Proposal on a Best Practice Forum under the banner of the BPF on Cybersecurity on **Protecting Core Internet Resources and Access in Contexts of Conflict and Crises**

Updated 14 April 2025

Background

The IGF2024 Thematic Main Session on the IGF theme "Enhancing the digital contribution to peace, development, and sustainability" took place on 17 December with the title 'Protecting Internet infrastructure and general access during times of crisis and conflict.' The outcome of this session pointed unambiguously to the need for work to be done to clarify the roles and responsibilities of the multistakeholder internet community - and the institutions that are part of it - with regard to securing and protecting core internet resources (also referred to as the public core of the internet) and access to the internet for civilians in context of crisis and conflict. One of the overarching themes of IGF 2025 is "Building] Digital Trust and Resilience," and it includes the focus of this PBF as a sub-topic.

Outcomes of the 2024 main session

The documented outcome of the 2024 main session is a useful starting point for this new BPF. The session concluded that:

- Critical infrastructure includes technical infrastructure for internet access and telecommunications connectivity. There is an important role for the ITU in disaster relief and facilitating the repair and rebuilding of damaged infrastructure. Technical bodies responsible for internet governance must remain neutral to function effectively and be free from sanctions and protected from legal and extra-legal attacks.
- Efforts must be taken at all major forums and institutions responsible for the maintenance of international peace and security to ensure open and secure access to telecommunications infrastructure and protection of the public core. This includes the UN Security Council, which could incorporate attention to telecommunications in the conflicts it monitors, as well as peace and justice institutions, who can assist in efforts to seek accountability for disruptions that impact fundamental rights and security.
- All stakeholders must collaborate to ensure protection of essential telecommunications and internet infrastructure, even in times of crisis. Speakers proposed new working groups to take forward Global Digital Compact guidance that states refrain from internet shutdowns, and the creation or enhancement of IGF Best Practice Forums to look at the roles/responsibilities of the multistakeholder community in ensuring the protection of the public core/access in times of conflict and crisis.
- The primary responsibility for preserving internet and telecommunications connectivity in times of crisis and conflict lies with the parties to the conflict themselves, who shall refrain

from abusing civilian infrastructure for military purposes, or targeting it outside of the strict boundaries set by the laws of armed conflict and international humanitarian law.
- They should refrain from weaponizing or withholding access to telecommunications equipment, fuel, and repair parts -- which have direct links to economic development.
- Displaced persons suffering calamities and conflicts are increasingly asked to engage with digital services to access assistance, including essential foods, medicines, and services, underlining the importance of connectivity even in dire conditions.

Scope of work

Essentially, this BPF will analyse the overall topic, assessing key issues, challenges and needs from the perspective of various role players and stakeholder groups. It will assess what work has been done, including through a literature review and identify good practices and gaps and set a forward-looking agenda for protecting the public core of the internet and securing access in contexts of conflict and crisis. It will adopt a holistic approach: preparing for crisis, prevention and protection under legal frameworks, resilience, mitigating impacts, and rebuilding/recovery. As mentioned above, the 2024 main session outcomes present a good place to start, but ultimately it is up to the participants in the BPF to, at the outset of its 2025 work planning, review and decide on the BPFs scope of work.

The work advanced at RightsCon 2025 on digital ceasefire and the #ReconnectGaza campaign both merit attention in more traditional conflict negotiation and resolution bodies. Groups like the Center for Humanitarian Dialogue and Chatham House, who study both geopolitical crises and the role of tech and its governance, could assist or host regular discussions. Additionally, the Freedom Online Coalition group of 42 states is likely to increase attention and activities at the intersection of conflict and internet shutdowns in this calendar year, under the Chairship of the Government of Estonia. If we develop a concrete set of recommendations, we could carry out consultations, tabletop exercises, and a review of potential policy and operational changes at the relevant institutions to implement.

The goal is to gather perspectives on the scope of work between April and June 2025, validate these during the IGF in Oslo in June and then build the rest of the year's workplan accordingly.

On an ongoing basis, this workstream speaks to essential infrastructure for peace and security work, from monitoring to conflict resolution to rebuilding, and therefore carries relevance for a regular programmatic discussion at the Munich Security Conference and WEF Annual Meeting, and at other conflict resolution centers/fora. We suggest this BPF continue its work intersessionally in the first year, at the standard internet governance world's global events like ICANN and other I-Star gatherings, IGF, RightsCon, and the Global Gathering and regional events, especially in MENA and sub-saharan Africa, while aiming to speak outside these familiar confines in the second and third years.

Note on topic/title/name: If we are trying to distinguish ourselves from the previous cybersecurity BPFs we could highlight 'stability' or 'continuity' or 'protection' of access rather than security. Other values or goals we seek are uninterrupted, unobstructed, reliable, and consistent access to the open and secure internet. We should aim for a catch title or acronym. We also need to consider whether we want to speak of 'internet' or telecommunications. BPF on the Stability of Telecommunications (and Internet) Access in Crisis and Conflict Situations would be BPF on STICCS or STACCS.

Partners and participants

IGF BPFs are open to all. A MAG member needs to act as a liaison for the BPF and the IGF Secretariat assigns a part time consultant to support the BPF's work. Other individuals or institutions can join the BPF's "steering group".

Key partners to build into this process will be NROs, RIRs, ccTLD and gTLD Registries, ICANN, ISOC, humanitarian relief institutions in the UN and outside of it, including OCHA, ICRC, and more, the ITU, and relevant civil society and private sector institutions. The Dutch Government, which first introduced the notion of the norm to protect the public core is a potential partner. From the academic community, participation has been committed by Dennis Broeders from the University of Leiden, the person who first conceptualised the idea of the public core of the internet as well as by Madeline Carr from University Colleague London.

Civil society groups who have expressed interest include 7amleh, Access Now, Human Rights Watch, and the Association for Progressive Communications and several of its members. Also the Center for Humanitarian Dialogue and Chatham House.

There is a running list of individuals who have contributed to this document who will be invited to join the BPF.

Next steps / initial work plan

BPF meeting I: BPF Kick off call *(1st week of May)*

- Open call, invitation shared on BPF CS & MAG mailing list + IGF Secretariat socials
- Presentation of the BPF's focus, scope and initial work plan
- Launch of the Call for written inputs from key stakeholders

Call for written input from key stakeholders *(May - 1st week June)*

- What? Key stakeholders are invited to share brief input (max 2 pages) addressing the following questions
    - Feedback on problem statement
    - What are the main challenges ?
    - What norms and processes are applicable ? What gaps exist ?
    - Operational : what operational best practices exist ?

BPF Meeting II: Compilation of Input received from key stakeholders *(before 13 June)*

- First analysis and discussion of feedback received
- Compilation and publication of the contributions on the BPF page
- Open call for public feedback

BPF Meeting III: Session at the IGF 2025 in Norway

- The input of key stakeholders & received background serves as main input for the session
- The Session could discuss the same question as asked to key stakeholders
    - Problem statement / challenges / applicable norms & gaps / operational best practices
- The session should discuss the next steps and workplan for the BPF
- This session should also frame the BPF's work within GDC / WSIS
- Develop an action plan and timeline for the period after the IGF meeting.

Further BPF Meetings, Next steps and action, and format/content final BPF output

- To be discussed
- 1 November - publication BPF final output for 2025