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 29 October 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 is to provide an update on progress and the preparation of the BPF output report, and to have an exchange on how and where the proposed work in the three work areas can be taken up, within the IGF context and elsewhere.

3. The BPF, in May, developed a draft problem statement, which provided the basis for further exploration of the topic. Through subsequent discussions, three concrete work areas were identified: 'multistakeholder emergency mechanism', 'normative discussion', 'multistakeholder governance'. The three work areas are being translated into concept notes for further work. The BPF is also preparing an output report covering its discussions during the 2025 cycle.

Input for the draft report and BPF work

4. Participants walked through the outline of the draft BPF report and were invited to comment and contribute.

5. It was suggested that developing a more precise problem statement would be helpful to guide further work. It was recommended that the problem statement clearly defines the scope of the work, identifies the different elements of the scope, and clarifies who should

be engaged in which part(s) of the conversation. For example, the reason for not having access to the Internet may be the unavailability of electricity, a shutdown resulting from a government decision, a kinetic attack on the infrastructure, or a cyber attack. There are different scenarios, and addressing them requires the involvement of different people, organisations and stakeholders. Similarly, depending on the interpretation of what is considered core Internet or information infrastructure, different stakeholders should be involved in its protection.

6. It was noted that the problem statement lacks the perspective of the people who are directly affected. Integrating this perspective would provide an extra justification for the BPF's work. There are a lot of local organisations, including in the most affected countries whose work sometimes lacks visibility, to engage in the discussion. Adding this perspective also raises the question of socio-economic rights and connectivity. This would influence the normative discussion as more human rights and positive obligations should be considered.

7. It was pointed out that the explanation of the technical community's response to requests for action following the outbreak of the war in Ukraine on 24 February 2022 requires more nuance. It was noted that the narrative that suggests that the technical community refused to take action is a mischaracterisation. In reality, actions were taken in cases involving violations of RIPE policies, for example, when IP address space allocated to Ukraine was or was at risk of being taken away from the country.

8. A concern was raised that, while it is good that the topic is approached from three different angles in the work streams, this may lead to a fragmentation and dilution of the discussion. It will therefore be important to ensure connections between the streams.

9. It was noted that the Red Cross and Red Crescent Movement would be an important stakeholder in the discussion on an emergency mechanism, because of its local presence and connections through the National Red Cross and Red Crescent Societies. It was alos pointed out that the International Committee of the Red Cross (ICRC) is leading the Global Initiative to Galvanize Political Commitment to International Humanitarian Law which has a work stream on technology that also deals with connectivity. It was suggested to look for opportunities to engage them in the BPF's normative discussion. Other suggestions for outreach included ITU, GNI, GSMA, SPHERE.

Next steps

10. It was noted that the BPF report should present a strong argument for the continuation of the work (while acknowledging that the renewal of the IGF mandate will be discussed by

the UN General Assembly in December) by demonstrating interest in the topic and collaboration with organisations and individuals also working in this field.

11. Participants were invited to reflect on how to advance the work on the three work streams, and to focus on who should be involved. It was reiterated that, to align with the IGF cycle and finalise a BPF output, the short-term aim was to frame the issues, identify areas that require action, and determine which key partners and stakeholders should be involved in discussions addressing the issues. It was suggested that identified key stakeholders could be invited to share short testimonials on the relevance of the work to them.

12. It was agreed to organise a final webinar for the BPF to conclude the work for the 2025 cycle. This session would provide an important opportunity to present the BPF's report, pitch further work on the three streams, and engage stakeholders in a follow-up. It was also noted that this session should be an opportunity to invite institutions and organisations to share priorities and work underway related to the BPF's work areas because it is important to take stock of what is already happening and not reinvent the wheel.