



**WSIS
FORUM 2026**

**6-10 July 2026
Geneva, Switzerland**

Session Outcome Document

When digital systems fail: Understanding the Risk of a Global Digital Pandemic

International Telecommunication Union

09 July 2026, 15:00-15:45

<https://www.itu.int/net4/wsis/forum/2026/Agenda/Session/408>

Key Issues discussed:

- Up to 89% of digital-service disruptions caused by natural hazards result from secondary ripple effects, with up to 10 times more people affected than were exposed to the initial event.
- Cascading risks across power grids, data centres, cloud services, mobile networks, hospitals, payment systems and emergency alerts.
- Dependence on submarine cables, which carry over 99% of international data traffic through nearly 600 active and planned systems spanning 1.7 million kilometres; around 200 faults occur each year.
- Economic exposure: a one-day worldwide Internet outage could generate around USD 29 billion in direct losses.
- National preparedness gaps, including limited mapping of critical dependencies, unclear crisis leadership and insufficient cross-sector testing.
- Need for redundancy across cable routes, mobile networks, satellites, data centres, power supplies and emergency communications.
- Importance of international information-sharing, cyber diplomacy and public-private coordination, as most critical digital infrastructure is privately owned or operated.

Key Outcomes of the session

- Digital resilience is not solely a technical issue; it requires governance, investment, diplomacy and public-private cooperation.
- Participants identified mapping critical digital dependencies, cross-sector stress testing and clear institutional responsibilities as immediate national priorities.

- Infrastructure resilience should combine geographical diversity, alternative cable routes, satellite and mobile backup, emergency roaming, backup power and offline procedures.
- Practical examples showed that preparedness measures such as regular exercises, redundant infrastructure and pre-agreed crisis protocols can keep essential services operational during major disruptions.
- The discussion highlighted the risks created by incomplete information during crises, including misidentification of the cause, delayed response and possible cross-border escalation.
- Business-continuity arrangements should be agreed in advance among governments, regulators, operators, energy providers, financial institutions and emergency services.
- Participants supported integrating digital risks into wider multi-hazard disaster risk management and expanding practical simulations at national and international levels.
- **Initiatives highlighted:** The [When Digital Systems Fail](#) report, [ITU's cybersecurity support and drills](#), and the [International Advisory Body for Submarine Cable Resilience](#).

Key Recommendations and Forward-Looking Actions

- Map national critical digital infrastructure, cross-sector dependencies, chokepoints and single points of failure.
- Conduct regular cross-sector and cross-border stress tests covering power, telecommunications, cloud services, finance, healthcare and emergency alerts.
- Require redundancy and fallback capacity, including geographically diverse cable routes, backup power, satellite alternatives, emergency roaming and offline or analogue procedures.
- Establish named crisis coordinators, decision thresholds and trusted information-sharing channels before disruptions occur.
- Integrate digital resilience into national disaster risk reduction frameworks, investment decisions and emergency telecommunication plans; by 2023, 83% of countries had such plans, but implementation and testing remain uneven.