IGF 2025

Best Practice Forum

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

(BPF Cybersecurity)

BPF Kick-off Call 6 May 2025

Call Summary

Introduction to the Best Practice Forum

1. Best Practice Forums (BPFs) are a modality of the IGF intersessional activities. They provide an open and inclusive platform for sharing experiences on Internet policy issues and support the development of bottom-up, community-driven IGF outputs. BPFs aim to 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 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 Best Practice Forum (BPF) during the IGF 2025 cycle (BPF proposal). The BPF can build on the work of the BPF Cybersecurity, which in previous years - amongst other things - focussed on the development, value, and application of cybersecurity norms agreements. Previous output reports can be found on the BPF webpage, listed in a table at the bottom of the page.

3. The timeline and activities for the 2025 cycle will be structured around a BPF kick-off call in May, a main session during the IGF2025 annual meeting in Norway (23-27 June), and the publication of the final BPF Output by 1 November.

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

4. Recent examples, such as the war in Ukraine and the conflict in Gaza, show that there is no coordinated response to threats of damage and actual damage to the core Internet resources in situations of conflicts or crises. Established norms relevant and applicable in these contexts, such as the rules of war, international humanitarian law, principles on the open interoperable Internet, are inconsistently applied or not well known and

internalised. In cases of natural disasters or damage to the undersea fiber optic cable system, response efforts are generally led by the private sector.

5. The thematic main session at the IGF2024 in Riyadh on 'Protecting Internet Infrastructure and General Access during times of crisis and conflict', among other things, concluded that there is a need for coordinated efforts to ensure open and secure access to the Internet for civilians, protect core Internet infrastructure, and foster collaboration among stakeholders, state and non-state actors, to achieve these goals. It also discussed a comprehensive definition of what is meant by critical or core Internet infrastructure.

BPF scope and purpose

6. The BPF aims to clarify the roles and responsibilities of the multistakeholder Internet community and the institutions that are part of it; evaluate the key issues, challenges, and needs from the perspectives of various relevant actors and stakeholder groups; and adopt a holistic approach that encompasses preparedness for crisis, prevention and protection under legal frameworks, resilience, impact mitigation, and rebuilding and recovery.

7. To limit its scope, the BPF will not address the use of the Internet in conflicts, such as the malicious use of Internet infrastructure for cyberattacks or disinformation campaigns. The BPF also does not address the lack of basic infrastructure often resulting from socio-economic inequality. However, it may consider how pre-existing connectivity gaps increase vulnerability and affect efforts to protect core Internet resources and maintain access during crises and conflicts.

Stakeholder participation

8. The BPF is an open and voluntary process. Establishing a multistakeholder dialogue on its subject matter is a BPF objective in its own right. Therefore, identifying, inviting, and including relevant stakeholders in the discussion will be an ongoing task. Various ways will be explored to encourage broader stakeholder participation, including webinars, open mailing lists, main session, and requests for input.

9. In addition to the traditional IGF stakeholder groups (governments, businesses, civil society, the academic and the technical community) and stakeholders involved in rebuilding infrastructure (such as fiber optic cables, microwave links, or other forms of access) to (re-)establish the connection to the Internet's logical layer (incl. the unique identifiers - IP addresses and domain names), the BPF should engage relevant humanitarian actors and stakeholders - public and private - form the Internet's

application layer, as they are essential in ensuring that civilians can access services that operate on top of the logical layer.

BPF problem statement and next steps

10. The following draft problem statement will serve as a starting point for the BPF's work: "*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.*"

11. The community is invited to provide feedback on the draft problem statement, identify key challenges, highlight applicable norms and processes - or gaps therein - and share operational best practices. A call for written input will be launched, and received input will be reviewed and discussed at the next BPF call in early June. This community input will directly feed into the BPF main session at the IGF meeting in Norway.

AoB

12. The BPF will create a dedicated discussion group to enable more focussed conversations and support the review of the received input. Information will be shared along with the call for written input.

13. The BPF invites to share existing materials (articles, research, reports) relevant to its subject matter, which can be used and listed as background information.

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