After Doha: Can Global Cyber Diplomacy Make Digital Infrastructure Resilient?

The ITU’s November 27 conference placed resilient networks, AI and connectivity on its agenda. The challenge now is to turn diplomatic consensus into funded, inclusive and accountable capacity.

Vladimir Tsakanyan, Ph.D. · Center for Cyber Diplomacy and International Security

November 29, 2026

By Vladimir Tsakanyan, Ph.D., Center for Cyber Diplomacy and International Security.

Cover image: AI-generated conceptual illustration.

The world’s digital infrastructure rarely becomes the subject of a diplomatic summit until it fails. Yet on November 27, 2026, governments meeting at the International Telecommunication Union’s Plenipotentiary Conference in Doha made the resilience of that infrastructure part of the organization’s agenda for the years ahead. The ITU reported consensus on priorities spanning artificial intelligence, connectivity, submarine cables, terrestrial and satellite networks, and emergency communications. [1]

The meeting brought together 179 participating member states, according to the ITU, and 158 signed the conference’s Final Acts. It also approved strategic and financial plans for 2028–2031. Those are meaningful institutional decisions. They do not, by themselves, establish a single new worldwide cybersecurity law or resolve every dispute about who should govern the internet. Their importance lies in the work governments and other participants choose to make possible afterward. [1] [2]

The central question is whether a broad promise of secure connectivity can become a practical bargain: countries with very different resources must be able to maintain services, repair shared infrastructure, participate in technical decisions and protect rights. If resilience remains an aspiration without capacity, the conference will have identified a common interest without sufficiently reducing a common vulnerability. [1] [3]

What the conference actually decided

The ITU’s plenipotentiary conference is its principal governing meeting. Held every four years, it sets the direction of a UN specialized agency whose work includes radio spectrum, satellite coordination, telecommunications standards and development. Governments take the formal decisions, while companies, research bodies and other organizations participate

in the union’s wider work in roles defined by its rules. [2]

In its closing account, the ITU identified priorities including secure and interoperable AI, support for international standards and best practices, resilient communications infrastructure, affordable connectivity, and emergency and disaster communications. It said governments also chose a 48-member Council and a 12-member Radio Regulations Board. The elected leaders’ 2027–2030 terms and the 2028–2031 strategic and financial plans are distinct time periods. [1] [2]

The distinction between a conference outcome and a directly enforceable obligation matters. The ITU describes its formal outcomes as Final Acts, but the legal effect of a particular instrument depends on its text, its provisions and applicable processes. The public document record for the provisional Final Acts indicates that the full text is restricted to authorized users. This analysis therefore relies on the ITU’s public closing account and does not assert the wording or legal effect of provisions that could not be independently examined. [1] [10]

Resilience is a shared dependency

The conference’s infrastructure language matters because communications services cross organizational and national boundaries. A local hospital, a payment provider or a government office may depend on a chain that includes power supplies, landing stations, terrestrial backhaul, a submarine cable, cloud services and equipment from several vendors. Security in one organization is limited if a critical link elsewhere cannot be repaired or replaced promptly.

The ITU’s November 10 resilience discussion brought terrestrial, satellite and subsea networks, cloud and data centres into the same conversation. Participants emphasized redundancy, diversified routes, cyber cooperation and regional planning. These measures address different failure modes: a malicious intrusion requires a different investigation from accidental cable damage, but both can interrupt the services that rely on a network. Treating all outages as attacks would obscure that operational reality. [9]

Work on submarine cables also predates this conference. In July 2026, the ITU reported that the International Advisory Body on Submarine Cable Resilience had approved its final report. Its account identifies cooperation among governments and industry as central to protecting and restoring the infrastructure. The relevant diplomatic problem is not simply naming cables as critical; it is agreeing how permits, specialist vessels, spare equipment and communications among authorities can support timely repair. [5]

For an island state or a country with only a few international routes, resilience may mean paying for a redundant connection that appears uneconomic in ordinary times. For a larger economy, it may mean mapping hidden dependencies between ostensibly separate

providers. International assistance can help, but it works best when local engineers, regulators and operators have the resources and authority to maintain systems long after a conference concludes.

Connectivity and security cannot be separated

The ITU's own review of 127 national policy statements illustrates why security is only one part of the agenda. Updated on November 24, it counted 112 statements addressing expanded connectivity, 91 mentioning AI, 89 digital skills, and 74 cybersecurity and online trust. The organization says themes were identified with AI assistance and checked against keyword searches; these are counts of issues raised, not a representative survey of global public opinion. [3]

The figures point to a practical tension. A government trying to connect rural communities may prioritize affordability and rapid deployment. Another may focus on equipment assurance, incident reporting or national security. These aims need not be mutually exclusive, but security requirements that impose costs without financing or technical support can slow deployment, while inexpensive systems without maintenance can create risks that communities cannot manage.

A useful policy response is to finance security over the life of a network, not only its installation: procurement, patching, spare parts, staff training, independent testing and recovery exercises. Assistance should also be measured against outcomes that local users can recognize, such as restoration time and affordable service in underserved areas. Counting devices installed or workshops held is a poor substitute for knowing whether a network still functions during a disruption.

AI standards: potential and limits

PP-26 placed secure and interoperable AI alongside standards, best practices and developing-country capacity. In telecommunications, that could support better testing and deployment of AI-assisted network management. It could also make it easier for systems from different suppliers to work together. These are potential benefits, not evidence that the conference adopted a mandatory global audit regime for AI providers. [1]

Standards involve choices about who participates and which risks receive attention. Operators need systems that remain dependable under pressure; smaller states need the technical capacity to evaluate products; vendors need workable specifications; and users need meaningful protection when automated decisions affect their services. Security testing should examine not only whether a system performs under normal conditions but how it behaves when data are manipulated or a component fails.

The November 9 Paris Declaration on AI Safety and Security provides a comparison rather than an equivalent legal instrument. A group of governments and companies endorsed

cooperation on matters including information sharing and early warning. Its participants and purpose differ from those of the ITU conference, and a declaration of cooperation should not be described as a binding global AI law. Together, the initiatives show the value of coordination while leaving important questions of oversight, implementation and participation open. [7]

Who gets a voice in global digital rules?

Technical cooperation is never free of institutional politics. The European Union's June 8 preparation document supported resilient communications and an open, interoperable internet, while emphasizing a human-rights-based, multistakeholder model and respect for the mandates of different organizations. It also opposed convening a new world conference to revise the International Telecommunications Regulations. These were the EU's positions before PP-26, not proof that every government shared them or that any particular final text adopted them. [4]

The concern behind such positions is real even when the parties disagree about remedies. Telecommunications networks carry expression, commerce, research and public services. Security measures can protect those activities, but poorly bounded controls can also restrict access or reduce transparency. Policymakers should be precise about a measure's objective, legal basis, independent review and effects on users; the word resilience alone does not answer those questions.

The United Nations Global Digital Compact recognizes a global, multistakeholder approach to internet governance involving governments, the private sector, civil society, technical and academic communities, and international organizations. The ITU has important capabilities within a larger ecosystem; it does not replace every other forum. Coordination is most credible when relevant expertise can influence the process and when responsibilities are not portrayed as belonging to one institution alone. [6]

Participation is also a capacity issue. A state may formally possess a voice but struggle to send specialists to meetings, analyze complex proposals or contribute to standards between conferences. Industry and civil society face their own barriers, including expense, language and time. Fellowships, accessible documents, regional coordination and transparent opportunities for technical input are concrete ways to make participation more meaningful without pretending that all actors have identical voting roles.

From diplomatic alignment to operational cooperation

Regional arrangements can translate broad priorities into exercises and shared response. At their November 20 summit, the EU and the United Kingdom said they would strengthen cooperation against cyber and hybrid threats, exchange experience and explore further cybersecurity work under their Trade and Cooperation Agreement. That joint statement is an

expression of bilateral cooperation and intentions, not evidence that the ITU created a new global enforcement mechanism. [8]

The challenge is to connect such arrangements without assuming that every country has the same alliances, resources or threat perceptions. Practical projects can begin with less politically contentious questions: who is authorized to contact a neighbouring operator after a cable fault; how can a port accelerate repair permissions; which emergency communications can operate if a terrestrial route fails; and what information can be shared safely during an incident? Answers should be tested before a crisis.

A balanced implementation plan should make room for different national circumstances while protecting common standards of accountability. Exercises ought to involve regulators and emergency responders as well as network operators. Governments should publish the objectives of publicly funded resilience projects, explain how they will measure results and provide independent channels for reporting failures. Sensitive network details can remain protected without making all performance information secret.

The test after Doha

The ITU’s closing statement describes a broad consensus, but the hard work is in the distance between agreement and capability. The next assessment should ask whether countries can obtain expert support, repair cross-border links faster, participate effectively in standards work and extend secure connectivity to communities that currently lack it. It should also ask whether technical security measures preserve the rights and trust they are meant to serve.

PP-26 did not make the world’s networks resilient by declaration. It placed shared infrastructure, AI and inclusive connectivity on an institutional agenda with a budget and a timetable. Cyber diplomacy can now add value by turning that agenda into funded maintenance, trusted cooperation and measurable recovery. The most meaningful outcome will be visible not in the number of communiqués issued, but in whether people can continue to rely on essential digital services when the unexpected happens. [1]

Sources and links

[1] International Telecommunication Union: PP-26 closing announcement, 27 November 2026

https://www.itu.int/en/mediacentre/Pages/PR-2026-11-27-PP26-closing.aspx

[2] ITU: What you need to know about the Plenipotentiary Conference

https://www.itu.int/en/mediacentre/backgrounders/Pages/what-you-need-to-know-ahead-of-pp.aspx

[3] ITU PP-26: National policy statements on connectivity, AI and resilience, updated 24 November 2026

https://pp.itu.int/2026/en/newsroom/highlights/policy-statements-connectivity-first-ai-close-behind/

[4] Council of the European Union: EU lines to take at the ITU Plenipotentiary Conference, 8 June 2026

https://data.consilium.europa.eu/doc/document/ST-10314-2026-INIT/en/pdf

[5] ITU: International Advisory Body on Submarine Cable Resilience final report, 10 July 2026

https://www.itu.int/en/mediacentre/Pages/PR-2026-07-10-Submarine-cable-resilience-report.aspx

[6] United Nations: Global Digital Compact, annex to the Pact for the Future

https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact

[7] Government of the Netherlands: Paris Declaration on AI Safety and Security, 9 November 2026

https://www.government.nl/documents/2026/11/10/paris-declaration-on-ai-safety-and-security

[8] Council of the European Union: EU–UK Summit joint statement, 20 November 2026

https://www.consilium.europa.eu/media/ccpczdvj/joint-statement-eu-uk-summit-20-november-2026.pdf

[9] ITU PP-26: Network resilience—design for disruption, 11 November 2026

https://www.itu.int/hub/2026/11/network-resilience-design-for-disruption/

[10] ITU: Provisional Final Acts of PP-26, document record (access to full text restricted)

https://www.itu.int/md/S26-PP-C-0188/_page.print

Read the original article online

https://cybercenter.space/insights/itu-doha-pp26-global-cyber-diplomacy-digital-resilience-2026/