IGF 2025

Best Practice Forum

Securing Access to the Internet and Protecting Core Internet Resources
in Contexts of Conflict and Crises

(BPF Cybersecurity)

Call for written contributions
On the problem statement and challenges

Introduction

The Best Practice Forum (BPF) is an IGF intersessional activity that, through the exchange of experiences and the development of community-driven outputs, aims to contribute to the understanding of global Internet policy issues and good practices, and to inform policy discussions, standards development, business decisions, and public awareness and discourse. The IGF Multistakeholder Advisory Group (MAG) selected Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises as topic for a BPF during the IGF 2025 cycle (BPF proposal).

At IGF2024, the main session 'Protecting Internet infrastructure and general access during times of crisis and conflict' highlighted the need for coordinated efforts and stakeholder collaboration to protect core Internet infrastructure and ensure access to the Internet in contexts or conflict and crises.

The BPF, at its kick-off call, formulated the **draft problem statement** that "*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 BPF now invites written inputs on the following questions:

1. **Feedback on the draft problem statement:**
   Do you agree with the way the problem is framed? Are there aspects that should be added, clarified, or reworded? How do you define the '*core Internet resources*' referenced in the statement?
2. **Main challenges:**
   What are the key challenges in ensuring the protection of the core Internet infrastructure and access during crises and conflicts?
3. **Applicable norms, agreements, and processes:**
   Which existing norms, agreements, or processes are relevant to this issue? How effective are they in practice? Are there notable gaps?

4. **Operational best practices:**
   Can you share examples of successful practices or approaches—at national, regional, or organisational level—that address these challenges?
5. **Relevant resources:**
   Please share links to articles, case studies, reports, or other background materials that could inform the BPF's work.

Instructions for providing written feedback

- Please submit your written feedback, preferably not exceeding **2 pages**, in **Word or PDF format**.
- The **deadline for submissions is Wednesday, 11 June**.
- Send your feedback to: **bpf-cybersecurity-info@intgovforum.org**.

All submissions will be published on the **BPF webpage**. If you do **not wish your name or organisation to be listed**, please indicate this clearly in your submission.

The input received will contribute to the ongoing work of the **BPF** and inform its session at **IGF 2025 in Norway**.

The BPF webpage is the primary source for updates and key information about its work.
https://intgovforum.org/en/content/bpf-cybersecurity