WSIS FORUM 2026 | 6-10 July 2026 Geneva, Switzerland

Session Outcome Document

Operationalizing Digital Resilience

GNKS Consult; Marconi Society Resilience Institute

Thursday, 9 July 2026, 15:00 – 15:45 (UTC +2)

https://www.itu.int/net4/wsis/forum/2026/Agenda/Session/235

Key Issues discussed:

- The Internet's resilience has been built over more than four decades through open standards, interoperability, distributed architectures, infrastructure diversity, and voluntary cooperation among technical, operational and policy communities. These principles have enabled the Internet to continue operating despite failures, attacks and continuous growth, providing an enduring foundation for global digital development.
- As societies become increasingly dependent on digital services, Artificial Intelligence (AI), Digital Public Infrastructure (DPI), cloud computing and global digital trade, Internet resilience becomes the foundation for creating justifiable trust in the digital society. Trust must be earned through demonstrable reliability, continuity and resilience—not assumed.
- Internet resilience ultimately exists to ensure that people, businesses and governments can reliably achieve their objectives through digital services. Delivering this outcome depends on a complex ecosystem of cooperating networks, Internet infrastructure, cloud platforms, power systems, supply chains, standards organizations and governance arrangements that often remain invisible to end users.
- The Life of a Packet demonstrates that even the simplest digital interaction depends on numerous technical, operational and institutional components working together. Understanding these dependencies—including those deep within routing, DNS, transport infrastructure and their supporting services—is fundamental to identifying systemic risks, preventing cascading failures and strengthening resilience across the digital ecosystem. The framework illustrates that resilience extends well beyond the visible application layer to include critical supporting infrastructures such as power, security, supply chains, finance and governance.
- A recurring finding from the Business Resilience Guide's engagement with organizations: many believe they have redundancy, but their "independent" connections often share the same physical trench, upstream provider, or power source, which are invisible until the moment of failure. Redundancy is not resilience if the underlying dependencies are shared. The Guide operationalizes this through four sequential steps adapted from hyperscaler-grade practice for organizations without dedicated continuity teams: assessing availability needs, modeling risk through scenario mapping, building a contingency plan, and establishing governance through named ownership and regular testing.

- As practical contributions to implementing the WSIS Action Lines and the Global Digital Compact, the session will present the Marconi Society Internet Resilience Institute's two flagship Phase 1 outputs: the Life of a Packet Mapping Framework, providing a common model for understanding Internet dependencies, and the Business Resilience Guide, translating resilience practices developed by hyperscale infrastructure providers into practical guidance for SMEs and other organizations. Both resources are intended as living frameworks and are offered openly to the global community for continued refinement through broad multistakeholder participation.
- Justifiable trust must be engineered by design and sustained through operational excellence. This requires diversity of infrastructure and suppliers, interoperability, optionality in network paths and services, avoidance of circular dependencies, continuous monitoring, resilience testing, operational preparedness and ongoing evaluation of hidden technical, operational and geopolitical dependencies. Practical examples include increasing geographic diversity of critical infrastructure, reducing dependency on single providers, and designing architectures that favour long-term resilience over short-term efficiency.
- Emerging developments—including AI-enabled cyberattacks, cloud concentration, edge computing, Internet of Things deployments and the transition to post-quantum cryptography—introduce new dependencies and attack surfaces. These disruptions are already occurring. These developments reinforce the need to evolve resilience practices while preserving the Internet's open, interoperable and collaborative architecture.
- Effective resilience models must also reflect human realities. Failure scenarios experienced by mobile-first users, young people, informal economies and underserved communities often differ fundamentally from those assumed in enterprise environments. A resilience framework is only as complete as the failure scenarios against which it has been tested. Incorporating these lived experiences is therefore essential to building resilience that serves all Internet users.

Key Outcomes of the session

- Recognition that the Internet's resilience has been achieved through decades of collaborative engineering, distributed design, open standards and multistakeholder cooperation, providing valuable lessons for future digital development.
- Shared understanding that Internet resilience is a prerequisite for creating justifiable trust in the digital society, and should therefore become an explicit consideration in implementing the WSIS Action Lines, the Global Digital Compact and emerging AI governance frameworks.
- Recognition that resilience depends not only on sound architecture and standards, but equally on the expertise, operational practices and continuous cooperation of Internet operators responsible for delivering reliable Internet services every day.
- Recognition that voluntary, measurable frameworks, such as the Business Resilience Guide's four-step model (assess, model, plan, own and test), give organizations of any size a concrete entry point for implementation, directly responsive to the session's goal of advancing measurable resilience approaches within national digital strategies.
- Increased awareness that creating justifiable trust requires understanding and managing hidden dependencies across technical infrastructure, organizations and users, including reducing concentration risks through diversity, optionality and resilience-by-design.
- Presentation and public availability of the Internet Resilience Institute's Phase 1 outputs—the Life of a Packet Mapping Framework and the Business Resilience Guide—as practical resources for governments, infrastructure operators, businesses, researchers, academia and civil society.

Participants will be invited to contribute practical experience and additional use cases as these resources evolve through the Institute's Phase 2 activities.

- Strengthened dialogue between governments, industry, standards organizations, the technical community, academia, civil society and youth representatives on advancing Internet resilience as an implementation priority for WSIS+20 and beyond.

Key Recommendations and Forward-Looking Actions

- Continue strengthening the architectural principles that have made the Internet resilient, including open standards, interoperability, distributed architectures, infrastructure diversity and voluntary multistakeholder cooperation.
- Embed resilience-by-design as a foundation for creating justifiable trust, reducing hidden dependencies, avoiding unnecessary concentration, increasing optionality, strengthening routing and DNS resilience, and continuously evaluating technical, operational and geopolitical risks.
- Integrate Internet resilience into the implementation of the WSIS Action Lines, the Global Digital Compact and national digital strategies, recognising resilient Internet infrastructure as foundational to AI, Digital Public Infrastructure, digital public services and sustainable digital transformation.
- Adopt ownership and testing as standard organizational practice: name a resilience owner, and require regular testing of failover and contingency plans. Resilience becomes real only when it has an owner, a test, and a learning loop - not simply a written plan.
- Expand resilience modelling and testing to incorporate both technical dependency analysis and real-world user experiences, ensuring that resilience frameworks reflect the needs of youth, mobile-first users, SMEs and underserved communities whose failure scenarios often differ from those of large enterprises.
- Strengthen collaboration between policymakers, technical standards bodies and Internet operators, ensuring that operational experience directly informs resilience policies, implementation guidance and future Internet architecture.
- Continue developing the Internet Resilience Institute's open resilience frameworks through broad international participation, encouraging governments, operators, standards bodies, industry, academia, civil society and youth to contribute practical experience, additional failure scenarios and implementation guidance as the frameworks evolve through Phase 2.

Closing Reflection

- The Internet has demonstrated remarkable resilience because it was designed as an open, distributed and collaborative system, and because it has been continuously strengthened through decades of operational excellence, engineering innovation and multistakeholder cooperation. As digital transformation accelerates and societies become increasingly dependent on AI, Digital Public Infrastructure and globally interconnected services, the challenge is not to reinvent these principles, but to extend them to new technologies, new dependencies and new users.
- Yet the same architectural resilience that protects the Internet at a global level can create a false sense of security at the organizational level: many entities assume they are protected by redundancy that, on inspection, shares a single point of failure. Translating architectural resilience into organizational survivability requires deliberate, tested, owned practice - the gap the Business Resilience Guide is built to close.

The Life of a Packet Mapping Framework and the Business Resilience Guide, developed collaboratively through the Marconi Society Internet Resilience Institute, represent practical first steps towards that

objective. They are offered to the global WSIS community as open implementation resources and an invitation to participate in their continued refinement through the Institute's Phase 2 activities. By combining resilient architecture, operational excellence, practical implementation guidance and the lived experiences of Internet users, they help translate the ambitions of the WSIS+20 Review and the Global Digital Compact into concrete actions that strengthen resilience and build justifiable trust in the digital society.

Engineering Justifiable Trust through Internet Resilience

Why this organization of the take-aways: the narrative that I plan to make explicit in my moderator's framing is that each speaker represents one stage in the resilience lifecycle:

- Vint Cerf: The architectural principles that have made the Internet resilient.
- Victor Kuarsingh: Understanding dependencies through the *Life of a Packet*.
- Ram Mohan: Turning resilience into practical implementation through the *Business Resilience Guide*.

Followed by comments from stakeholders in the chain:

- Philippe (Orange): Operational excellence: how resilience is maintained every day.
- Moritz Müller (SIDN): Engineering resilience by design.
- Katarina (SCION): Building diversity and optionality into future Internet architectures.
- Raneem Zitoun: Ensuring resilience is validated against the lived experiences of diverse users.

This progression, from architecture to dependencies to implementation to reflections from operations, engineering, and society demonstrates that Internet resilience is not solely a technical issue or a policy issue, but a continuous lifecycle of design, operation, learning and improvement that creates justifiable trust in the digital society. I believe that framing will resonate strongly with the implementation focus of both the WSIS+20 Review and the Global Digital Compact.