

Session Outcome Document
Towards Resilient Information Ecosystems in Times of Crisis:
Rethinking 'Preparedness' in Digital Governance

UNESCO

July 7, 2026 - 14:00-14:45

<https://www.itu.int/net4/wsis/forum/2026/Agenda/Session/309>

Key Issues discussed:

- Over the past twenty years of implementing WSIS Action Line C9, digital transformation has significantly expanded access to information, participation, and media pluralism. At the same time, it has introduced systemic challenges to the availability, visibility, and sustainability of trustworthy public-interest information, particularly during crises. The concept of information integrity provides an integrated framework for understanding the resilience of information ecosystems. In line with UNESCO's [Internet 4 Trust](#) initiative and the [Guidelines on the Governance of Digital Platforms](#), protecting journalists and public-interest media; strengthening media and information literacy; and promoting human rights-based digital platform governance and resilient information ecosystems should no longer be treated as separate, siloed issues, particularly in crisis contexts.
- Crisis communication has fundamentally changed. Rather than relying primarily on national communication systems, crises now unfold across interconnected digital and data ecosystems, including digital platforms, cloud services, artificial intelligence, satellite systems and connectivity infrastructure, which have become critical components of crisis response and resilience. These infrastructures should therefore be considered core elements of crisis governance rather than merely "technical add-on" to existing frameworks.
- Humanitarian action has also become increasingly dependent on digital communication. Digital communication infrastructures now support not only information flows but also the delivery of essential services, humanitarian coordination, rights-enabling functionalities, and the preservation of cultural memory. At the same time, growing dependence on private technology providers, cloud infrastructure and digital platforms has introduced new vulnerabilities, including cyberattacks, surveillance, internet shutdowns, spyware, data exploitation and restrictions on humanitarian access. These challenges stemming from digital transformation often outpace the development of new or existing humanitarian and protection frameworks. Much of the gaps, including the protection of digital records, online cultural heritage, digital identities or demographic records and other rights-enabling communication systems, often remain outside traditional protection mandates, despite becoming increasingly essential for affected populations. The usual course of action often enforced by traditional mandate holders is blanket shutdowns, which then forced affected population to untrustworthy information bubbles, now with AI as accelerator. At the same time, it is often local journalists and digital rights activists on the grounds who work to fill in these gaps at high personal/professional costs and with limited support.

- ICTs regulators have an increasingly important role in safeguarding information resilience. Experiences shared from disaster preparedness in South Africa demonstrated the importance of risk assessment, early warning systems, clear institutional roles, regular testing of communication systems, multilingual communication and coordinated multi-stakeholder responses that prioritize the needs of affected communities.
- Practical experience from conflict settings in Ukraine also illustrated the growing limitations of national regulatory approaches. While Ukrainian legislators and regulators had developed some measures between 2014 and 2022, including identifying key actors, threats and digital platforms likely to amplify harmful content, effective implementation has increasingly been constrained by declining cooperation from digital platforms. Although many platforms initially engaged closely with authorities in 2022, this cooperation has gradually diminished. By 2026, meaningful dialogue between major technology companies and Ukrainian authorities had gone down to almost zero, leaving national authorities with few mechanisms to ensure platform responsiveness, transparency or accountability. This is a challenging reality for countries with limited market leverage like Ukraine, where platforms often apply global policies without adapting their systems and designs to the specific realities and risks of crisis contexts.

Key Outcomes of the session:

- Preliminary findings from UNESCO's collaboration with the University of Melbourne, based on a global survey of more than 200 regulatory experts (to be published soon in 2026), highlighted: 61% of respondents indicated that their country's digital regulatory frameworks do not include specific provisions for crisis situations or were unsure whether such provisions exist; most respondents reported that critical transnational digital infrastructures, including cloud services, satellite systems and other digital infrastructure, are not adequately addressed within national crisis communication frameworks; and approximately 70% reported that privacy safeguards during crises are either absent or unclear, pointing to significant governance and accountability gaps. The results of the survey underlined the importance of strengthening international cooperation to address the increasingly transnational character of crisis communication and digital governance.
- More broadly, the session highlighted that regulation of digital communication during crises represents an emerging policy field requiring new governance approaches. Existing regulatory models are often insufficient to address the transnational nature of contemporary digital communication ecosystems.

Key Recommendations and Forward-Looking Actions:

Panelists proposed the following considerations during the discussion:

- Adopt a whole-of-ecosystem approach to crisis communications. Governance frameworks should explicitly integrate digital platforms, cloud infrastructure, satellite communications, artificial intelligence and other critical digital infrastructures into preparedness planning, while strengthening institutional capacities and cross-sector coordination.
- Strengthen international multistakeholder cooperation in this regard, including under the WSIS framework. Meaningful and continued collaboration and dialogue will be essential to

develop shared norms, evidence and governance approaches capable of responding to increasingly transnational and digitally mediated crisis communication.

- Place human rights at the core of international governance frameworks. Future policy frameworks should ensure that humanitarian communication remains grounded in international human rights principles.
- Translate theories to practice with clear governance arrangements to strengthen institutional preparedness. While many guidance and studies have been emerging at the international level, they need to be institutionalized in established frameworks with clearly defined roles and responsibilities, operational coordination mechanisms, multilingual public communication systems, and regularly tested crisis communication protocols that place affected communities at the center of preparedness efforts.
- Enhance platform accountability during crises. There is a need for stronger international cooperation to develop governance mechanisms that require meaningful platform engagement during crises, including enhanced due diligence, transparency and accountability obligations, while ensuring safeguards against the misuse of these frameworks by governments and authorities.