

IGF 2025

**Best Practice Forum**

**Securing Access to the Internet and Protecting Core Internet Resources**

**in Contexts of Conflict and Crises**

(BPF Cybersecurity)



BPF Meeting 27 November 2025

---

## Call Summary

### Introduction

1. The Best Practice Forum (BPF) [Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises](#) ([BPF webpage](#)) is an IGF 2025 intersessional activity. BPFs provide an open platform for sharing experiences on Internet policy issues and support the development of bottom-up, community-driven outputs that contribute to an understanding of global good practices and inform policy discussions, standards development, business decisions, as well as public understanding, awareness, and discourse. The BPF was launched in May and organised a main session during the IGF 2025 annual meeting in Lillestrøm, Norway ([session recording](#), [summary](#)).
2. The purpose of the call was to present the BPF output report and discuss next steps for the three work areas conceptualised in the report: a multistakeholder emergency Internet connectivity mechanism, normative discussion, holistic multistakeholder governance approach.
3. At the opening of the meeting, Valeria Betancourt, MAG co-facilitator of the BPF, thanked stakeholders for their commitment and contributions to the BPF, and expressed particular appreciation for those who took on leading roles in driving the three work streams. BPF co-facilitator Anriette Esterhuysen also reminded participants that the BPF is an open and inclusive IGF modality, and that anyone interested may join at any time.

### BPF outcome, report, and way forward

4. The [BPF output report](#) will be officially launched, together with the other IGF intersessional work outputs at a [PN & BPF Publication Ceremony](#) on Monday, 1 December 2025.

5. BPF consultant Wim Degezelle provided background on how the BPF topic builds on previous IGF discussions and IGF Messages, gave a brief overview of BPF activities and how the work evolved over the year, and clarified the scope of the BPF. The BPF focuses on the roles and responsibilities of the multistakeholder Internet community and its institutions in ensuring civilian Internet access and protecting core Internet resources in contexts of conflict and crisis. It was also noted that the BPF does not intend to address uses of the Internet that contravene international law, nor issues related to the lack of basic infrastructure resulting from socio-economic inequality.
6. It was explained how the BPF discussions led to the identification of three work areas, for which detailed concept notes were developed and included in the output report to support further work. At the same time, it was noted that working in separate streams requires coordination and cooperation to avoid the creation of silos and fragmentation of the work.
7. Marwa Fatafta (Access Now) introduced the first work area and explained how it is based on the observation that there exists no comprehensive global emergency response mechanism that provides connectivity solutions for the wider civilian population in conflict contexts. Existing initiatives, such as the Emergency Telecommunications Cluster (ETC), emergency mechanisms within the ITU, or initiatives such as the Freedom Online Coalition (FOC) or the Keep It On initiative, typically focus on restoring connectivity for specific categories (e.g. emergency responders), are specialised in specific contexts (e.g. natural disasters) or actions (e.g. monitoring and advocacy). The BPF is well-positioned to examine the gaps between existing initiatives and the unique challenges posed by armed conflict, and explore the scope, role, and objectives of a comprehensive emergency connectivity mechanism.
8. Chantal Joris (Article19) outlined that the second work area focuses on the question of how International Human Rights Law (IHRL) and International Humanitarian Law (IHL) interact or complement each other, as well as where gaps and discrepancies may exist. While this has been prominently discussed in other contexts, the discussion is more recent when it comes to the digital sphere and connectivity in armed conflict. In this work area, the BPF could bring together experts and organisations working in both fields, civil society actors engaged on these issues, and other relevant stakeholders, to explore whether a shared position or interpretative guidance could be developed and advanced.
9. Jochen Michels (Kaspersky) presented the third work area, which focuses on multistakeholder cooperation to protect digital infrastructure and connectivity in contexts of conflict and crisis. This should encompass cooperation efforts in peacetime and measures taken long beforehand, to ensure greater resilience when a crisis occurs. With additional outreach, the BPF could establish a more inclusive dialogue and ongoing

cooperation at the global level, which would be beneficial and essential for the long-term health and viability of the Internet.

10. Chengetai Masango (IGF Secretariat) shared that, at the start of 2026, the IGF Secretariat hopes to be able to announce the venue and dates of the next IGF, along with details on intersessional activities. It was also noted that the BPF is ready to submit a proposal to continue its work once the new MAG is in place.

#### Links

BPF Webpage

<https://intgovforum.org/en/content/bpf-cybersecurity>

BPF 2025 Output report

[https://intgovforum.org/en/filedepot\\_download/339/30209](https://intgovforum.org/en/filedepot_download/339/30209)

---