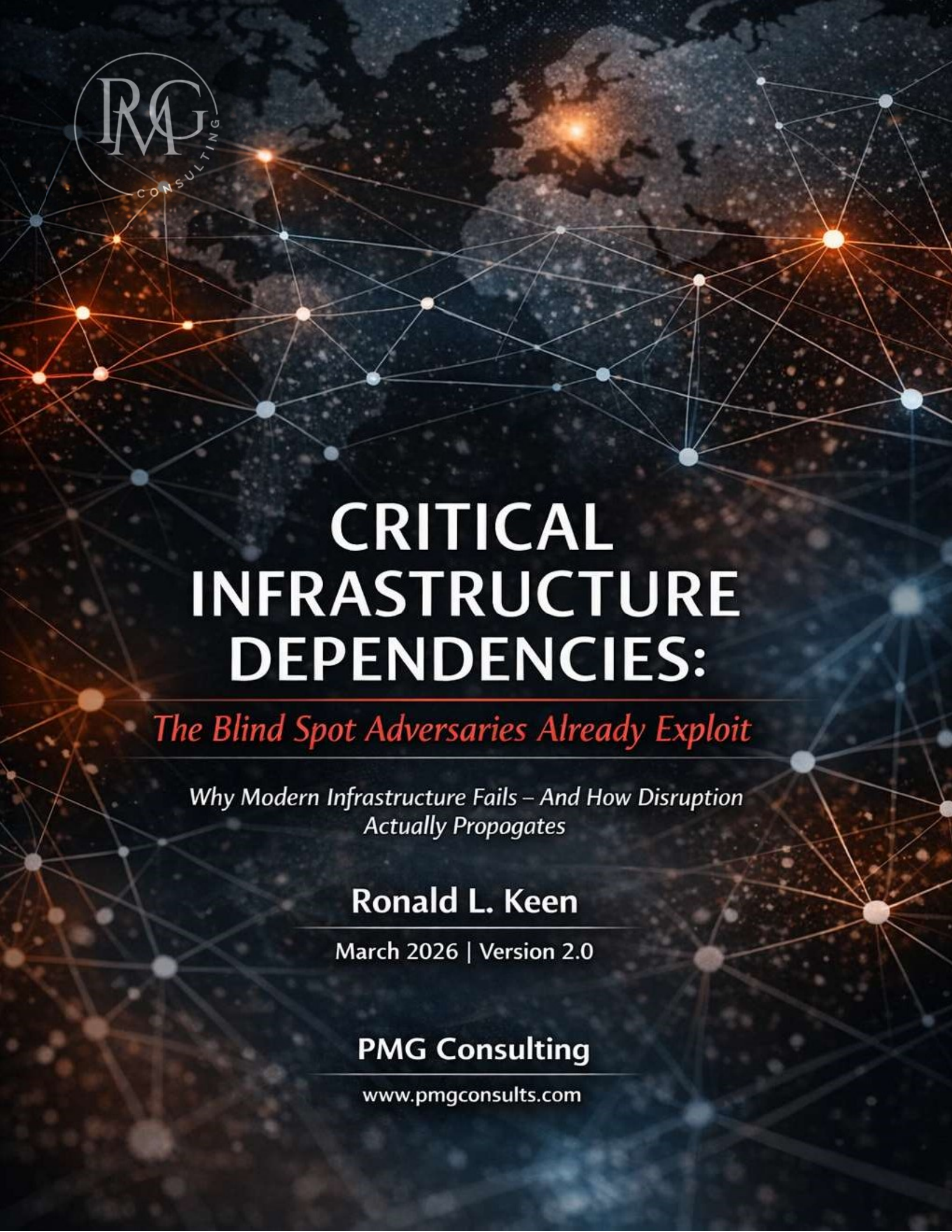


CRITICAL INFRASTRUCTURE DEPENDENCIES:

The Blind Spot Adversaries Already Exploit

Why Modern Infrastructure Fails – And How Disruption Actually Propogates

Ronald L. Keen

March 2026 | Version 2.0

PMG Consulting

www.pmgconsults.com

CRITICAL INFRASTRUCTURE DEPENDENCIES:

The Blind Spot Adversaries Already Exploit

Prepared by:
PMG Consulting
Trusted Advisors in Critical Infrastructure Dependence and Resilience

Author:
Ronald Keen

Edition and Date:
March 1, 2026, Version 2.0

FORWARD

The reality is stark: virtually all governments, including the U.S. Federal and most U.S. State governments, do not possess a comprehensive, baseline of critical infrastructure dependencies — nor do they have the capability to quantify or track them in real time. Dependencies are not static – they shift and cascade across sectors at a velocity often invisible until failure occurs, leaving leaders without the situational awareness needed for sound decisions. The result is a widening blind spot where adversaries exploit chokepoints with precision and even routine natural events create disruptions that ripple into economic, security, and societal crises. In a world of accelerating interconnection, an absence of dynamic dependency insight is itself a national and global vulnerability.

WHAT CRITICAL INFRASTRUCTURE REALLY IS

Critical infrastructure is often described as the backbone of modern society. It is typically categorized in terms of purpose – power plants, water systems, hospitals, ports, pipelines, and data centers. It is physical. Tangible. Definable.

The United States defines critical infrastructure as "…assets, systems, and networks, physical or virtual, so vital that their incapacity or destruction would have a debilitating effect on national security, economic security, public health, or safety", structuring the U.S. infrastructure into 16 designated sectors. Those critical infrastructure sectors have responsibility assigned to Sector Risk Management Agencies (SRMAs), focused on protection, resilience, and risk management. U.S. critical infrastructure is highly governance-driven and designed for administrative clarity. Dependency mapping exists in pockets, but the system is structured vertically.

The United Kingdom defines critical infrastructure much the same, stating that Critical National Infrastructure (CNI) includes facilities, systems, and sites necessary for the functioning of the country and the delivery of essential services. The UK system has 13 sectors with strong central coordination via the Cabinet Office and National Cyber Security Centre (NCSC). The sector designation is clear with an emphasis on resilience and risk assessment and more centralized oversight than the U.S. While the UK system is operationally serious, it remains fundamentally sector-based.

Almost every country defines critical infrastructure in terms of vital sectors, essential services, national security, economic stability, and public safety and almost every system assigns sectors, designates assets, imposes regulatory frameworks, and conducts risk assessments within those sectors. Very few define critical infrastructure explicitly in terms of dependency density[1],

[1] Dependency density refers to the concentration and interconnectedness of dependencies associated with a given system, asset, or function. High dependency density exists when multiple systems rely on a shared component, service, or input, increasing the likelihood that disruption to that node will affect numerous downstream systems simultaneously.

cascading propagation[2], cross-sector amplification thresholds[3], or dynamic criticality under stress[4]. Even fewer structurally integrate space-based dependencies, infrastructure interdependence or machine-speed propagation modeling (MSPM)[5].

The descriptions and definitions are not wrong. They reflect the visible systems upon which daily life depends – electricity keeps homes warm and factories running, water systems sustain public health, transportation networks move goods and people, and data centers power the digital economy. The systems are undeniably vital.

But the description is incomplete.

For more than two decades, governments defined critical infrastructure primarily through a common process - sectors identified, responsibilities assigned, funding streams created, regulations written and compliance regimes are then established. Agencies publish guidance while operators demonstrate adherence to standards. Risk assessments are conducted within defined sector boundaries and the architecture appears rational. It provides clarity, allocates accountability, demonstrates budget justification, and creates measurable outputs and reportable milestones. It gives policymakers metrics which are definable for oversight. In short, it creates order.

Order is comforting. If something is "on the list," it receives attention and, if it is assigned to a sector, someone is responsible. If regulations exist, oversight can be claimed. In essence, the system feels governed. But infrastructure itself does not operate according to administrative charts. It operates according to dependency and the assumption embedded in sector-based designation is that criticality is a property of the asset itself – certain facilities, networks, or systems are inherently critical by virtue of what they are.

---

[2] Cascading propagation describes the process by which disruption in one system spreads through interconnected dependencies to affect additional systems over time. These effects may be sequential or simultaneous and can amplify as they move across infrastructure layers, often producing consequences that exceed the scale of the initial disruption.

[3] Cascading propagation describes the process by which disruption in one system spreads through interconnected dependencies to affect additional systems over time. These effects may be sequential or simultaneous and can amplify as they move across infrastructure layers, often producing consequences that exceed the scale of the initial disruption.

[4] Dynamic criticality under stress refers to the condition in which the importance of a system, asset, or dependency changes based on operational context, demand, or environmental conditions. Systems that are non-critical under normal conditions may become critical during periods of peak demand, disruption, or constrained redundancy.

[5] Machine-speed propagation modeling (MSPM) refers to the computational analysis of how disruptions spread through interconnected infrastructure systems at speeds matching or exceeding automated system operations. As conceptualized, MSPM leverages real-time data, algorithms, and network-based modeling to simulate how failures propagate across digital, physical, and economic dependencies faster than traditional human-driven analysis can observe or respond. This approach becomes necessary in modern infrastructure environments where automated control systems, algorithmic decision-making, AI-assisted control systems, and high-frequency data exchanges can transmit disruption effects across multiple sectors in seconds or milliseconds.

In reality, criticality should not be a label. It is a condition which emerges from the degree to which other systems depend on a function and how those dependencies behave under stress. A facility may be designated critical and yet possess sufficient redundancy to absorb disruption with limited systemic effect. Conversely, a component that appears secondary, unlisted, or commercially mundane may serve as a structural hinge point whose disruption cascades across sectors. Designation organizes responsibility. Dependency determines consequence.

Modern infrastructure systems no longer operate primarily as independent stove-piped sectors. Advances in digital technology, automation, and global connectivity have transformed infrastructure into a highly interconnected system of dependencies in which disruption rarely remains confined within a single sector. Failures in one system increasingly propagate across others through shared energy supplies, communications networks, digital platforms, logistics systems, and information ecosystems.

As a result, infrastructure disruptions often unfold as cascading events rather than isolated failures. Power outages affect telecommunications networks and transportation systems while communications disruptions affect financial transactions, emergency response coordination, and supply chain logistics. Digital infrastructure failures can simultaneously disrupt healthcare systems, government operations, and commercial activity and traditional sector-based analysis still provides valuable administrative organization but does not fully capture how cascading dependencies operate within modern infrastructure systems.

And in an era where disruption travels faster than decision-making cycles, that distinction is no longer academic. It is structural.

THE HIDDEN FRAGILITY OF CRITICAL INFRASTRUCTURE

Critical infrastructure is often described as the backbone of a nation's prosperity and national security. Energy systems, water networks, healthcare delivery, transportation corridors, financial platforms, communications networks, and digital infrastructure represent the visible lifelines of modern society. These systems sustain daily life, enable economic activity, and support the functions of government and national defense.

Yet this visible infrastructure tells only part of the story.

Beneath these systems exists a complex and often poorly understood network of dependencies and interdependencies—a dynamic architecture in which infrastructure systems do not operate independently, but instead rely continuously on one another to function. Power enables communications. Communications enable financial transactions. Digital systems coordinate logistics and supply chains. Each system both supports and depends upon others, forming a tightly coupled network in which disruption rarely remains isolated.

Within this dependency architecture lie critical chokepoints – shared systems, services, and processes whose disruption can propagate rapidly across multiple sectors. These chokepoints are frequently invisible within traditional sector-based models because they do not belong to a single

sector but instead operate across many. In many cases, even infrastructure operators understand their own systems in detail but lack visibility into the broader dependency environment in which those systems operate.

As infrastructure systems have become more digitized, automated, and interconnected, the nature of these dependencies has evolved. The speed at which systems interact has accelerated, the number of interconnections has increased, and the distance over which dependencies operate has expanded. Infrastructure is no longer constrained by geography alone—it is shaped by networks of data, synchronization, and coordination that extend beyond traditional physical boundaries.

Increasingly, these dependencies are not confined to terrestrial systems.

CRITICAL INFRASTRUCTURE IS NOT A SET OF SILOS — IT IS A FRAGILE WEB OF DEPENDENCIES. ONE FAILURE CAN RIPPLE ACROSS SECTORS IN MINUTES OR HOURS.

THE EXPANSION OF DEPENDENCY BEYOND GEOGRAPHY

Historically, infrastructure dependencies were largely regional or national in scope. Energy systems served defined geographic areas. Transportation networks operated within physical corridors; communications infrastructure bound by terrestrial networks and national jurisdictions. While interdependencies existed, they were often limited by physical proximity and slower rates of interaction.

That constraint no longer holds. Modern infrastructure systems operate within a globally interconnected environment where dependencies extend across borders, domains, and operational layers. Data flows, financial transactions, supply chains, and control systems now operate across distributed networks that are not tied to a single location. As a result, disruption in one region can propagate rapidly into others, and dependencies that appear local may, in fact, rely on systems operating at national or global scale.

THE RISE OF NON-PHYSICAL DEPENDENCIES

Equally important is the shift from purely physical dependencies to non-physical ones. Traditional infrastructure models focused on tangible assets—pipes, wires, roads, facilities, and equipment. While these remain essential, modern infrastructure increasingly depends on intangible systems such as data, software, algorithms, and synchronization services. These systems do not always appear on infrastructure maps, yet they control, coordinate, and optimize the operation of physical infrastructure at scale.

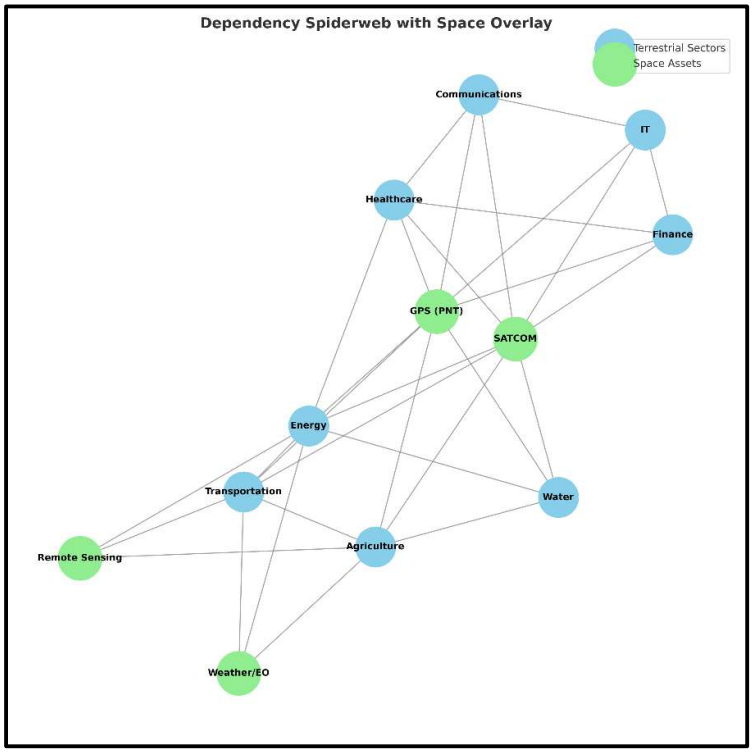
Because these dependencies are less visible, they are often less understood and less protected. However, their disruption can produce effects that rival or exceed those of physical infrastructure failure, particularly when they serve as shared enabling systems across multiple sectors.

SPEED, SCALE, AND COMPLEXITY

The combination of expanded geographic reach and non-physical dependencies has fundamentally altered how disruption propagates. Infrastructure systems now operate at speeds determined by automated processes, digital communications, and machine-to-machine interaction. As a result, disruptions can spread across interconnected systems faster than human operators can detect, assess, or respond. What may begin as a localized event can quickly escalate into a multi-sector disruption through cascading propagation across shared dependencies.

This shift from human-paced to machine-speed interaction represents a fundamental change in the infrastructure risk environment. Understanding and managing this environment requires analytical approaches capable of modeling dependencies, propagation pathways, and systemic effects at the same speed and scale at which they occur.

SPACE



Every sector of modern critical infrastructure now relies—often invisibly—on space-based systems as a foundational enabling layer. Positioning, Navigation, and Timing (PNT) services synchronize financial markets to the microsecond, stabilize power grid frequency, and guide aviation and maritime operations. Satellite communications underpin emergency response coordination, military command and control, and serve as critical redundancy when terrestrial networks fail. Weather and earth observation systems inform agriculture, disaster response, logistics planning, and energy demand forecasting at national and global scale.

These are not ancillary services. They are embedded dependencies and what distinguishes space-based infrastructure from traditional dependencies is its reach and simultaneity. A single disruption in space does not remain localized—it affects every dependent system within its coverage area at once. Unlike terrestrial failures, which are often geographically bounded and operationally containable, space-based disruptions propagate across sectors and regions simultaneously, creating immediate, multi-domain consequences.

Most critically, these dependencies are largely invisible in traditional infrastructure models. They do not reside within a single sector, fall neatly under a single regulator, or appear as discrete

assets in risk assessments. As a result, their systemic importance is often underrepresented until disruption occurs. When it does, the effects do not unfold sequentially—they emerge concurrently across multiple sectors, compressing response timelines and amplifying cascading impact.

In this context, space infrastructure functions not as a supporting capability, but as a shared dependency layer upon which modern infrastructure stability increasingly depends.

"EVERY SECTOR OF CRITICAL INFRASTRUCTURE NOW DEPENDS ON SPACE."

ARTIFICAL INTELLIGENCE AND MACHINE LEARNING

A second and increasingly consequential layer of risk emerges from the integration of artificial intelligence (AI) into infrastructure operations. Unlike traditional systems, which operate within defined parameters and human oversight cycles, AI-driven systems make decisions, execute actions, and interact with other systems at machine speed. They are not simply tools layered onto infrastructure, they are becoming embedded within the operational logic governing how infrastructure functions.

AI systems are already optimizing power grid distribution, managing logistics networks, detecting anomalies in cybersecurity environments, and supporting clinical decision-making in healthcare. As adoption expands into autonomous transportation, dynamic supply chain coordination, and defense systems, AI will increasingly operate as a real-time control layer across multiple infrastructure sectors simultaneously.

This shift introduces a fundamental change in how disruption propagates.

When AI-enabled systems are interconnected through shared data sources, cloud platforms, and space-based inputs such as Positioning, Navigation, and Timing or satellite communications, disruption is no longer constrained by physical infrastructure boundaries. Instead, errors, corrupted data, or degraded inputs can be processed, amplified, and transmitted across systems at speeds far exceeding human response capabilities. What might once have been a localized disruption can be interpreted, acted upon, and redistributed across multiple sectors in seconds.

In this context, AI functions as a force multiplier of dependency risk. It does not create dependencies on its own, but it accelerates how those dependencies interact and how disruption propagates through them. When coupled with space-based infrastructure—which provides the global synchronization, connectivity, and data inputs upon which many AI systems rely—the result is a tightly coupled, high-speed dependency architecture where disruption can scale rapidly and simultaneously across sectors.

AI does not simply increase efficiency within infrastructure systems. It compresses time, expands interconnectivity, and reduces the margin for human intervention. As a result, the combination of AI-enabled control systems and space-based dependencies represents a new class of infrastructure risk—one defined not only by interdependence, but by the speed and scale at which disruption can propagate. This condition can be understood as Machine-Speed Propagation

(MSP) – the ability of disruption to move through interconnected infrastructure systems at the pace of automated decision-making rather than human response.

Under MSP conditions, infrastructure systems no longer fail in a sequence that can be observed, assessed, and managed through traditional human-centric processes. Instead, disruption is ingested as data, processed through algorithms, and acted upon by automated systems in real time. Artificial intelligence and machine learning models, trained to optimize efficiency, stability, and performance, can inadvertently amplify disruption when operating on degraded, incomplete, or adversarial data inputs. In such environments, systems do not wait for human validation; they execute.

This creates a fundamental asymmetry between system behavior and human oversight. Human operators, regulators, and decision-makers operate within cognitive and organizational timeframes measured in minutes, hours, or longer. Machine-driven systems operate in milliseconds. By the time a disruption is detected and understood by human actors, it may have already propagated across multiple infrastructure layers, triggering secondary and tertiary effects that are no longer easily reversible.

Artificial intelligence does not simply introduce new vulnerabilities. It transforms the tempo of infrastructure risk. In a machine-speed environment, resilience can no longer rely solely on human detection and response. It must incorporate computational models capable of identifying, interpreting, and mitigating cascading effects at the same speed at which they propagate. Without such capabilities, infrastructure systems become increasingly exposed to disruptions that move faster than the institutions designed to manage them.

CASCADING FAILURE AS A WEAPON

Modern infrastructure systems do not exist solely within the context of natural hazards or accidental disruption but represent potential targets within strategic competition between nation-states. Increasingly, strategic writings and operational behavior from adversarial competitors indicate a growing interest in exploiting systemic infrastructure vulnerabilities as part of broader geopolitical and military strategy. Understanding how adversaries analyze infrastructure systems is therefore essential to developing an effective national infrastructure protection framework.

Traditional infrastructure protection models often focus on the defense of individual assets or sectors. However, several adversarial doctrines emphasize targeting systemic dependencies rather than isolated facilities. In these approaches, infrastructure disruption is most effective when it propagates across multiple systems simultaneously, creating cascading effects that amplify the strategic impact of relatively limited actions.

Chinese military writings provide one of the clearest examples of this approach. The concept of "Unrestricted Warfare," articulated by People's Liberation Army (PLA) officers Qiao Liang and Wang Xiangsui in 1999, argued modern conflict increasingly extends beyond conventional military domains to include economic, technological, informational, and infrastructure systems. In this

framework, adversaries seek to exploit interconnected systems in ways creating strategic advantage without necessarily engaging in traditional kinetic conflict. Subsequent Chinese military publications continue emphasizing the importance of identifying systemic vulnerabilities within technologically dependent societies.

Russian strategic thinking has also emphasized the exploitation of systemic weaknesses in critical infrastructure as evidenced by Russian military strategy in the current Russia-Ukraine conflict (i.e., energy systems, dams, etc.). Russian military doctrine and associated writings on information confrontation and hybrid warfare describe approaches combining cyber operations, information manipulation, and infrastructure disruption to destabilize adversaries and complicate their decision-making during crises. Western analyses of Russian cyber operations, including attacks on Ukrainian energy infrastructure beginning in 2015, demonstrate how digital systems supporting physical infrastructure can be targeted to create cascading operational disruptions.

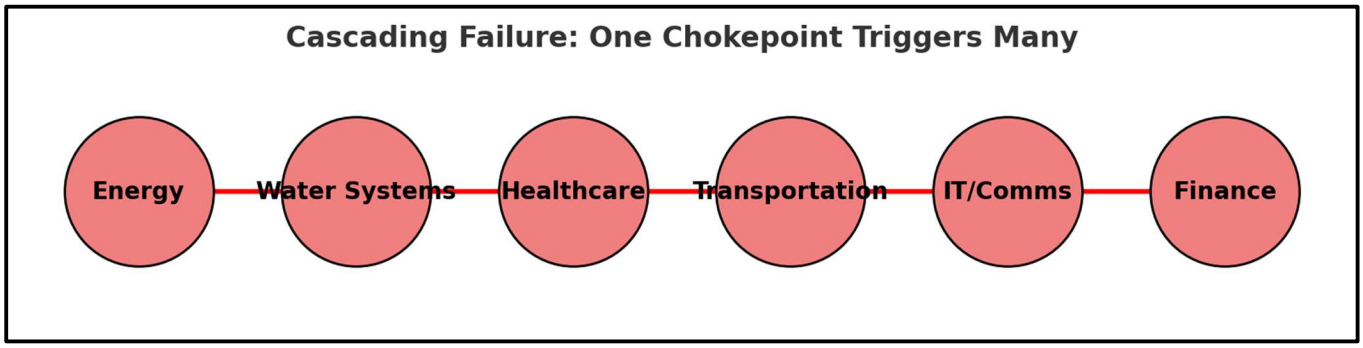
Such approaches reflect an understanding that modern infrastructure operates as a system of systems. Disruption to shared enabling services such as telecommunications networks, cloud computing infrastructure, positioning and timing services, or industrial control platforms can propagate across multiple sectors simultaneously. From a strategic perspective, these shared dependencies represent high-leverage targets capable of generating cascading consequences across a nation's infrastructure ecosystem.

A stratified infrastructure framework aligns more closely with this strategic reality than traditional sector-based models by examining infrastructure through functional layers – lifeline systems, enabling systems, national infrastructure, and societal stability mechanisms. This layered perspective highlights infrastructure systems whose disruption could produce cascading effects across multiple sectors, enabling more accurate threat assessment and resilience planning.

Incorporating adversarial infrastructure targeting concepts at a high discussion level into national infrastructure policy reinforces the importance of cross-sector analysis and integrated resilience planning. Infrastructure protection strategies that focus exclusively on sector boundaries may overlook vulnerabilities that emerge at the intersection of multiple systems. Conversely, understanding how adversaries evaluate systemic dependencies allows policymakers to prioritize protective measures and resilience investments where disruption would produce the greatest national consequence.

Ultimately, modern infrastructure protection must recognize infrastructure systems are essential to economic and societal stability as well as increasingly relevant to national security competition. As technologically advanced societies become more interconnected and digitally integrated, the infrastructure dependencies supporting everyday life may also represent potential avenues for strategic disruption. Integrating stratified dependency analysis into national infrastructure policy

therefore strengthens the nation's ability to anticipate adversarial targeting strategies and reduce the risk of cascading infrastructure failure during periods of geopolitical tension or crisis.

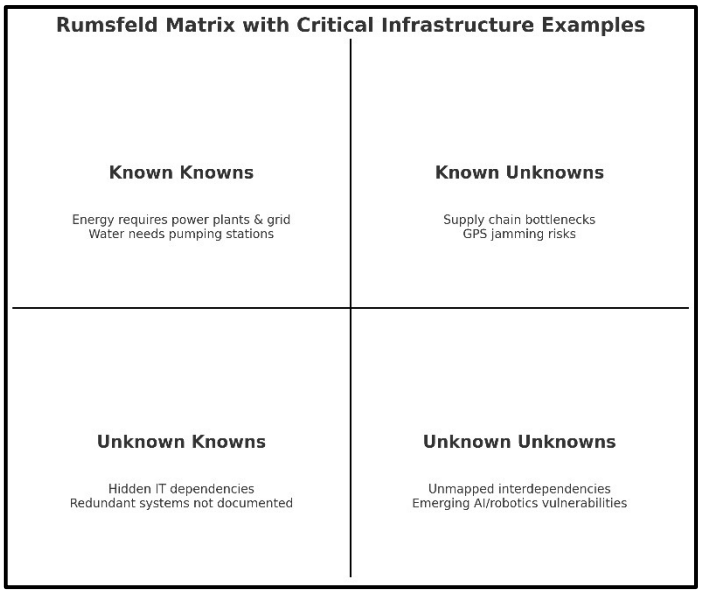


This is not theory — it has already happened:

- **Fukushima Earthquake & Tsunami (Japan, 2011):** Triggered a nuclear crisis, massive power outages, and global supply chain disruptions in automotive and electronics sectors.
- **China Container Recall (2020–21):** Small logistics shifts disrupted U.S. agriculture and global trade, underscoring worldwide dependence on maritime supply chains.
- **GPS Disruptions (Europe, 2019–22):** Aviation and logistics delays highlighted the fragility of space-based dependencies across borders.
- **Colonial Pipeline (U.S., 2021):** Ransomware disrupted nearly half of East Coast fuel supplies in days, rippling into aviation and logistics.
- **Texas Winter Storm (U.S., 2021):** $100B in losses as energy collapse paralyzed water, healthcare, and food systems.
- **Gaza Conflict (2023, 2025):** Infrastructure strikes cascaded across every sector defined and undefined, demonstrating wartime impacts on the economy as well as civilian lifelines.

Adversaries understand this: cascading failure is the weapon. A single chokepoint — cyberattack, energy collapse, GPS outage, or supply chain disruption — can ripple across sectors, disable entire systems, and undermine both economic stability and military capacity.

THE UNKNOWN CHOKEPOINTS



The most dangerous vulnerabilities are not those already mapped, but the unknown dependencies which remain invisible until they fail. When viewed through the lens of dependency analysis, the Rumsfeld matrix provides more than a conceptual categorization of uncertainty. It becomes a practical framework for understanding why traditional infrastructure risk assessment consistently underestimates systemic vulnerability. In infrastructure terms:

• **Known Knowns** – Represent dependencies both recognized and actively managed. These include well-understood relationships such as energy supporting water treatment and distribution, or GPS-based timing enabling financial transaction synchronization. These dependencies are typically incorporated into planning, redundancy strategies, and regulatory oversight. They form the visible portion of the infrastructure dependency environment and are the primary focus of most existing resilience efforts.

• **Known Unknowns** – Represent dependencies acknowledged but not fully understood in terms of their behavior under stress or failure conditions. These include complex supply chain dependencies, communications interdependencies, cloud infrastructure reliance, and space-based services. While these dependencies are recognized, their cascading impacts, failure modes, and cross-sector consequences are often only partially modeled. As a result, they introduce uncertainty into risk assessments and are frequently underestimated in both planning and investment decisions.

• **Unknown Knowns** – Represent dependencies which exist and are understood in isolated contexts but not recognized as part of the broader infrastructure dependency architecture. In many cases, technical experts, operators, or specific organizations are aware of these dependencies within their domain, but that knowledge is not integrated across sectors, agencies, or systems. This creates a condition where critical information exists but is not operationalized at the system level. Examples include software dependencies embedded within critical systems, localized infrastructure constraints, or sector-specific reliance on shared services that are not visible outside of their immediate operational context. In the threat intelligence arena, these represent known risks that have not been connected, shared, or elevated to inform broader systemic analysis.

• **Unknown Unknowns** – Represent dependencies and interdependencies entirely unrecognized prior to disruption. These are the most dangerous category within modern infrastructure systems because they exist outside current models, assumptions, and planning frameworks. Hidden

chokepoints embedded in tightly coupled systems—such as energy-water interactions, reliance on shared timing signals like GPS, or undiscovered software and data dependencies—often fall into this category. These dependencies are typically revealed only through failure, when cascading effects expose relationships that were previously invisible. Unlike unknown knowns, there is no prior awareness to draw upon, making prediction and mitigation significantly more difficult.

The critical insight is that modern infrastructure risk is not defined solely by what is known, but by the expanding boundary between what is known and what remains unseen. As infrastructure systems become more interconnected, digitized, and automated, the proportion of dependencies falling into the "known unknown," "unknown known," and "unknown unknown" categories increases. This creates a structural condition in which infrastructure operators and policymakers are making decisions based on incomplete representations of the systems they are attempting to protect.

In this context, the Rumsfeld matrix is not an abstract framework, but a diagnostic tool for identifying Dependency Blindness within infrastructure systems. It highlights where knowledge exists, where uncertainty persists, where knowledge is fragmented and unintegrated, and where systemic risk is effectively invisible until triggered by disruption. This becomes particularly significant in a machine-speed environment. Under conditions of Machine-Speed Propagation (MSP), disruptions do not unfold slowly enough to allow unknown dependencies to be discovered and managed in real time. Instead, hidden interdependencies are revealed through cascading failure, often after propagation has already extended across multiple sectors. The result is not simply a lack of awareness, but a loss of the ability to intervene effectively.

For this reason, understanding and mapping dependencies across all four categories is not optional—it is foundational to modern infrastructure resilience. Without the ability to identify and integrate unknown knowns, and to anticipate the existence of unknown unknowns, infrastructure risk assessment remains anchored in partial visibility, and resilience strategies are built around an incomplete picture of how systems actually behave under stress.

THE NEW DOMAINS – AND WHAT THEY TRULY REPRESENT

Beyond the U.S. Department of Homeland Security's (DHS) 16 designated sectors, as well as critical infrastructure sectors designated by other nations, new domains continue to emerge as critical components of national infrastructure systems. These domains are often discussed as potential "new sectors," yet framing them solely as sectors risks misunderstanding their true role within the infrastructure ecosystem.

In reality, many of these emerging domains do not function as independent sectors. They operate as cross-cutting dependency layers that influence, control, or enable multiple sectors simultaneously. As a result, their importance is often underestimated within traditional designation-based models, which are structured around discrete categories rather than systemic interaction.

Examples of these emerging domains include:

- **Artificial Intelligence** – managing grids, healthcare, and logistics but utterly dependent on space data. Increasingly embedded within infrastructure operations, AI functions as a real-time decision and control layer, influencing how multiple sectors operate simultaneously rather than serving as a stand-alone sector.
- **Biosciences** – driving pharmaceuticals, medical research, and food security, sustained by energy and global logistics. Bioscience systems intersect with healthcare, agriculture, supply chains, and national security, creating dependencies that extend across multiple infrastructure layers.
- **Robotics** – enabling defense and manufacturing, but reliant on continuous timing and connectivity. Robotics systems depend on communications, positioning and timing services, and digital control systems, integrating tightly with both physical and digital infrastructure environments.

These are not simply additional sectors waiting to be designated. They represent converging domains of capability and dependency that operate across the existing infrastructure landscape. Treating them as isolated sectors risks obscuring the very interdependencies that make them strategically significant.

This reveals a broader limitation within current infrastructure designation methodologies. Sector-based frameworks are designed to organize governance and assign responsibility, but they are less effective at capturing how modern infrastructure systems actually behave. As new domains emerge, the instinct to assign them to a sector—or create a new one—reinforces a structure that may not reflect the underlying dependency architecture.

The result is a growing mismatch between how infrastructure is categorized and how it operates. This mismatch becomes even more pronounced when examining additional domains that have been historically treated as secondary, embedded, or "supporting" functions rather than as critical components of infrastructure dependency:

- **Cloud and Hyperscale Data Infrastructure** – often subsumed within the Information Technology sector, yet functioning as a foundational platform upon which multiple sectors operate. Financial systems, healthcare, logistics, government services, and communications increasingly rely on a small number of globally distributed cloud providers. This creates high dependency density and concentrated systemic risk, where disruption within a limited set of platforms can propagate across numerous sectors simultaneously.
- **Global Supply Chain and Logistics Coordination Systems** – frequently treated as components of transportation or commercial activity rather than as infrastructure in their own right. Modern supply chains are digitally orchestrated systems dependent on real-time data, financial clearing mechanisms, energy availability, and global communications. Disruption within logistics coordination platforms can cascade into manufacturing, healthcare, food systems, and national defense.
- **PNT Services** – typically associated with space infrastructure, but rarely treated as a distinct dependency layer despite its systemic importance. PNT underpins telecommunications synchronization, financial transaction timing, power grid stability, transportation safety, and

military operations. Its loss or degradation produces immediate cross-sector effects that are disproportionate to its visibility within traditional infrastructure frameworks.

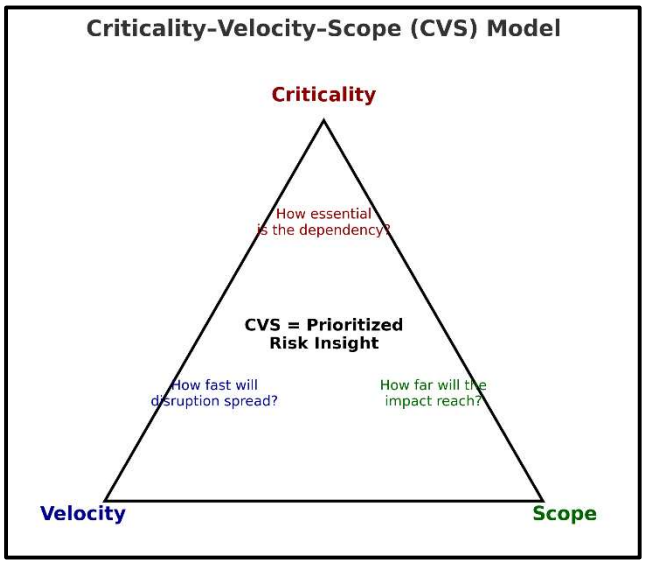
- **Data and Algorithmic Decision Systems** – increasingly embedded across sectors but rarely recognized as infrastructure. Predictive analytics, optimization algorithms, and automated decision systems now influence energy distribution, financial markets, logistics routing, and emergency response. These systems create dependencies not only on data integrity but on model behavior, introducing new forms of systemic risk tied to data quality, bias, and adversarial manipulation.
- **Human Capital and Specialized Workforce Dependencies** – often excluded from infrastructure definitions but critical to system continuity. Highly specialized personnel required to operate, maintain, and restore infrastructure systems—such as grid operators, cybersecurity professionals, and industrial control engineers—represent a form of dependency that is difficult to scale or rapidly replace. Workforce disruptions can therefore create bottlenecks that propagate across infrastructure systems during crisis conditions.

These domains are rarely ignored entirely, but are frequently diffused across sectors, underrepresented in risk models, or treated as subordinate functions rather than systemic dependencies. As a result, their role in enabling and sustaining infrastructure operations is often underestimated until disruption exposes their significance. These undesignated dependencies, in some cases, are barely tracked, leaving widening blind spots. Because they do not fit cleanly within existing sector definitions, they may fall outside formal risk assessments or be evaluated only within narrow domain-specific contexts. Meanwhile, the sectors that continue to shape a nation's economic and security future may be building on fragile foundations adversaries continue to aggressively probe.

Compounding this challenge is the way infrastructure insight is generated and shared. Past assessments have been accomplished, especially in the U.S., but findings are typically classified at levels that limit accessibility to the very operators, regions, localities, and agencies responsible for implementing resilience measures. As a result, critical insights into systemic vulnerabilities may exist but remain fragmented, restricted, or disconnected from operational decision-making. This creates a paradox within infrastructure risk management: knowledge is generated but not broadly integrated, dependencies exist but are not fully mapped, and emerging domains influence multiple sectors without being fully recognized within existing frameworks.

In this context, the challenge is not simply identifying new sectors, but understanding how these emerging domains reshape the dependency architecture of modern infrastructure systems. Without that understanding, designation-based approaches risk lagging behind the very systems they are intended to protect.

THE CVS FRAMEWORK: FROM DESCRIPTION TO ACTION



A structured methodology is required to move beyond descriptive infrastructure analysis and into actionable, predictive capability. The Criticality–Velocity–Scope–Duration (CVS-D) model (patent pending) provides such a framework, enabling the quantification of infrastructure dependencies in a manner not previously achieved within traditional sector-based or qualitative assessment approaches.

CVS-D moves dependency analysis from description to action by quantifying four essential major dimensions:

- **Criticality** – how essential is a dependency to the function of the system, sector, or broader infrastructure environment? This dimension evaluates not only direct importance, but also the degree to which a dependency supports multiple systems simultaneously, reflecting its role within the broader dependency architecture.
- **Velocity** – how quickly will a disruption in the dependency spread through interconnected systems? This dimension captures the rate of propagation, particularly in environments where automated systems, digital networks, and AI-driven processes operate at machine speed, enabling disruption to move faster than human response.
- **Scope** – how broad will the impact be: local, regional, national, or global? This dimension evaluates the geographic and systemic reach of disruption as it propagates across infrastructure layers and sectors.
- **Duration** – how long will the disruption persist and continue to generate operational, economic, or systemic effects? Duration captures the temporal dimension of disruption, including whether impacts are transient, sustained, or compounding over time. It reflects not only the length of the initial disruption, but also the persistence of downstream effects as systems struggle to recover, stabilize, or adapt.

Using the data from these four major dimensions, as well as the minor dimensions supplementing them, the CVS-D model transforms dependency mapping into actionable intelligence. It reveals not only where chokepoints exist, but also how disruption will behave—how rapidly it will propagate, how widely it will spread, how long it will persist, and how severely it will impact interconnected systems.

This represents a fundamental shift in infrastructure analysis.

Traditional infrastructure assessments tend to identify assets, vulnerabilities, and risks within defined sector boundaries. While useful for governance and compliance, these approaches do not adequately capture how disruption propagates across interconnected systems. CVS-D

addresses this gap by focusing not on isolated assets, but on the behavior of dependencies under stress.

Duration plays a particularly important role in this context. Short-duration disruptions may be absorbed by redundancy, contingency planning, or adaptive system behavior. However, extended-duration disruptions—especially those affecting enabling infrastructure—can exhaust redundancy, degrade system stability, and amplify cascading effects across multiple sectors. In many cases, it is not the initial disruption that produces systemic failure, but the inability of systems to recover within a timeframe that prevents secondary and tertiary impacts from emerging.

In doing so, CVS-D provides the analytical foundation required to understand and manage infrastructure risk in a machine-speed environment. When combined with the concept of Machine-Speed Propagation (MSP), the model enables analysts to evaluate not only whether a disruption will occur, but whether it will propagate faster than response mechanisms can adapt and persist long enough to overwhelm recovery capabilities. This distinction is critical in modern infrastructure systems, where automated processes can transmit disruption across multiple sectors in seconds while recovery may take hours, days, or longer.

CVS-D also directly addresses the problem of Dependency Blindness. By quantifying relationships that are often unobserved, fragmented, or poorly understood, the model exposes hidden chokepoints, cross-sector amplification pathways, and systemic vulnerabilities that do not appear in traditional risk assessments. It provides a structured method for identifying both known unknowns and unknown knowns, and for bounding the potential impact of unknown unknowns through modeled propagation behavior and persistence over time.

Importantly, CVS-D is not simply an analytical tool—it is a decision-support capability. By translating dependency relationships into quantifiable dimensions, it enables policymakers, infrastructure operators, and national security planners to prioritize resilience investments based on systemic consequence rather than sector designation alone. It supports scenario modeling, stress testing, and contingency planning at a level of fidelity consistent with how modern infrastructure systems actually operate.

The absence of such a capability creates a structural disadvantage. Because most nations do not currently possess a methodology for quantifying dependency behavior across interconnected infrastructure systems, risk management remains largely reactive. Governments and operators respond to disruptions after they occur, often discovering critical dependencies only through failure. Without the ability to model propagation, identify high-velocity chokepoints, anticipate cross-sector impacts, and assess the persistence of disruption over time, resilience strategies are inherently incomplete.

In this context, CVS-D represents more than an analytical improvement. It represents a necessary evolution in how infrastructure risk is understood and managed. As infrastructure systems become more interconnected, digitized, and dependent on machine-speed processes, the ability

to quantify dependency behavior, including how long disruption persists, will increasingly define the difference between reactive response and anticipatory resilience.

"CVS-D REVEALS NOT JUST WHERE FAILURES CAN HAVE SIGNIFICANT IMPACTS, BUT HOW FAST AND HOW FAR THEY WILL SPREAD."

The message is clear: without structured tools with the capability of the CVS-D model, decision-makers remain blind to the very risks adversaries exploit.

WHY THIS MATTERS NOW

Modern critical infrastructure can no longer be understood as a collection of independent sectors. It operates as a layered, interdependent system in which disruption propagates across physical, digital, economic, and societal domains. This paper has demonstrated several key realities:

- Infrastructure criticality is not defined by designation, but by dependency and cascading impact
- Modern systems operate within a stratified architecture, where lifeline, enabling, national, and societal layers interact continuously
- Disruption increasingly propagates at machine speed, outpacing human detection and response
- Critical dependencies—particularly in space, AI, data systems, and supply chains—are often invisible within current frameworks
- Effective resilience requires the ability to measure dependency behavior, not simply identify assets

Taken together, these realities point to a single conclusion: the current sector-based model, while valuable for governance, is insufficient for understanding and managing modern infrastructure risk.

NATION'S DO NOT HAVE A COMPLETE BASELINE UNDERSTANDING OF CI DEPENDENCIES. LEADERS ARE MAKING DECISIONS BLIND WHILE ADVERSARIES STRIKE WITH CLARITY.

Without a comprehensive, all-inclusive effort, many nations remain dangerously exposed. Adversaries will continue to exploit chokepoints that are unrecognized or poorly understood. Natural disasters will trigger cascading losses across interconnected systems. States, agencies, and companies will remain blind to their most consequential vulnerabilities—not because those vulnerabilities do not exist, but because they are not visible within existing analytical frameworks. With the right approach, leaders gain the ability to identify chokepoints before adversaries do, anticipate how disruptions will spread and at what speed, and target resilience investments with precision. This includes understanding not only where dependencies exist, but how they behave under stress—how quickly disruption propagates, how broadly it spreads, and how long it persists. The payoff is stronger deterrence, protection of millions of lives, preservation of billions or even trillions in economic activity, and improved readiness both within national borders and across international partnerships.

However, insight without accessibility has limited value. Prior assessments have generated important findings, but many remain classified at levels that prevent their use by the operators, regions, and agencies responsible for implementing resilience measures. As a result, knowledge exists but is not operationalized. This study must therefore be redone—or extended—at an accessible level, ensuring that actionable insights are placed in the hands of those responsible for safeguarding critical infrastructure at every level of governance.

The challenge is no longer one of awareness, but of adaptation.

The question is not whether nations can continue to rely on existing models, but whether those models accurately reflect how infrastructure systems now function. In an environment defined by interdependence, machine-speed propagation, and expanding dependency layers, failure to adapt analytical frameworks will result in persistent strategic disadvantage.

The real question is not whether the United States—or any nation—can afford to do this work. It is whether it can afford to remain dependent on models that no longer reflect reality.

VULNERABILITIES ARE REAL. ADVERSARIES ARE ACTIVE. CHOKEPOINTS REMAIN UNKNOWN.

ABOUT PMG CONSULTING

PMG Consulting began as a trusted advisor in utility regulatory work for multiple U.S. states, building a reputation for integrity, technical depth, and clear-eyed analysis across energy, telecommunications, water, and other lifeline sectors. With decades of hands-on experience in these foundational infrastructures, PMG has become a natural partner for organizations seeking to understand and mitigate critical infrastructure interdependencies. Our expansion into resilience, continuity of operations (COOP), contingency, and emergency planning reflects that expertise — helping terrestrially based critical infrastructure clients address cascading risks that cross sector boundaries. While PMG focuses on terrestrial lifeline systems, we leverage Orion Space's expertise in space-based dependencies in the background, ensuring our clients benefit from a complete picture of vulnerabilities without diluting our terrestrial credibility.