INTERNET RESILIENCE INSTITUTE

BUILDING GLOBAL RESILIENCE

Strengthening the Internet's Capacity to Withstand Disruption

Internet Resilience Forum and Experts Workshop Report
November 2025

The Marconi Society

Table of Contents

About the Marconi Society

The Marconi Society builds communities of leaders and stakeholders that are at the forefront of emerging technology so that together we can create a more connected and sustainable world.

For over five decades, we have celebrated the innovators, both established and emerging, who have shaped our connected world. The Institutes provide platforms to convene our network of visionaries to collaborate on identifying, assessing, and recommending ways to ensure that emerging technologies benefit society.

About the Institute Forums

The Institute Forums bring together experts in Advanced Wireless, AI, and Internet Resilience to explore emerging opportunities and challenges. Each Forum fosters informed dialogue and actionable insights that strengthen the future of global connectivity.

About the IR Institute

The Internet Resilience (IR) Institute advances Internet resilience by convening global experts across technical, industry, and policy domains to identify challenges, foster collaboration, and drive actionable solutions for a secure, reliable, and accessible digital future.

The invitation-only, IR Experts Workshop was held at ICANN Headquarters in Los Angeles, CA on November 13, 2025. The IR Forum was held at the UCLA Meyer and Renee Luskin Conference Center in Los Angeles, CA on November 14, 2025. The findings presented herein are drawn directly from participants at the IR Experts Workshop and IR Forum. AI tools were employed to support the organization of these discussions. This report was reviewed for accuracy and context by the IR Institute team and IR Advisory Council.

2025 Year in Review

One year ago, the Internet Resilience (IR) Institute began with a straightforward idea: bring together a diverse community of experts to better understand how to strengthen the resilience of the global Internet. In twelve months, that idea has matured into an initiative that is generating original, practical tools for operators and businesses.

The Institute's work was sparked by a provocative question posed at its inaugural workshop at the National Academy of Sciences (NAS) in Washington, DC in November 2024:

If the Internet suffered a global failure, what would be needed for a reboot?

This question exposed that Internet resilience is ultimately a global coordination problem, not just a technical one, and it is deeply rooted in governance and shared accountability across sectors. The Institute's work, now widely referenced in Internet governance and technical circles, are grounded in key activities, including:

- Critical briefings within the 2024 IR Report presented to the U.S. Council for International Business (USCIB) Digital Policy Committee.
- Engaged with stakeholders at major global meetings, including ICANN Prague, ICANN Dublin, and in other fora, reinforcing the Institute's presence as a trusted convener.
- Hosted a high-profile session at the 20th Annual IGF Norway, "*Internet Resilience: Securing a Stronger Supply Chain*", highlighting systemic interdependence, electricity-digital infrastructure loops, and operational risk.
- Secured a workshop at the WSIS+20 High-Level Event in Geneva, reinforcing Resilient Infrastructure for a Sustainable Future.
- Held an online *Global Briefing* addressing pressing global challenges in Internet resilience and to set the stage for collaborative action through the Institute's working groups.
- Convened global leaders at the 2nd Annual IR Institute Experts Workshop and Forum from infrastructure providers, hyperscalers, financial institutions, utilities, and public-interest organizations to examine systemic vulnerabilities and produce practical tools toward a more resilient digital future.

The IR Institute's two flagship projects, the *Business Resilience Guide* and the *Life of a Packet Mapping Exercise*, demonstrate the importance of multi-stakeholder partnerships, with continued expert engagement and renewed corporate funding, to continue positive momentum.

The Institute's progress has elevated the Marconi Society's standing in global resilience discussions. Its convening capability, combined with practical tools and credible expert leadership, positions the Marconi Society as a trusted actor able to bridge technical, operational, and governance communities.

Executive Summary

The Marconi Society IR Institute's 2025 Experts Workshop and IR Forum meetings represent the culmination of a year-long collaborative effort to address critical vulnerabilities in global Internet infrastructure. Building upon an initial gathering at the NAS in Washington DC and sustained work through two dedicated working groups (IR Supply Chain Mapping and Hyperscaler Engagement), both meetings united operational, technical, policy, and governance leaders to translate diverse expertise into actionable resilience strategies. Their insights underscore that **resilience must be treated as a foundational design principle**, not a secondary consideration. Internet resilience is no longer simply about recovering from failures. It is about designing systems that can withstand and adapt to disruption. The IR Experts Workshop and IR Forum were held under Chatham House Rule, with the exception that participants can be identified, though no attributions are to be made to individuals or entities.

The discussions revealed six key themes recommended for developing practical, industry-usable outputs while strengthening cross-sector relationships essential to Internet stability:

- **Resilience failures come from hidden dependencies, not from single systems breaking.** Failures tend to propagate through hidden, cross-sector dependencies (power, cloud, logistics, governance, people). Making these dependencies visible is foundational to resilience.

- **Practical tools matter more than abstract principles**. Effective resilience planning should be grounded in realistic scenarios rather than theoretical extremes, with particular attention to usable tools that others can learn from and apply.

- **Resilience only exists if it is tested and rehearsed**. Redundancy, backups, governance processes, and contracts fail if they are not exercised. Stress-testing, drills, and failure rehearsal are essential, moving resilience from aspiration to operational practice.

- **Learning from practice**. Resilience improves when lessons from practice are captured, shared, and institutionalized.

- **Human and institutional failure matter as much as technical failure.** Internet resilience demands more than technology; it requires people, institutions, incentives, and governance. Skills shortages, fatigue, regulatory misalignment, and institutional failure can take down systems as effectively as technical faults.

- **Raising awareness about Internet resilience remains critical.** No single actor can address systemic Internet risk. Cross-sector expansion and sustained partnerships are needed to connect sectors, disciplines, and communities.

The IR Institute occupies a singular position to address these critical themes through operational credibility, multistakeholder governance expertise, and serving as a neutral, cross-sector convening power. This unique positioning enables the IR Institute to serve as the essential coordination layer - translating diverse perspectives into shared norms, facilitating cross-sector information sharing, and

producing recommendations that respect the Internet's distributed governance while addressing its systemic vulnerabilities.

Key Themes and Recommendations

Theme 1. Resilience failures come from hidden dependencies, not from single systems breaking.

The Internet's resilience depends not merely on technical infrastructure, but on complex, often unmapped dependencies spanning power grids, financial systems, cloud platforms, and supply chains. In early 2025, millions of people lost electricity across Portugal, Spain, and parts of France, effectively halting operations for some in southwestern Europe for hours. Initial blame focused on renewable energy. However, experts later found multiple triggers took place shortly before the blackout occurred.

Multiple organizations have experienced operational paralysis when hyperscale providers suffered outages. Cascading power failures highlight how Internet operators remain vulnerable to systemic events beyond their direct control. For instance, organizations acknowledged that resilience planning routinely overlooked how payroll systems and banking depend on network connectivity (many had not verified with banks how payments would continue during connectivity loss). Ensuring financial continuity plans extend beyond mere technical considerations to encompass the human and operational dimensions of extended outages is critical.

To address these cascading vulnerabilities, there is a need for greater visibility into dependencies as demonstrated by the IR Institute's Supply Chain Mapping Working Group's *Life of a Packet Mapping Exercise*. The *Mapping Exercise* emphasized making dependencies visible in ways that enable coordination, testing, and dialogue across sectors. Additionally, information-sharing mechanisms between Internet operators, power utilities, financial institutions, and cloud providers are encouraged to ensure coordinated incident response, while regular dependency risk assessments with mitigation plans should become standard practice.

Theme 2. Practical tools matter more than abstract principles.

Today's systems are riddled with circular dependencies. Power grids rely on digital controls; digital controls rely on connectivity; connectivity relies on power. Similar loops exist across software, cloud services, routing, content delivery, and security. These loops mean that small failures propagate in unexpected ways. Understanding, mapping, and mitigating these circular dependencies is essential. The *Business Resilience Guide* and *Life of a Packet Mapping Exercise* demonstrate modern resilience planning.

The IR Institute's Hyperscaler Engagement Working Group set out to address the question: how can the operational discipline of hyperscalers be translated into practical, usable guidance for small and medium-sized enterprises (SMEs)? Unlike large organizations with CISOs, engineering teams, and mature continuity processes, most SMEs are highly exposed to outages, misconfigurations, supply-chain failures, or local infrastructure disruptions—vulnerabilities that can cascade across entire economic networks, given SMEs' central role in global productivity.

In response, this working group developed a guide distilling hyperscaler-grade resilience principles into accessible, actionable steps organized around four elements: awareness of Internet-layer dependencies,

an impact–likelihood risk matrix with scenario tools, practical mitigation measures, and real-world case studies demonstrating how SMEs can strengthen continuity. Several key insights emerged from hyperscaler experiences and adapted for the SME context:

(1) Concentration risk remains largely invisible. Many SMEs believe they are protected by redundancy, but in practice their "independent" connections often share the same physical trench or upstream infrastructure. This creates hidden single points of failure that only become obvious during a crisis.

(2) Resilience requires testing. A backup connection, a mirrored server, or a cloud failover plan is meaningless if it has never been exercised. Hyperscalers routinely test failure scenarios; SMEs rarely do.

(3) Distributed models increase resilience. Workloads, data storage, and connectivity pathways benefit from diversification, not only for performance but to mitigate systemic risk.

(4) Cloud interoperability remains a barrier. Despite the rhetoric of multi-cloud strategies, moving workloads across providers remains deeply challenging. Standards for interoperability are still immature, limiting SMEs' ability to adopt resilient architectures.

(5) Transparency builds trust. Industry best practices should include outage disclosures, detailed post-incident analyses, and explicit corrective actions. A culture of transparency strengthens resilience ecosystems by allowing others to learn from each failure.

The IR Institute's Supply Chain Mapping Working Group set out to address another unique question: is it possible to make the Internet's hidden interdependencies visible to the many actors whose decisions shape its resilience? Working group members recognized that many of those who rely on the Internet every day often do not see themselves as part of a broader resilience ecosystem. Individuals may understand their own systems, but not the complex layers and external infrastructures (i.e., power, cooling, logistics, cloud, governance) on which their connectivity depends.

In response, this working group built a visual model revealing cross-layer and cross-sector relationships in a way that non-specialists could intuitively grasp. The goal was to show how functional, physical, and dependency layers interact during a single Internet transaction, and where failures can propagate across them. To achieve this, this group adopted a concrete scenario: a simple Zoom call. By tracing the "life" of each packet in that call (from user device through service logic, control systems, routing layers, physical networks, and into cloud infrastructure) it quickly became apparent how complex the journey becomes. Every step involved branching paths, hidden assumptions, and deep interdependencies. Even this narrowly defined scenario moved across service, control, and transport layers and intersected with countless external systems, such as power grids, cooling systems, supply chains, logistics networks, governance frameworks, and security architectures. The resulting model organizes the system into three conceptual layers:

(1) **Upper Layer**: application behavior, service logic, user-facing functions;

(2) **Lower Layer**: routing, transport mechanisms, physical transmission;

(3) **Dependency Layer**: power, water, machinery, supply chains, governance frameworks, and other infrastructures without which the Internet cannot operate.

This model breaks new ground as the first attempt to visually integrate the Internet's functional, physical, and institutional components into a single, comprehensive framework.

Theme 3. Resilience only exists if it is tested and rehearsed.

Resilience is a multi-dependency, multi-actor challenge, which must be engineered, measured, and continually practiced across digital and physical infrastructures. Achieving resilience requires continuous testing, stronger interdisciplinary communities, collaborative regulatory engagement, and a more explicit recognition of shared vulnerabilities.

Infrastructures that once relied on single-point systems have transformed into distributed, multi-layer architectures capable of absorbing failures. This evolution forced a shift in mindset: resilience is not synonymous with redundancy. It depends on minimizing the blast radius of failures, building systems that can degrade gracefully, and replacing outdated assumptions with continuous verification and zero trust principles. An early, yet notable, example includes each satellite as a single point of failure. If it ran out of fuel or failed, service stopped. In response, architecture shifted over time to multi-orbit, multi-band constellations. Security follows a similar trajectory; once an afterthought at the end of a project plan, security and resilience today correspond to the same design problem: zero trust-style assumptions and independent decision points. Heavy reliance on automation and observability are desired to detect configuration drift and silent failures. Resilience must be built into the architecture and proven through continuous testing. It cannot be assumed or proclaimed.

Resilience only exists when someone inside the organization genuinely takes ownership of the end-to-end service, rather than focusing narrowly on individual components, making resilience not just an individual concern, but a cultural and organizational one. Compliance, audits, and policy obligations may confirm rules are followed, but ultimately do not create the behaviors or situational awareness required to perform under stress. Resilience is produced through relentless internal pressure, routine stress tests, simulated outages and drills that build organizational muscle memory. Testing cannot be episodic. Organizations are strongly encouraged to routinely force failovers, conduct simulated outages, and intentionally "turn things off" to observe how people, processes, and systems behave in adverse conditions. Tension remains, however, because small suppliers (who are essential parts of the service chain) often lack the resources to participate in such tests. Yet each failure exercise uncovers new weaknesses, and each discovery is an opportunity to strengthen both the technical system and a team's operational playbook.

Theme 4. Learning from practice.

Resilience is not built solely through design, testing, or rehearsal; it is strengthened when organizations and sectors systematically learn from real-world events and ensure that hard-earned lessons do not need to be learned again. Across Internet infrastructure, as well as in mature critical infrastructures such as the power and financial sectors, experience shows that failures, whether near-misses, localized outages, or major disruptions, often recur not because solutions are unknown, but because lessons are insufficiently captured, shared, or embedded into operational practice.

Learning from practice must be treated as a core resilience function, not an informal or ad-hoc activity. In Internet operations, post-incident reviews, outage reports, and routing or cloud failure analyses already generate valuable insights. However, these lessons frequently remain siloed within individual organizations, constrained by commercial sensitivity, liability concerns, or lack of trusted forums for exchange. As a result, similar misconfigurations, dependency failures, and coordination breakdowns continue to occur across different operators and regions.

Other critical infrastructures offer instructive parallels. In the power sector, structured incident reporting, mandatory root-cause analysis, and sector-wide dissemination of failure patterns have contributed to steadily improving grid reliability. In the financial sector, stress testing, scenario analysis, and supervisory review processes have institutionalized learning from past crises, reducing systemic blind spots over time. These sectors demonstrate that resilience improves when learning is cumulative, shared, and translated into changed behavior, standards, and governance practices.

For the Internet ecosystem, this implies moving beyond one-off postmortems toward repeatable learning mechanisms that connect technical findings to organizational decision-making, governance processes, and cross-sector coordination. Learning from practice should include not only technical root causes, but also human, institutional, and policy factors such as unclear accountability, regulatory friction, or breakdowns in cross-operator communication that shape incident outcomes. In fact, in recent disruptions with Cloudflare and ACS such an approach has been demonstrated.

The IR Institute is well positioned to support this shift by providing neutral, trusted environments in which experiences can be analyzed without attribution, patterns can be identified across incidents, and lessons can be translated into practical guidance. By fostering cross-sector dialogue that connects Internet infrastructure operators with peers from energy, finance, and other critical infrastructures, the Institute can help ensure that resilience knowledge compounds over time, reducing the likelihood that the same failures recur and strengthening collective preparedness for future disruptions.

Theme 5. Human and institutional failure matter as much as technical failure.

Internet resilience relies on deep linkages between digital, physical, and human systems. Modern Internet and service operations rest on multiple unseen layers: cloud platforms, routing infrastructure, data centers, power grids, cooling systems, water supplies, logistics chains, and even the mobility of people responsible for managing critical processes. Organizations typically understand only their immediate operational environment, while remaining unaware of upstream components such as storage backends, shared cloud services, or third-party vendors. Operational resilience is impossible without clear visibility into the full dependency stack and an honest reckoning with how tightly these systems are intertwined.

What's more, even highly redundant systems can fail if human operators have not rehearsed crisis procedures or if backup mechanisms have not been exercised under realistic conditions. Misconfigurations, stalled failover paths, insufficiently tested backups, and procedural bottlenecks frequently determine the outcome of an incident. Humans often provide the flexibility and improvisation needed to navigate situations that automation cannot handle, particularly when physical presence, manual overrides, or creative workarounds are required. Technology cannot replace human judgment, especially under unexpected constraints; resilience planning must fully incorporate human roles, limitations, and capabilities.

Resilience challenges are magnified by differing operational cultures and timelines across sectors. Some environments prioritize reliability, safety, and regulatory compliance; others emphasize agility, rapid deployment, and iterative change. These contrasting rhythms can complicate coordination, even as interdependencies deepen. Especially considering energy demand from high-density compute workloads, the growing dependence of power systems on digital monitoring, and the dependence of digital systems on stable electricity. Load growth tied to AI and data centers is reshaping planning assumptions, while regulatory frameworks often struggle to keep pace with emerging needs. Cultural and temporal mismatches between sectors create new vulnerabilities, particularly as physical infrastructure becomes increasingly dependent on digital infrastructure, and vice versa.

Theme 6. Raising awareness about Internet resilience remains critical.

Raising awareness about Internet resilience represents far more than an academic exercise, it addresses a fundamental gap between society's profound dependence on Internet infrastructure and its dangerous underestimation of systemic vulnerabilities that could lead to significant failures affecting billions of users. The modern global economy, emergency services, healthcare delivery, financial systems, and democratic institutions operate under the assumption of continuous Internet availability, yet few organizational leaders, policymakers, or citizens comprehend the fragile interdependencies that underpin this critical infrastructure or the cascading consequences when components fail. Under-funded prevention initiatives create a perilous illusion of preparedness while leaving genuine vulnerabilities unaddressed; organizations may develop resilience plans that fail to account for second-order dependencies like payroll continuity during extended outages, invest in expensive but operationally meaningless protections against theoretical threats while ignoring realistic attack vectors, or implement fragmented approaches that protect individual components while leaving systemic weaknesses exposed.

The asymmetry between prevention costs and incident consequences is staggering: comprehensive supply chain mapping, cross-sector coordination protocols, and distributed resilience investments require sustained multi-million dollar commitments, yet a single cascading identifier system failure or coordinated infrastructure attack could generate economic losses measured in billions of dollars per day, disable emergency services for millions of people, and undermine public confidence in digital systems that modern society cannot function without.

Without adequate investment in prevention, awareness-raising efforts become hollow exercises that identify risks without enabling meaningful action, while the Internet community's distributed governance model—though powerful for coordination—lacks mechanisms to compel resource allocation toward unglamorous but essential resilience measures. Reactive responses to incidents remain well-funded and visible. Preventative work, such as training, best practices, and system design, remains consistently under-resourced. The IR Institute and its stakeholders are working to shift that dynamic.

Summary and Conclusions

The Internet's resilience depends not on any single actor or technology but on the interconnected health of technical systems, supply chains, institutional practices, and human coordination. This initiative's power lies in its multistakeholder foundation: bringing together operational expertise, policy perspective, and governance experience to produce practical, actionable guidance. No actor can address systemic risk alone; collective preparedness must become a deliberate, structured priority supported by cross-sector cooperation.

Resilience efforts should focus first on sectors where failure is catastrophic: energy, water, finance, healthcare, core communications, and critical industrial systems. The pace of preparedness is no longer keeping up with the pace of risk. This gets harder with accelerating geopolitical shocks and interdependencies deepening. Even highly resilient cloud platforms cannot shield organizations from their own hidden dependencies, making it essential to question assumptions about supply chains and shared infrastructure. This underscores that resilience is ultimately human-centered, which heightens expectations for transparency when things go wrong. Trust grows when institutions openly communicate during incidents rather than closing ranks, and organizational structures must support this behavior. Institutional culture, incentives, and clarity of responsibility are as important as technical safeguards in determining whether services withstand or fail under stress. Success requires moving beyond theoretical scenarios to realistic planning, from isolated organizational efforts to coordinated cross-sector action, and from reactive responses to proactive norm-setting.

Long-term resilience requires more than preparedness; it requires learning. Systematic learning from incidents and near-misses within Internet infrastructure and across interdependent sectors such as power and finance ensures that failures do not need to be relearned. Embedding such learning loops into operational, institutional, and governance practices allows resilience to accumulate over time rather than reset after each disruption.

The recommendations presented here offer a roadmap for distributed resilience building that respects the Internet's architecture while addressing its systemic vulnerabilities. The work ahead requires sustained commitment, resource investment, and willingness to challenge assumptions about dependencies, threats, and responsibilities. Yet the alternative—continued fragmented approaches to resilience—risks significant failures with global consequences. This initiative represents a critical step toward ensuring the Internet's stability, security, and availability for the billions who depend on it daily.

IR Experts Workshop Participants and IR Forum Speakers

Fiona Alexander, Distinguished Fellow and Professor, American University

Maarten Botterman, Director, GNKS Consult BV

Vinton Cerf, VP/Chief Internet Evangelist, Google

Andrew Coward, Principal Consultant, Kirin Solutions

John Crain, SVP, Chief Technology Officer, ICANN

Steve Crocker, President & CEO, Edgemoor Research Institute

David B. Cross, CISO, Atlassian

John Curran, CEO, ARIN

Brian Cute, CEO, Global Cyber Alliance

Chris Earnshaw, Former Group Engineering Director and CTO

Kyle Gilgan, CTO, Offsite

Pablo Hinojosa, Strategic Advisor, Marconi Society

John Janowiak, President and CEO, Marconi Society

Pat Kane, SVP, Naming Services, Verisign

Victor Kuarsingh, Managing VP, Capital One Financial

Ram Mohan, Chief Strategy Officer, Identity Digital

Nancy Morgan, Strategic Advisor, Cantellus Group

Paul Moroney, VP of Security Engineering, Viasat

Ramakant Pandrangi, SVP, A&E, Verisign

Radia Perlman, Fellow, Dell Technologies

Caleb Queern, Managing Director, KPMG Cyber, KPMG

Jeff Simmons, Energy Advisor

Michael Smith, Principal, Utility 2030 Leadership Collaborative

Paul Vixie, VP and Distinguished Engineer, AWS Security

Dan York, Senior Director, Online Trust & Safety, Internet Society

IR Advisory Council

We extend our gratitude to the IR Institute Advisory Council, whose leadership, vision, and partnership have been instrumental in shaping the Institute's strategic priorities. This distinguished group of experts guided the development of the IR Experts Workshop and IR Forum by ensuring session topics reflected real-world challenges and opportunities in strengthening the resilience of the global Internet.

Fiona Alexander
Distinguished Fellow
American University

Maarten Botterman
Director
GNKS Consult BV

Leo Cloutier
Zettacycle

David B. Cross
CISO
Atlassian

Brian Cute
Chief Operating Officer and Capacity & Resilience Program Director
Global Cyber Alliance

Taher Elgamal
General Partner
Evolution Equity Partners

Pat Kane
SVP, Naming and Registry Services
Verisign

Olaf Kolkman
Principal, Internet Technology, Policy & Advocacy
Internet Society

Ram Mohan
Chief Strategy Officer
Identity Digital

Mark Nottingham
Standards Lead
Cloudflare

Dan York
Senior Director, Online Trust & Safety
Internet Society

Marconi Society IR Institute Contacts

John R. Janowiak
President and CEO
john@marconisociety.org

Flora Tromelin
VP for International Engagement
ftromelin@marconisociety.org
WhatsApp: +1 480 828 6064

Marina Pappas
Institute Director
mpappas@marconisociety.org
WhatsApp: +1 262 888 9820

Yeimidy Lagunas
Director, Communications and Membership
ylagunas@marconisociety.org
WhatsApp: +1 224 399 7333

Jaymee Bohannon
Executive Relations
jbohannon@marconisociety.org