IGF 2025 NORWAY

IGF Internet Governance Forum

IGF Best Practice Forum

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

BPF kick-off call, Tuesday, 6 May

www.intgovforum.org/en/content/bpf-cybersecurity

IGF Best Practice Forum
Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises

6 May 2025, Kick-off call

Agenda

1. IGF Best Practice Forum - Introductions
2. Focus: Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises
3. Suggested approach & next steps
4. Discussion and feedback

IGF Best Practice Forum

-> IGF intersessional activity

-> provides a platform to exchange experiences in addressing Internet policy issues

-> open, bottom-up and collective process to produce community-driven IGF outputs

-> BPF outputs intend to contribute to an understanding of global good practice, and to serve as a resource to inform policy discussions, standards development, business decisions, as well as public understanding, awareness, and discourse.

IGF Best Practice Forum Cybersecurity

2018 - 2024

-> different aspects of **CYBER NORMS AGREEMENTS**

Culture, norms and values in cybersecurity (2018)

Cybersecurity norms operationalisation (2019)

Lessons from norms in non-cyber governance (2020)

Drivers behind cybersecurity initiatives (2021)

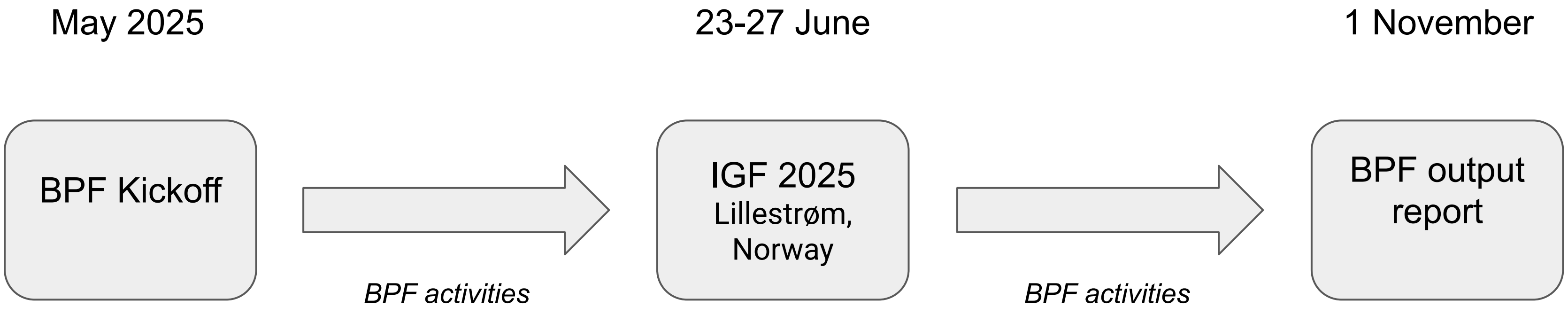
Norms elements & use of storytelling (2022)

Cybersecurity events to inform norms deliberation (2023)

-> Mainstreaming capacity building for cybersecurity, trust and safety online (2024)

These output reports are available on the BPF’s webpage at https://intgovforum.org/en/content/bpf-cybersecurity

IGF Best Practice Forum timeframe for 2025



May 2025

BPF Kickoff

BPF activities

23-27 June

IGF 2025
Lillestrøm,
Norway

BPF activities

1 November

BPF output report

IGF 2025 Best Practice Forum

Securing Access to the Internet and Protecting Core Internet Resources

in Contexts of Conflict and Crises

IGF 2024 Main session : Protecting Internet infrastructure and general access during times of crisis and conflict.

- Critical infrastructure includes technical infrastructure for internet access and telecommunications connectivity. (...) 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.
- All stakeholders must collaborate to ensure protection of essential telecommunications and internet infrastructure, even in times of 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.

BPF 2025 : Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises

- The thematic main session on '*Protecting Internet Infrastructure and general access during times of crisis and conflict*' at the IGF2024 in Riyadh 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 and access to the Internet for civilians in contexts of conflicts and crises.

- The BPF intends to evaluate key issues, challenges, and needs from the perspectives of different relevant actors and stakeholder groups. It will assess what work has been done, including through a literature review and identify good practices and gaps, and propose a forward-looking agenda for securing access to the Internet and protecting core Internet resources in contexts of conflict and crisis

- The BPF will adopt a holistic approach: preparing for crisis, prevention and protection under legal frameworks, resilience, mitigating impacts, and rebuilding and recovery.

BPF 2025 : Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises

Planned approach for 2025

Gather community and stakeholder input to

- Formulate a problem statement
- Identify the main challenges
- Identify applicable norms, agreements, processes; assess their relevance and adherence; identify any gaps
- Identify existing operational best practices

Work plan - next steps until July

- Call for written input *(May),* review of input & opportunity for community feedback *(June),* session at IGF 2025 (*23-27 June*)

Draft problem statement and call for written input

Draft 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 and protecting core Internet resources and ensuring civilian access to the Internet during conflicts and crises. ”

Call for written input

- Comment on the problem statement, suggest refinements, rephrasing, …
- What are the key challenges that need to be addressed
- What are relevant norms and processes
- Any practical good/best practices to share/document or any specific bad/not so good practices that can be addressed
- Stories or cases that illustrate the challenges and/or possible responses
- 1-2 pages, deadline 5 June

Discussion and feedback ?

Please share your thoughts on the BPF’s focus, work plan and draft problem statement

Conclusion and next steps

- New mailing list to advance the work
- General bpf cybersecurity mailing list remains active & announcements and updates will be shared

- Next BPF update - 1st week June (date/time tbc)

BPF webpage

www.intgovforum.org/en/content/bpf-cybersecurity