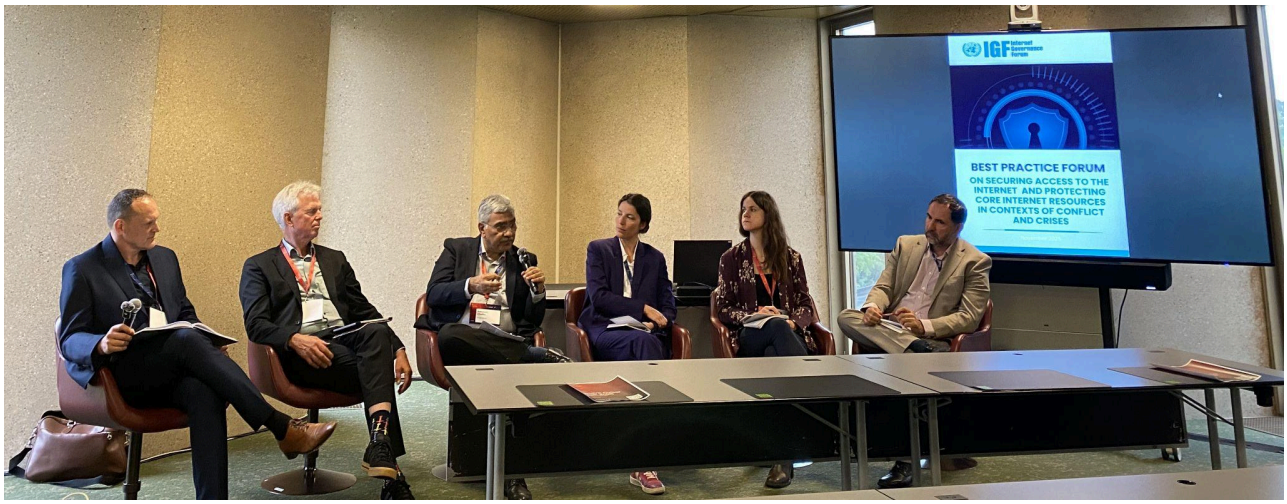
Geneva Cyber Week | Geneva, Switzerland | 4 May, 2026

IGF Secretariat session: *IGF Best Practice Forum: Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises*



Session Summary

- Recording
- 15 onsite participants
- 47 online participants

Panelists:

- Anna Deborah Kruip, Programme Management Officer, UNDRR
- Olivier Alais, Programme Coordinator, Telecommunication Standardization Bureau, ITU
- Kayle Giroud, Head European Affairs, Cyberpeace Institute
- Ashutosh Chadha, Senior Director, UN and International Organisation's, Microsoft
- Ernst Noorman, Ambassador at Large for Cyber Affairs, Ministry of Foreign Affairs of The Netherlands

Moderator:

- Wim Degezelle, IGF Secretariat Consultant on IGF Best Practice Forum on Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises.

The meeting focused on lessons and recommendations emerging from the IGF 2025 Best Practice Forum that explored how to secure civilian internet access and protect core internet resources during conflict, crisis, and disruption scenarios. The session emphasized gathering expert input from the panelists to help shape a multistakeholder approach to secure civilian internet access and protect core internet resources .

Key Discussion Points

1. The IGF Best Practice Forum

- The moderator explained that the IGF Best Practice Forum (BPF) operates as an intersessional IGF activity and provides a platform for stakeholders to collaborate in greater depth on specialized topics and produce a report on key findings.
- The 2025 work was coordinated by Valeria Betancourt (IGF MAG member, APC) and Anriette Esterhuysen (APC), with support from organizations including Article 19, Access Now, and Kaspersky.
- Key outline of the BPF Report:
    - Challenge: *There is a clear and pressing need to clarify the roles and responsibilities of the multistakeholder Internet community - and the institutions within it - in securing core Internet resources and ensuring civilian access to the Internet during conflicts and crises.*
    - The challenge led to the conceptualisation of three key work areas for multistakeholder cooperation to take the work further:
        - Creation of a **multistakeholder emergency mechanism** for immediate action to protect and restore.
        - Clarifying applicable **legal and regulatory frameworks**, including Human Rights Law and International Humanitarian Law.
        - Establish a **comprehensive governance approach** that covers preparing for conflict and crisis situations, acting during conflict, restoring after conflict, and takes into account other socioeconomic factors.

2. Securing Civilian Internet Access During Conflict and Crisis

Participants discussed the growing importance of protecting internet access as an essential service during armed conflict, disasters, and political instability.

Key concerns included:

- Deliberate internet shutdowns and disruptions.
- Damage to telecommunications infrastructure.
- Risks to submarine cables and other critical internet infrastructure.
- The impact of cyber operations on civilian populations.
- Dependence of humanitarian response and essential services on reliable connectivity.

The discussion highlighted that internet access increasingly functions as a prerequisite for:

- Humanitarian coordination.
- Access to information.
- Public safety.
- Financial systems.
- Health and emergency services.

3. The Need for Multistakeholder Cooperation

A recurring theme throughout the session was the importance of multistakeholder collaboration. Participants stressed that:

- Governments alone cannot address internet resilience challenges.
- Technical community actors, private sector operators, civil society, academia, and international organizations all have essential roles.
- Open and inclusive dialogue is necessary to build trust and coordinate effective responses.
- Certain technical and operational challenges require rapid coordination among stakeholders that no single actor can solve independently.

There was broad support for ensuring that cybersecurity and resilience discussions remain inclusive and transparent rather than taking place in closed or isolated forums.

4. Infrastructure Resilience and Systemic Risks
Panelists discussed increasing vulnerabilities affecting digital infrastructure globally. Topics included:

- Physical attacks on infrastructure.
- Cyber threats to internet infrastructure.
- Cascading failures caused by interconnected systems and supply chains.
- Risks posed by natural hazards such as solar storms, volcanic eruptions, and extreme weather events.
- The fragility of submarine cable systems and related dependencies.

During the discussion, reference was made to a report jointly developed by UNDRR, ITU, and Sciences Po on critical risks to digital infrastructure and cascading failures. The report was published the day after the session and is available **here**.

5. The Role of International Organizations
The International Telecommunication Union (ITU) was highlighted as an important facilitator in maintaining global connectivity and interoperability. Examples of ITU contributions mentioned included:

- Convening discussions among member states and technical actors.
- Supporting the Partner2Connect initiative.
- Developing technical standards for infrastructure interoperability.
- Supporting projects related to submarine cable systems and connectivity expansion.

Participants recognized the importance of international coordination mechanisms in maintaining a stable and interoperable internet ecosystem.

Emerging Themes

Internet Access as Critical Civilian Infrastructure
Participants increasingly framed internet connectivity as critical civilian infrastructure that should be protected during crises and conflicts.

Interdependence and Cascading Risk
The session emphasized how digital systems are deeply interconnected, meaning disruptions in one area can rapidly affect broader societal systems.

Importance of Technical Coordination
There was strong recognition that technical coordination mechanisms are essential during emergencies and infrastructure disruptions.

Need for Continued Dialogue
Participants supported continuing the discussion within future IGF Best Practice Forum cycles and through broader international cooperation.

Main Takeaways

- Protecting civilian internet access is becoming a major global governance and cybersecurity issue.
- Multistakeholder cooperation is essential for internet resilience and crisis response.
- Critical infrastructure protection must include both cyber and physical resilience dimensions.
- International organizations such as the ITU play an important convening and standards-setting role.
- Future work should continue exploring practical coordination mechanisms, resilience strategies, and norms related to internet protection during crises.

Suggested Follow-Up Actions

1. Panelists confirmed the three focus areas conceptualised by the BPF and suggested to continue the IGF Best Practice Forum discussions in future cycles.
2. Expand engagement with technical operators, governments, and civil society organizations.
3. Develop more concrete operational guidance for crisis coordination and infrastructure protection.
4. Further examine systemic and cascading risks affecting global internet infrastructure.
5. Strengthen international cooperation around infrastructure resilience and interoperability.

Session Outcome
The session reinforced broad agreement that resilient and secure internet access is increasingly central to civilian protection, humanitarian response, and global stability. Participants emphasized that future solutions will depend on inclusive multistakeholder cooperation, stronger infrastructure resilience measures, and continued international dialogue.