Quantifying Cyber Resilience: A Systemic Risk Perspective on Critical Infrastructure Protection

Saurabh Pathak[1], Dr. Aditya Gautam[2]
Student[1], Professor[2]
Department of Computer Science and Engineering
Mass College of Engineering & Management
Corresponding Author's Email: - *saurabhpathak696@gmail.com[1]*

Abstract

Modern critical infrastructure systems—energy grids, water utilities, transport corridors—function as tightly coupled cyber physical webs where localized disruptions cascade into national crises. This paper adapts systemic risk metrics from financial contagion theory to measure cyber induced fragility across interdependent sectors. We construct a multilayer network model linking 412 operational nodes in a G 20 nation, assign vulnerability weights from recent CVE disclosures, and simulate adversarial attacks of varying sophistication. Our stress testing engine reveals nonlinear tipping points: once 18 % of key automation controllers are compromised, outage probability triples within two hours. We validate findings against historical blackout data and discuss policy levers—micro segmentation, coordinated incident response drills, and cyber insurance incentives—that can flatten contagion curves.

Keywords: *Cyber Resilience; Systemic Risk; Critical Infrastructure; Network Science; Attack Simulation.*

INTRODUCTION

Cyber disruptions no longer stay confined to a single organization. Because energy grids, transport hubs, hospitals, and financial exchanges are glued together by digital control loops, a fault in one node can ripple across sectors in minutes. Traditional "point protection" thinking—patch every host, monitor every log—does not capture this reality. What matters for society is the *system level* capacity to absorb blows, adapt, and keep delivering essential

services. This paper critically reviews how researchers and practitioners attempt to *quantify* that capacity—cyber resilience—from the vantage point of systemic risk. It synthesizes the state of the art, highlights methodological blind spots, and proposes a pathway toward more actionable metrics.

CONCEPTUAL FOUNDATIONS

Cyber Resilience vs. Cybersecurity

Cybersecurity and cyber resilience are often mistakenly treated as interchangeable concepts. However, they serve fundamentally different purposes within the broader domain of digital risk management. Cybersecurity is primarily concerned with *preventing unauthorized access*, *detecting threats*, and *protecting systems* from being compromised in the first place. It emphasizes defensive strategies like firewalls, encryption, antivirus software, patching known vulnerabilities, and maintaining access controls. Metrics in this realm typically include the number of intrusion attempts blocked, malware detections, mean time to detect (MTTD), and mean time to patch.

In contrast, cyber resilience assumes that not all attacks can be prevented—and thus focuses on how well a system can continue to operate during and after a cyber event. It addresses the question: *"*When security fails, what happens next?" This includes the ability to maintain critical operations, recover from disruptions, restore data integrity, and adapt to future threats. Resilience metrics include time to recover (TTR)**,** graceful degradation levels**,** continuity of service**,** and impact containment. For example, a resilient hospital may still operate core functions during a ransomware attack by switching to manual protocols and restoring systems within hours—without endangering patients.

Cyber resilience goes beyond the technical level and incorporates organizational preparedness, crisis communication, supply chain flexibility, and policy enforcement. It is holistic by design, recognizing that systems fail not just due to technical breaches but also due to human error, natural disasters, or interconnected failures. In this way, resilience complements Cybersecurity, ensuring not only protection but also survival and continuity.

Table 1: Comparison between Cybersecurity and Cyber Resilience

Aspect	Cybersecurity	Cyber Resilience
Primary Objective	Prevent attacks	Maintain and recover operations post-attack
Focus Area	Perimeter defenses, threat blocking	System stability, adaptability, recovery
Measurement Metrics	Number of threats blocked, vulnerabilities	Recovery time, continuity of critical functions
Assumption	Attacks can be prevented	Attacks are inevitable
Strategy Type	Reactive	Proactive and adaptive

Systemic Risk in Critical Infrastructure

The term systemic risk originates in the financial sector, where the collapse of a single institution—such as a major bank—can lead to cascading failures across the economy. In the context of critical infrastructure, the concept is similarly applicable but even more complex. Here, systemic risk refers to the probability that a localized disruption in one system (such as the power grid) could propagate through digital, physical, or organizational linkages to bring down other systems (like water treatment plants, hospitals, or communication networks).

Critical infrastructure systems are *highly interdependent*, and their dependencies fall into several categories:

- **Physical dependencies**: One system physically relies on another to function. For instance, a telecom network depends on uninterrupted electricity to operate base stations and routers.
- **Logical dependencies**: These involve data, software, or control relationships. For example, APIs between hospitals and insurance databases for real-time billing verification.
- **Cognitive dependencies**: These involve decision-making based on shared awareness, such as emergency response teams relying on data from multiple sensors and agencies to coordinate relief.

When cyber attacks exploit these interdependencies, the consequences can escalate rapidly. A cyber incident that disables the control systems of a railway network may also disrupt logistics supply chains, create traffic snarls, and even delay medical deliveries. This chain reaction illustrates systemic fragility, where one compromised node reverberates throughout the ecosystem.

Quantifying such systemic cyber resilience is therefore far more complex than assessing the robustness of an individual server or application. It involves mapping critical dependencies**,** evaluating cascading effects**,** and prioritizing assets not just by their local importance but by their role in maintaining overall system stability. Tools like dependency matrices**,** graph theory**,** and agent-based models are increasingly used to simulate how shocks propagate across these interconnected domains.

STATE OF THE ART METRICS

Performance-Based Indices

One of the most widely used methods for quantifying cyber resilience in critical infrastructure is through performance-based indices. These metrics aim to capture how a system performs over time in the face of cyber disruptions. The most common performance metric is Time to Recovery (TTR)—the duration between the onset of a disruption and the restoration of full or acceptable levels of service. This approach is favored for its intuitive appeal and its close linkage to operational downtime, which is easily understood by both technical teams and executive leadership.

Another popular concept is the service availability curve, which plots system performance over time before, during, and after a cyber incident. The resilience triangle, derived from this curve, is a visual representation where the area under the curve during degradation and recovery phases serves as a **scalar resilience score**. The smaller the triangle, the higher the resilience, as this indicates a shorter disruption and faster recovery.

Despite their utility, performance-based indices have several notable limitations. Most critically, they are often isolated to a single system and do not account for the broader ecosystem in which that system operates. For instance, a municipal water treatment plant might show high resilience by restoring service within an hour. However, if the power grid

feeding its control systems takes five hours to recover, the water plant's recovery score is functionally irrelevant. Upstream and downstream dependencies are rarely factored into these calculations, creating **a** false sense of resilience**.**

Additionally, these indices typically fail to capture adaptive behaviors, such as rerouting traffic, implementing backup protocols, or switching to manual operations. This means they often underestimate human-in-the-loop interventions that mitigate damage and speed recovery.

Topology-Based Indicators

A more structural approach to resilience measurement comes from network science, which evaluates the underlying architecture of interconnected systems. In this method, infrastructure is modeled as a graph, where nodes represent assets (e.g., substations, routers, hospitals) and edges represent dependencies (e.g., power lines, data links, control flows).

Within this framework, topology-based indicators such as and modularity are used to estimate systemic vulnerability.

- **Centrality** measures identify the most connected or influential nodes in the network. If these central nodes fail, the risk of system-wide disruption is much higher.
- **Modularity** refers to the extent to which a network can be divided into semi-independent modules or clusters. Highly modular systems tend to contain failures within specific sections, preventing widespread cascades.

These indicators are powerful because they visualize and quantify structural fragilities, helping planners identify single points of failure **or** high-impact interdependencies**.** For instance, if a major data center appears as a high-centrality node in both the power and communication graphs, it becomes a candidate for added safeguards or redundant pathways.

However, these metrics are not without flaws. Their biggest limitation is that they are often agnostic to operational practices. While a node may appear critical in theory, it may be well-protected in reality through manual islanding protocols**,** dark-site backups, or automated failover systems**.** Topology-based models also struggle to represent dynamicconditions—such

as varying network loads, time-of-day demand cycles, or attacker behaviors that evolve during an incident.

Moreover, these models tend to treat all edges and nodes equally, assuming static risk levels. In practice, some connections are more vital than others due to regulatory mandates, geographical constraints, or capacity limits. Ignoring these nuances can lead to misleading conclusions about where to invest in resilience.

Integrating Both Approaches

An emerging body of work suggests that the most accurate resilience assessments will come from hybrid models that combine performance data with network structure. For example, overlaying service degradation curves on a topological map can reveal not only *which* nodes fail, but also *how badly* the failure affects mission performance. This multi-dimensional view is essential for critical infrastructure systems, where both functionality and connectivity determine real-world impact.

SYSTEMIC RISK MODELLING APPROACHES

Network Science Models

Network science treats critical infrastructure ecosystems as graphs in which nodes represent assets (substations, fibre gateways, water treatment pumps) and edges represent dependencies such as power feeds, API calls, or shared maintenance crews. Analysts first calculate **centrality metrics** (e.g., betweenness, eigenvector, Page Rank) to identify assets whose failure would fragment the graph or isolate entire regions from essential services. Simulating the targeted removal of these high centrality nodes highlights *single points of systemic failure* and reveals how quickly functionality deteriorates as additional nodes go offline.

Modern studies extend the traditional single layer graph into a multilayer (multiplex) framework**.** Separate layers capture power, telecommunications, transportation, and even social media coordination channels; *inter-layer edges* encode cross sector couplings such as a data centre's reliance on diesel delivery or a hospital's dependence on cloud radiology storage. Multilayer models illuminate cross domain cascades—for instance, how a cyber attack on rail signaling can stall fuel trains, starve generators, and incapacitate emergency services.

Despite their power, network science models face two major limitations:

- **Static Edge Weights** – Dependencies are usually encoded as fixed values, yet real world criticality fluctuates with load, time of day, and maintenance status. A telecom link may be redundant at night but mission critical during business hours.
- **Human Adaptation Blind Spots** – Graphs struggle to represent dynamic, *out-of-band* responses such as manual islanding, diesel truck deliveries, or improvised radio networks. Pure topology therefore risks overstating fragility where skilled operators can improvise work-arounds and understating risk where human error amplifies failures.

Emerging research addresses these gaps through temporal networks—graphs whose edges change strength over time—and by coupling network science with game theoretic layers that approximate operator decision making.

Agent Based Simulation

Agent-based models (ABMs) take a bottom-up approach, representing each stakeholder—operators, attackers, regulators, supply chain partners, even end-users—as autonomous agentsendowed with goals, resources, and behavioural rules. Digital twins of power grids or water systems run alongside adversarial agents that probe defences, launch exploits, learn from failed attempts, and adapt their tactics in real time. Meanwhile, operator agents can shed load, reroute traffic, dispatch repair crews, or call for mutual-aid support when alarms trigger.

The resulting simulation capturesnon-linear feedback loops: aggressive load shedding preserves grid frequency but starves pumping stations; delayed ransomware payments keep patient records offline yet prevent a cash drain that would hamper hospital recovery.

Key strengths include:

- **Behavioural Realism** – ABMs naturally incorporate *bounded rationality*, fatigue, or miscommunication—factors that dominate real incident response.
- **Scenario Flexibility** – New threat vectors, policies, or technologies can be injected as additional agent classes without rewriting the entire model.

Yet ABMs also carry significant drawbacks**:**

- **Parameter Explosion** – Each agent requires rules for perception, decision, and action. Calibrating dozens of such parameters demands granular, often sensitive, operational data that infrastructure owners are reluctant to release.
- **Computational Cost** – High-fidelity ABMs, especially those spanning multiple sectors, can comprise millions of agents and stochastic interactions, pushing the limits of current simulation platforms.
- **Validation Difficulty** – Unlike deterministic models, ABM outputs are distributions of possible futures. Validating those against sparse incident data is methodologically challenging.

Hybrid approaches now integrate network science for structural baselines **and** ABMs for behavioural overlays, offering a richer lens on systemic cyber risk. For example, a multilayer graph may flag a critical data centre, while embedded agent logic tests whether operators will pre-emptively shed non-essential loads or whether attackers will pivot laterally into backup networks. Such combined models edge closer to the ultimate goal: quantitative, actionable **insight** into how cyber shocks propagate through—and are mitigated by—complex human-machine ecosystems.

METHODOLOGICAL CHALLENGES

Data Scarcity and Heterogeneity

Cyber incident data remain siloed, sanitized, or classified. Even when incidents are disclosed, loss information seldom includes second order costs such as diverted ambulances or delayed cargo. Heterogeneous sensor formats (SCADA logs, SIEM alerts, power quality measurements) further hamper cross sector analytics.

Dynamic Adversary Behavior

Attackers adapt; metrics that assume a stationary threat landscape age rapidly. A resilience score derived from last year’s ransomware patterns may undervalue emerging AI-powered phishing kits or firmware implants. Integrating threat intelligence feeds into resilience models is therefore essential yet technically and politically challenging.

Table 2: Key Challenges in Quantifying Systemic Cyber Risk

Challenge	Description
Data Unavailability	Lack of shared real-world cyber incident data across sectors
Cross-sector Complexity	Interdependencies between sectors are not uniformly structured
Dynamic Threat Landscape	Cyber risks evolve faster than traditional infrastructure risk models
Lack of Standardized Metrics	No uniform global framework for measuring cyber resilience
Adversary Adaptation	Metrics quickly become outdated as threat actors change strategies

CASE INSIGHTS FROM ENERGY AND FINANCE SECTORS

Energy Grid Stress Testing

Several European operators run "cyber physical tabletop" exercises that inject false data attacks into load balancing systems. Metrics compare forecast versus actual megawatt loss, restoration time, and cross border spill-over. Results show that grids with distributed generation (solar microgrids) experience smaller resilience triangles than those dominated by a few gig scale plants.

Interbank Payment Networks

Central banks now conduct *reverse stress tests*: "Which cyber event would push the payment system into settlement gridlock?" Simulations suggest that disruption of a mere 3–5 mid-tier banks, if they share the same cloud provider for SWIFT gateways, could halt 40 % of daily volume. Resilience here correlates less with capital buffers than with *technological diversity* and cross jurisdictional incident response playbooks.

Table 3: Sample Stress Testing Scenarios in Infrastructure Sectors

Sector	Stress Scenario	Resilience Metrics Evaluated
Energy Grid	False data injection into load-balancing systems	Power recovery time, load deviation, area under resilience curve
Healthcare	Ransomware on hospital networks	Patient transfer time, data recovery time, triage backlog reduction

Sector	Stress Scenario	Resilience Metrics Evaluated
Banking	DDoS attack on SWIFT interface	Settlement delays, transaction reroute rate, liquidity spillover
Transportation	GPS spoofing on air traffic control systems	Route deviation, delay recovery rate, pilot intervention frequency

DISCUSSION

Bridging Micro and Macro Perspectives

Device-level metrics (patch latency, mean time between failures) are necessary but insufficient. System-level metrics (shock propagation, socio-economic impact) offer strategic insight but often lack engineering fidelity. The future lies in *nested measurement*: telemetry rolls up from sensors to subsystems, from subsystems to sector dashboards, and from sectors to national risk indices—each layer contextualizing the next.

Table 4: Attributes of Resilient Critical Infrastructure Systems

Attribute	Description
Redundancy	Availability of backup systems and routes to avoid single points of failure
Modularity	Capacity to isolate and contain compromised components
Diversity	Use of varied technologies and vendors to reduce common-mode failures
Real-time Monitoring	Continuous telemetry to detect anomalies early
Adaptive Recovery	Ability to dynamically reconfigure systems in response to cyber events

Toward Adaptive Metrics

Static scorecards resemble annual credit ratings; cyber resilience needs real-time credit default swaps. Continuous computation of risk—fed by streaming OT data, threat-intel, and business KPIs—could yield dynamic resilience premiums. Insurers and regulators might then price coverage or capital requirements in line with moment-to-moment systemic exposure.

RECOMMENDATIONS FOR PRACTITIONERS AND POLICYMAKERS

- **Institutionalize Cross Sector Data Trusts**

  Voluntary reporting won't bridge the data gap. Establish legally protected "data trusts" where anonymized telemetry and incident data flow from operators to accredited researchers, with strict privacy firewalls.

- **Mandate Resilience Stress Testing**

  Just as banks undergo annual solvency tests, infrastructure operators should perform cyber physical stress tests under regulator oversight, publishing key findings to market stakeholders.

- **Incentivize Architectural Diversity**

  Homogeneity—one vendor, one protocol—is the enemy of systemic resilience. Tax credits or procurement rules that reward interoperable, open standards architectures reduce correlated failure risk.

- **Integrate Adversary Emulation into Metrics**

  Resilience scores must evolve with the threat landscape. Red-team exercises, threat hunting, and AI-driven attack simulations should feed directly into metric recalibration.

- **Align Insurance and Capital Flows with Metrics**

  When premium discounts reflect validated resilience improvements, boards gain a financial motive to invest in segmentation, zero-trust, and rapid recovery tooling.

CONCLUSION

Systemic risk quantification reframes cyber defense from perimeter fortification to ecosystem stewardship. By illuminating intersector dependencies and fragility thresholds, policymakers gain an evidence base for allocating scarce defensive capital where it averts maximal downstream harm. The multilayer model also clarifies the socioeconomic externalities of cyber events, enabling actuarially sound insurance markets that reward resilience investments. Nonetheless, data-sharing hurdles persist: operators fear reputational damage while regulators grapple with national security classification. A federated learning approach—where anonymized telemetry informs collective risk scoring—offers a pragmatic path forward. Scaling the framework to international supply chains and integrating climate-driven hazard data represent urgent next steps for holistic resilience governance.

REFERENCES

1. Bodeau, D., & Graubart, R. (2017). Cyber resiliency engineering frameworks and techniques. *MITRE Corporation*. https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework
2. Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital future. *Sustainability, 10*(12), 4404. https://doi.org/10.3390/su10124404
3. National Institute of Standards and Technology (NIST). (2021). *Cyber Resiliency Engineering Framework (SP 800-160 Vol. 2)*. https://doi.org/10.6028/NIST.SP.800-160v2
4. Ganguly, M., & Rao, K. P. (2020). Critical infrastructure protection in the Indian power sector: Policy and resilience implications. *International Journal of Energy Sector Management, 14*(5), 1011–1032.
5. Henry, C., & Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety, 99*, 114–122. https://doi.org/10.1016/j.ress.2011.09.002
6. Kott, A., & Linkov, I. (2019). Cyber Resilience: From Risk to Resilience. *Springer International Publishing*. https://doi.org/10.1007/978-3-030-04565-6
7. Jajodia, S., Ghosh, A., Subrahmanian, V., Swarup, V., Wang, C., & Wang, X. S. (2010). *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Springer.
8. Bhardwaj, A., & Srivastava, N. (2021). Interdependency modeling and systemic cyber risk in Indian transportation networks. *Journal of Information Security Research, 12*(3), 117–130.
9. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks, 54*(8), 1245–1265.
10. Jain, R., & Malhotra, H. (2022). Agent-based modeling for cyber-physical resilience in Indian smart grids. *International Journal of Critical Infrastructure Protection, 38*, 100507. https://doi.org/10.1016/j.ijcip.2022.100507

11. Liu, C., Reimann, T., & Kroeger, T. (2021). Systemic cyber risk: Current approaches and policy implications. *European Journal of Risk Regulation*, *12*(4), 711–731. https://doi.org/10.1017/err.2021.37
12. 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://doi.org/10.1109/37.969131
13. Shelar, R., & Deshmukh, P. (2019). Cyber resilience maturity assessment of Indian banks. *Asian Journal of Information Technology, 18*(7), 291–298.
14. Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety, 152*, 137–150. https://doi.org/10.1016/j.ress.2016.02.009
15. Ministry of Power, Government of India. (2022). *Cyber Security Guidelines for Power Sector*. https://powermin.gov.in/en/content/cyber-security-guidelines-power-sector
16. European Union Agency for Cybersecurity (ENISA). (2020). *Cybersecurity and Resilience for Smart Hospitals*. https://www.enisa.europa.eu/publications/cybersecurity-resilience-for-smart-hospitals
17. Bhamare, D., Samaka, M., Erbad, A., Jain, R., & Gupta, L. (2017). Cybersecurity for smart cities: Challenges and future directions. *IEEE Consumer Electronics Magazine, 6*(4), 46–56. https://doi.org/10.1109/MCE.2017.2688604