implications of extreme events for different sectors and organizations.

4.3 Supply Chain Risk and Cyber Sovereignty

Supply chain risk takes center stage in cyber sovereignty as hidden dependencies and long-tail vendors come into focus. Cyber sovereignty is becoming clearer, and for critical infrastructure operators, that clarity could not have come soon enough, ushering in a new era of stronger, more resilient supply chains built on trust and accountability [5]. Typical rules of digital engagement are being rewritten when every third-party vendor relationship is a potential access point and adversaries have demonstrated they are willing to move silently through supply chains for months before conducting an attack. Regulators are increasing scrutiny, boards are raising the bar, and governments are drawing bright lines around trusted vendors, while requiring more transparency in software bills of materials (SBOMs).

Supply chain security across critical infrastructure installations can no longer afford to be an afterthought, but is now something that organizations must consider when building resilience planning. What was once treated as a compliance exercise is being reframed as something more fundamental, addressing control, resilience, and strategic autonomy.

5. Three-Scenario Decision Matrix

Scenario	Description	Organizational Impact	Required Action
Status Quo Disruption	Localized failure of a single critical node (e.g., power outage or minor cyber attack).	Temporary operational halt; manageable financial losses; minor reputational damage.	Implement basic redundancy; conduct regular vendor audits; establish clear communication protocols.

Scenario	Description	Organizational Impact	Required Action
Cascading System Failure	Failure of a primary system (e.g., energy) triggers secondary failures (e.g., telecommunications, finance).	Extended downtime across multiple sectors; significant financial and regulatory penalties; severe reputational harm.	Map second and third-order dependencies; invest in cross-sector simulation models; diversify supply chains.
Systemic Poly-Crisis	Simultaneous occurrence of multiple major disruptions (e.g., massive cyber attack during an extreme weather event).	Catastrophic failure of operations; potential existential threat to the organization; widespread societal impact.	Adopt a "resilience-first" architecture; ensure analog fallback capabilities; integrate geopolitical risk into strategic planning.

Table 2: Three-scenario decision matrix for critical infrastructure failures.

6. Implications for Executive Leadership

Boardrooms are taking a more active role, pushing for continuous assurance over periodic audits. Closing the remaining gaps will require tighter coordination between governments and industry. This comes with a shared recognition that supply chain security is no longer a side concern. It is central to cyber sovereignty. Governance is moving upward in response. Executives must shift their mindset from managing known risks to anticipating complex, interconnected, and evolving threats.

6.1 What a Properly Instrumented Organization Would Do Now

A properly instrumented organization would map its dependencies not just to its direct suppliers, but to its suppliers' suppliers, and the infrastructure that supports them all. It would invest in cross-sector exercises, simulation models, and stress tests. It would embed geopolitical exposure criteria directly into vendor qualification processes and technology procurement standards, alongside traditional factors such as functional safety, cybersecurity maturity, and interoperability. It would ensure that it can explain its own architecture under scrutiny and maintain analog fallback capacities for critical functions.

6.2 What Most Organizations Will Actually Do

The reality is that many organizations plan only for the familiar. They build playbooks based on what they've seen before, rather than preparing for what complex systems can evolve into. They will continue to treat vendor risk as a compliance exercise rather than a strategic imperative. They will rely on vendor self-assessments rather than conducting objective, third-party reviews. And they will remain blind to the hidden dependencies that threaten their operational continuity until a crisis forces them to confront reality.

7. Legal Notice and Methodology

This report is provided for informational and private-review purposes only. It does not constitute legal, financial, or operational advice. The findings are based on a synthesis of publicly available research, academic literature, and industry reporting as of August 2026. The analysis employs qualitative methods to identify trends and assess risks related to critical infrastructure dependencies.

8. References

[1] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11-25. https://www.sciencedirect.com/science/article/pii/S1874548215000803

[2] Cimellaro, G. P. (2024). Modelling infrastructure interdependencies and cascading failures. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S2772741624000218

[3] Swiss Re. (2026). Emerging risks: hidden dependencies in global supply chains. https://www.swissre.com/institute/research/topics-and-risk-dialogues/risk-dialogue-insurance-markets/emerging-risks/emerging-risks-hidden-dependencies-in-global-supply-chains.html

[4] UNDRR. (2021). Cascading risk. PreventionWeb. https://www.preventionweb.net/understanding-disaster-risk/key-concepts/cascading-risk
[5] Industrial Cyber. (2026). Supply chain risk takes center stage in cyber sovereignty as hidden dependencies, long-tail vendors come into focus. https://industrialcyber.co/features/supply-chain-risk-takes-center-stage-in-cyber-sovereignty-as-hidden-dependencies-long-tail-vendors-come-into-focus/
[6] EIS Council. (2026). The Hidden Web of Critical Infrastructure: Why Resilience Planning is A Must. https://eiscouncil.org/the-hidden-web-of-critical-infrastructure-why-resilience-planning-is-a-must/
[7] Macaulay, T. (2019). The Danger of Critical Infrastructure Interdependency. Centre for International Governance Innovation. https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/
[8] UNDRR. (2025). When digital systems fail: An expert report on the hidden risks of our digital world. https://www.undrr.org/publication/documents-and-publications/when-digital-systems-fail-expert-report-hidden-risks-our
[9] Soner, O. A. (2026). Invisible dependencies: The part of the analytics stack we stopped questioning. FinTech Weekly. https://www.fintechweekly.com/magazine/articles/analytics-dependencies-fintech-data-risk
[10] Attinasi, M. G., Boeckelmann, L., Gerinovics, R., & Meunier, B. (2025). Unveiling the hidden costs of critical dependencies. European Central Bank. https://www.ecb.europa.eu/press/economic-bulletin/articles/2025/html/ecb.ebart202505_01~c93c71e372.en.html
[11] C40 Cities Climate Leadership Group. (2019). How to manage infrastructure interdependencies and cascading risk. C40 Knowledge Hub. https://www.c40knowledgehub.org/s/article/How-to-address-infrastructure-interdependencies-when-adapting-to-climate-change?language=en_US