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 3 September 2025

Call Summary

Introduction and recap BPF Main session at IGF 2025

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. On 26 June, the BPF organised a main session during the IGF 2025 annual meeting in Lillestrøm, Norway (session recording, detailed session notes). The main session looked at concrete case studies of crisis situations (Soudan, Syria, Russia/Ukraine, Gaza, AFRINIC) to address the question of civilian Internet access and the protection of core Internet resources from a practical, normative, and multistakeholder perspective.

3. From the Norway discussion, the BPF has identified three possible action points:
    1. Support the establishment of a multistakeholder mechanism for emergency and rapid response to secure or restore connectivity in times of crisis.
    2. Provide a platform to address the gap between human rights and humanitarian law frameworks in the context of safeguarding civilian internet access and protecting .
    3. Forster a discussion on the role and functioning of the Multistakeholder model when it comes to securing access and protecting core Internet resources.

Discussion on the three actions and next steps

4. Emergency mechanism: mitigating the harm caused by shutdowns/disruptions.
    - Civil society actively advocates against shutdowns/disruptions and documents the harm they cause.

Mitigating the harm and ensuring that communities can reconnect and stay connected, requires resources, political pressure, funding. It requires the involvement of multiple stakeholders to restore and maintain connectivity in conflict situations.

- The BPF could advance the creation of a multistakeholder emergency mechanism by inviting relevant organisations to explore its various aspects and compile a detailed concept note.
  These discussions and concept paper should, amongst other things, look into:
  - What should the mechanism look like?
  - What can be learned from existing approaches in different contexts ? What are possible models, and their pros and cons?
  - Who should be involved? Who are relevant actors?
  - Where can it be housed?
  - Should it be, yes or no, tied to any existing mechanism or actor?
  - How should the mechanism connect to the Emergency Telecommunications Cluster (ETC), Freedom Online Coalition (FOC), UN mechanisms?
  - How to advocate for such an emergency mechanism?
  - Can the mechanism be used to strengthen infrastructure and connectivity resilience, including in periods between or prior to conflict?

5. Normative discussion: addressing shutdowns/disruptions under IHL.
   - There is limited and slow movement in addressing Internet shutdowns and connectivity disruptions under international humanitarian law (IHL). Some recent publications depolitise the issue and may help to bridge the gap between those who see shutdowns/connectivity disruption in conflict as a political matter and human rights groups that focus on their harmful nature.
     For example:
     - July 2025 International Committee of the Red Cross (ICRC) blog posts on the humanitarian consequences of connectivity disruptions and on international humanitarian law and connectivity disruptions during armed conflict.
     - June 2025 Freedom Online Coalition (FOC) Joint statement on protecting human rights online and preventing Internet shutdowns in times of armed conflict

   - The BPF could develop a concept note on how shutdowns and connectivity disruptions should be threatened under the different international legal frameworks, and as such contribute to a shared position that can be promoted to different actors and stakeholders, including states and international organisations.
     (A similar approach was taken by civil society to advocate that shutdowns are a clear violation of human rights law.)

6. Governance discussion.
    - The multistakeholder Internet governance model is intended to protect and safeguard an open and interoperable Internet. However, recent examples show that its responsiveness and effectiveness in protecting core infrastructure and connectivity during crises vary. This raises the question of how the multistakeholder model's role can be strengthened to enhance the resilience of infrastructure and communications.

    - The BPF could help to obtain a better understanding of the dynamics and processes of the multistakeholder model in preserving core Internet functions during situations of conflict and crisis. It could also explore what can be done to make the model more effective when the Internet is at risk in a certain context, and how it can further strengthen the resilience of core Internet infrastructure to ensure it remains operational in the face of military conflict or other crises.
        - The BPF could, for example though interviews, first-hand testimonials, surveys, gain insight in the technical community's refusal to intervene and limit Russia's connectivity at the outburst of the Russia-Ukrainian war, or understand how different non-state actors, including telcos, are prepared or prevented to provide cross-border connectivity to conflict zones.
        - At a time when several countries are developing new laws to increase the resilience of critical communications infrastructure within their jurisdictions against digital and physical threats, it is important to discuss at the global level how such measures may affect the overall stability and resilience of the Internet, also beyond the context of any specific conflict.

<u>Overarching issues</u>

7. The BPF's overarching 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,*" raises the question of how to conceptualise the notion of ensuring civilian access to the Internet.
        - Could a state argue that a reduction in access or connectivity without shutting down is permissible?
        - How can the notion of access to the Internet and the infrastructure that enables it be decoupled from its use, given that states often invoke use to justify shutdowns and destruction of infrastructure citing public safety or national security risks?
        - Two cases suggest that reduced connectivity should not be more permissible than shutdowns. In Iran, throttling to 2G left users exposed on unencrypted

networks, making government surveillance easier. The situation in Gaza, with in some parts 80% of infrastructure destroyed since the beginning of the conflict, could be regarded as a continuous shutdown.

8. Approaching connectivity in conflict through the lens of access, rather than focussing on protecting infrastructure, may be helpful since it avoids defining what is a legitimate military target. Access to connectivity could be framed through a multidimensional humanitarian protection framework, similar to an approach already applied in other contexts. Access to connectivity could then be broken down into specific dimensions, such as safe access and reliable access, which can be clearly defined.

Next steps

9. The BPF will begin developing detailed concept notes for the three actions mentioned above and will report on progress during the next call as well as through the mailing list (bpf-securing-access-internet-core@intgovforum.org - subscribe here to get involved). Volunteers are sought to join the three work teams and contribute to this effort.