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 17 June 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.

2. The purpose of the call was to review the initial feedback on the draft problem statement and discuss preparations for the BPF Main Session on Thursday, 26 June, 14:00-15:15 CEST, at the IGF annual meeting in Lillestrøm, Norway.

Feedback on draft problem statement

3. At its first call on 6 May 2025 the BPF developed the following draft problem statement: *"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."*

4. After the 6 May meeting, a Call for written contributions on the problem statement was shared on the BPF's webpage and distributed via the mailing list. The deadline line for feedback, initially 11 June, was extended until after the annual IGF meeting.

5. Contributions received so far raised that the different concepts in the draft problem statement, including core Internet resources, Internet access, and the Internet multistakeholder community would need to be developed in more detail as there exist various definitions and understandings of these concepts. It was also suggested that the BPF should not limit its scope to conflict and crisis situations and their aftermath, but

should also consider what can be done to prepare for these situations, including, for instance improving infrastructure resilience, capacity building, and awareness raising.

6. It was recommended that the BPF should not only look at roles and responsibilities of stakeholders, but also consider the applicability and compliance with existing norms (voluntary and binding). Such an analysis should look into whether there are gaps in the norms frameworks. It was also suggested to look into positive obligations, as for example in the human rights framework.

Preparations BPF Main Session

7. Participants discussed the outline for the BPF Main Session at the annual IGF meeting in Lillestrøm, Norway.

14:00 - 14:20 : Opening and setting the scene

1. Welcome and introductions
2. BPF 2025 focus and topic & objectives of the session
3. Message UN Office on Disarmament Affairs (pre-recoded)
4. Presentation of the BPF's problem statement and received feedback

14:20-14:35 : Case studies

14:35-14:50 : Discussion round 1: normative frameworks

Reflecting on the very different cases, what existing norms apply to the context of securing access and protecting core internet infrastructure? Are they sufficient? Is there a need for evolving or adapting such norms?

14:50-15:05 : Discussion round 2 : Accountability frameworks & Role of Stakeholders

What accountability frameworks would support compliance with such norms? Which institutions have a role? What's the role of different stakeholders?

15:05-15:15 : Next steps for the BPF

AoB and next steps

8. Participants discussed outreach to stakeholders and organisations to engage in the BPF. Suggestions include: Aspen Institute Global Cyber Security Group, Global Commission on the Stability of Cyberspace, cybersecurity agencies, ITU, national governments active on the topics.