STDs in Critical Infrastructure:

the growing risk of System-Transmitted Disasters and how they affect your Risk Management Framework (RMF)

Publication: 09 June 2026

Contributing Experts:
Dr. Dawn Hersey, Thomas Brown,
John Hart, Randy Nethers, John Farrell

Contact us: team@ferndon.com

FERNDON CONSULTING

Silos are for Grain not Knowledge

Executive Summary

Critical Infrastructure (CI) is facing an acute yet understated challenge through its interconnectedness and interdependence. Once considered a strength to enable rapid growth, interconnectedness is becoming a liability.

Rapid decentralization of security accountability, reduction of federal resourcing, geopolitical uncertainty, and increase of threats within a traditionally "stable" environment have created unprojected risk with marginal support for updating and implementing appropriate mitigation measures. Some organizations' Risk Management Frameworks (RMF) are increasingly underdeveloped and based off historical rather than evolving standards.

Abrupt decentralization of this historically interconnected and federally enabled system is occurring in tandem with increasing asymmetric conflicts, state-sponsored cyber sabotage, insider threats, and extremist attacks. Many attacks are intentionally targeting CI, and some of our opponents are overtly encouraging their operators to target "weak links" within our CI to maximize damage to our society.

Resilience requires more than hardening individual assets. Enabling resilience requires understanding how failure travels through the system, and that is where Intelligence as a Service enables dynamic resilience for organizations.

This white paper presents a scaffold for strategic insights targeting C-suite executives and board members. The intention is to enable a better understanding of the emerging and evolving threat landscape and how this plays into agile risk management.

(Information Cut-Off: 08 June 2026)

Table of Contents

The Governance Paradox: Devolution vs. Dynamic National Security Burden Sharing

The federal government has managed national standardization for many years. Traditionally, it was the central authority and provider resources required for compliance. Both policies and funding for securing CI are now being pushed to state, local, tribal, and organizational levels.

1. The Decentralization of Responsibility

The Federal Government shifted operational security responsibilities, fund sourcing, and compliance management to lower levels of authority in 2025. Previous standards used a federal baseline while enabling locally refined security "as needed" and appropriate. Grants, resources, and federal regulators were available to help maintain, at the very least, the baseline expectation. Some foresightful leaders of larger, forward-leaning, and more financially confident organizations are allocating resources to secure and prepare, regardless of federal assistance. However, many organizations lack resources and context to understand emerging threats. Rapid transition did not help local assumption of increased responsibilities.

2. Outdated Federal Benchmarks that were set to update in 2025

The federal government delegated responsibility for aligning and security resourcing the same year CISA had been tasked to update Federal standards for CI. The structural framework for Sector Risk Management Agencies (SRMAs) highlights an alarming lack of modernization, as the last comprehensive updates occurred in 2013. While Congress addressed the increasing likelihood of catastrophic impacts to our National Security through CI in 2024, and a 2024 National Security Memorandum (NSM) on CI mandated a comprehensive overhaul of federal standards by CISA in 2025, that mandate was not met. CISA has launched a "fortification" initiative in May 2026, but this is focused on Cyber fortification and not comprehensive. As a result, delegation is occurring without the required update to federal standards.

3. The Fallacy of the Strongest Link: Asymptomatic Vulnerabilities

A material flaw in some risk management practices is the assumption of partner reliability. In a highly interconnected ecosystem, managing only the risks arising from within your own perimeter is inadequate. This exposure creates severe blind spots regarding "trusted partners".

This is an example of "Latent Contagion": an organization's risk posture is only as resilient as the weakest link in its supply chain. In complex infrastructure networks, vulnerabilities frequently act as asymptomatic contagions.

Much like latent biological pathogens (e.g., HPV or Sailor's chlamydia), highly destructive network vulnerabilities can exist within a supply chain or utility network without exhibiting active symptoms or triggering standard perimeter alarms. *Any complacency can create an environment where threats projected at low or medium risk are literally a high risk*. When

seemingly stable third-party link breaks under geopolitical or operational strain, it creates an immediate and damaging whiplash effect across the entire ecosystem. If upstream partners conceal risks to protect their valuation, downstream enterprises unknowingly inherit liability.

Cross-Dependency & Hidden Vulnerabilities

Society is sustained by unseen, reciprocal infrastructure dependencies:

- **The Power Grid** drives traffic control, logistics, and cooling systems; backup generators for medical facilities, shelters, schools, and even penal facilities have finite fuel.
- **Telecommunications** sustain automated financial systems, payment systems, emergency response, and remote operations.
- **Cloud Infrastructure** is heavily concentrated in geographically localized data centers that are dependent on regional water tables and localized energy grids.
- **Defense Industrial Base (DIB)** is dependent on the civilian CI for operations while it also provides the necessary material for defense of that CI.

Decentralized risk management obscures cumulative threats, where a single entity's baseline risk can cascade into major downstream failures.

4. Real-World Case Studies: We are Interconnected and Interdependent

The vulnerabilities of decentralized infrastructure are no longer theoretical. Recent attacks have caused immediate financial and physical consequences; more numerous and devastating attacks have already begun and are likely to increase, according to both the 2026 Annual Threat Assessment of the U.S. Intelligence Community and the World Economic Forum.

Case Study: Energy Grid Dependency. January 2026 NECEC Interruption. The New England Clean Energy Connect (NECEC) transmission line, finally completed in January 2026, was engineered to deliver Canadian hydropower to the American northeast after years and complex regulatory hurdles were cleared. However, mere days after activation, power transmission was abruptly suspended by Canadian providers citing "reliability concerns" during a period of severe winter weather; New England, in a period when energy was needed locally to warm homes, began exporting energy. The NECEC includes interstate and international dependencies across austere environments: impacting a significant energy flow to freezing states in the depth of winter is a compounded challenge tied to policy, accountability, and human life.

- **Takeaway:** Infrastructure networks cross international and state jurisdictions with widely divergent priorities, regulatory obligations, and localized stressors. A risk model that fails to account for geopolitical or environmental change cannot guarantee business continuity. Power demands are increasing with growing of Artificial Intelligence and data

center demand. The United States Department of Energy has claimed the "status quo of more generation retirements and less dependable replacement generation" is unsustainable. Recognizing the likelihood of increased change and making modest, proactive spending decisions aimed at diversified sourcing, contractual resilience, and stress-testing —spending even in the low millions—could be small compared to the cumulative costs of a multi-year delay or a single significant winter interruption for replacements and losses into eight-figure territory.

5. The Asymmetric Threat Landscape: Adversarial Doctrine

CI is being targeted systematically by sophisticated state actors and criminal syndicates operating under advanced strategic doctrines. Some is direct, and some is indirect.

- **Chinese Capabilities:** China does not fight the way that we expect fighting - they fight to hit the weak link/underbelly as shown by doctrine and increasing targeting of U.S. CI.
- **Russian Capabilities:** Russia, by doctrine and practice, targets CI directly and indirectly to reduce an opponents' combat capacity and will to fight.
- **Iranian Operations:** Iranian proxies are already attacking American CI, as seen with the 2026 Stryker attack. CISA warns that Iran is now actively using its assets to target U.S. CI.

6. Executive Action: Agile Risk Management through Intelligence

To safeguard enterprise valuation and operational continuity, heavy reliance on historical risk experience and standard compliance checklists is ill-advised. *Effective risk management requires intentional agility in the design and application of frameworks: this is ideally driven by solid intelligence support*. Risk identification, analysis, and assessment must access timely intelligence and be consistently maintained in today's dynamic environment. Mitigation strategies, too, must constantly evolve and leverage technological innovation. The best strategies simultaneously increase transparency and collaboration, horizontally and vertically.

7. Conclusion: The Strategic "So What?" and what can be done about it

The preservation of CI and corporate continuity can no longer depend on the historical baseline of federal oversight or the assumption of regional stability. The delegation of responsibility means that the burden of national resilience has been effectively transferred to corporate executives and local operators to create and sustain their own organic intelligence-driven RMFs. *Organizational resilience requires more than hardening organic assets and liabilities*. Resilient teams and organizations are able to apply nuanced and evolving insight to their RMF: this decreases likelihood of unexpected devastating incidents. *RMFs unsupported by intelligence can become a liability in the dynamic, adversarial market of today.* Elevating your RMF to meet this threat landscape is highly complex, but it is critical for long-term organizational survival.