IGF 2025

Best Practice Forum

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

(BPF Cybersecurity)

BPF Main Session

Thursday 26 June, 2025, Lillestrøm, Norway

Key discussion points

This detailed summary of the BPF main session highlights the main conversations and conclusions and is intended to feed into further BPF work. The notes are based on the session recording, available at https://youtu.be/evZNOL7MtaE .

The session was moderated by BPF co-faciliator Anriette Esterhuysen (APC) and the introduction provided by BPF supporting consultant Wim Degezelle (IGF Secretariat). Panelists, in alphabetical order, were Chantal Joris (Article 19), Dennis Broeders (University of Leiden), Jalal Abukhater (7amlech), Madeline Carr (University College London), Marwa Fatafta (Access Now), Pablo Hinojosa (The Marconi Society).

Introduction

1. The Best Practice Forum (BPF) is an IGF intersessional activity, providing a platform for community-driven discussion on Internet policy issues and sharing of experiences. 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 BPF during the IGF 2025 cycle (BPF proposal). This builds on the thematic main session at the IGF2024 in Riyadh on 'Protecting Internet Infrastructure and General Access during times of crisis and conflict. The BPF webpage is the primary source for updates and key information about its work.

3. The work of the BPF is framed by the draft problem statement that '*there is a clear and pressing need to clarify the roles and responsibilities of the multistakeholder community - and the institutions within it - in securing core Internet resources and ensuring civilian*

access to the Internet during conflict and crises.' The statement is open for written community feedback.

Message on behalf of the UN Under Secretary General and High Representative for the Office of Disarmament Affairs (ODA)

4. Mr. Adedeji Ebo, Director and Deputy to the High Representative for the Office of Disarmament Affairs delivered a video message on behalf of the UN Under Secretary General and High Representative for the Office of Disarmament Affairs (ODA) reminded that safeguarding the critical digital components that ensure the general availability and integrity of the Internet across borders is essential for our shared digital future. International humanitarian law provides clear guidance and forbids deliberate attacks on civilian infrastructure and states have committed to a set of norms pertaining to the protection of critical infrastructure and not to conduct or knowingly support ICT activities that intentionally damages or impair the use and operation of critical infrastructure providing services to the public.

Internet access and the protection of core internet resources in context of conflict and crisis - case studies

5. The impact of crisis on Internet access in Gaza.
    - Ongoing collapse of the entire communications system in Gaza:
        - Repeated and deliberate blackouts
        - Near total destruction of the fixed landline infrastructure
        - June 2025 situation:
            - Fibre route targeted and destroyed
            - Redundancy has been lost
            - Mobile network may collapse due to lack of fuel, infrastructure, lack of spare parts
            - No repair missions permitted
    - Blackouts have severe consequences:
        - Medical agencies cannot coordinate aid
        - Emergency services are unreachable and unable to report
        - Civilians are not able to communicate or receive warnings
    - 'Digital erasure': connectivity is being used as a weapon of war, 2.2 million Palestinians in the Gaza strip remain digitally isolated
    - Norms perspective:
        - The destruction and obstruction of telecommunications infrastructure violates principles of international humanitarian law and human rights law:

        - The Geneva convention protects civilian infrastructure
        - Access to information is a recognised human right
    - Existing normative frameworks fail to protect lifelines in occupied or besieged territory, and there is no accountability
- Calls to stakeholders:
    - Treat telecom infrastructure the same way as water and electricity during humanitarian crises
    - Ensure enforceable protections for core infrastructure in situations of armed conflict
    - Establish enforceable emergency mechanisms for civil society humanitarian actors to deploy alternatives (e.g. by satellite, e-sim, potable networks)
- #ReconnectGaza is a campaign supported by over 16 organisations
- The World Bank estimates $164 million in damage to Gaza's ICT sector and $736 million in losses. Short-term reconstruction needs are put at $114 million, with total costs reaching $460 million.

6. Weaponising Internet access in Soudan
    - Destruction & occupation of infrastructure
        - Attacks against data centres in opposite controlled territory are used as a form of collective punishment against civilians
        - The occupation of datacentres and ISP offices has resulted in country-wide blackouts
    - Basic infrastructure maintenance as a political and logistical battlefield between warring parties
        - Access to spare parts and other critical components required for infrastructure repair is banned or restricted
        - Access to basic resources such as fuel and electricity, without which it not possible to provide Internet to civilians, is restricted

7. Restoring Internet access in Syria
    - 14 years of conflict have devastated large parts of Syria's infrastructure, including its telecommunications infrastructure
    - Challenges are magnified in sanctions-context, as restrictions make it difficult for private companies and telecommunication companies to import the equipment needed to repair, maintain, and run the infrastructure.
    - Internet connectivity is unreliable and fragmented
        - Parts of the territory rely on ISP under control of different warring parties
        - Northern regions rely on Internet connectivity through Turkey, and were cut off when Turkish authorities shut down the Internet in the aftermath of the 2023 earthquake

8. Disruption in the management of Internet core resources: AFRINIC
    - A functional RIR is essential for Internet stability. If a RIR does not function properly, this can, amongst others, make it harder to trust routing information and easier for cyber attacks to occur. This affects the global Internet.
    - AFRINIC, the Regional Internet Registry (RIR) for Africa, has faced over two years of institutional uncertainty, governance deadlock, and leadership gaps.
    - Lesson learned:
        - Internet resilience depends not only on infrastructure, but equally on people and organisations. Internet core resources can be at risk by weak governance, legal pressure in a specific jurisdiction, the absence of strong multistakeholder and community support.
        - The AFRINIC case challenges the long held view that non-interference is the best way to protect the Internet, and suggests that, sometimes, non-interference is not enough, and inaction can cause harm.
        - The multistakeholder model may not always be sufficiently strong on its own. Positive, protective measures are needed to help the people and organisations that ensure the Internet stays open, stable and secure.

Normative perspective on Internet access and the protection of core internet resources in context of conflict and crisis

9. Armed conflict has become the leading trigger of Internet shutdowns worldwide, according to #KeepItOn data. In such contexts, warring parties often treat civilian Internet infrastructure as a military target. Cell towers, fibre optic cables, switchboards, data centres, ISP offices, and even their maintenance and repair crews, can all come under attack. These are extremely complex situations, posing major challenges for civil society organisations that work to secure alternative connectivity.

10. The following three global frameworks are most relevant: International Humanitarian Law (or the Law of Armed Conflict); Human Rights Law; Protection of Critical Information Infrastructure.

11. International Human Rights Law
    - Any restriction on freedom of expression and on the right to share and receive information, must meet the tests of legality, necessity, and proportionality. This requirement applies equally to online environments and Internet-based communications.
        - For example, the Human Rights Court and other bodies have made clear that blanket shutdowns, because of their impact on populations, can never been justified under human rights law.

12. Humanitarian Law (Law of Armed Conflict)

- Humanitarian law does not provide an explicit protection of Internet access, nor an explicit prohibition of attacking Internet infrastructure or restricting Internet Access.
- Certain rules under Humanitarian Law become relevant depending the situation:
    - Warring parties need to respect international humanitarian law (Art. 1, Geneva Convention)
        - Example: an Internet shutdown to conceal violations of humanitarian law would be a violation
    - Protection of humanitarian organisations and hospitals (explicitly covered under several provisions of the Geneva Conventions and Protocols)
        - Example: this includes their ability to access and use ICT infrastructure, which enables them to operate effectively.
    - Rules on attack require distinguishing between civilian objects and military objectives. They prohibit attacking civilian objects (principle of distinction) and excessively causing incidental civilian harm (principle of proportionality) as opposed to the military objectives and combatants.
        - ICT infrastructure is often regarded as dual-use, which opens the door to allowing attacks:
            - 1st challenge: the proportionality requirement is forgotten or stretched
              For example, a HR lawyer and military advisor may make fundamentally different proportionality assessments of civil injury vs military advantage
            - 2nd challenge: lack of, or only partial, assessment of knock-on effects
              For example, what is the true impact of a shutdown? Are these factors taken into account: the impact on those unable to reach hospitals for help, the psychological impact on the affected population, the cost and losses caused a disruption of the banking services?

13. The gap between Human Rights law and Humanitarian law frameworks

- In practice, one is rapidly confronted with a scenario in which human rights law prohibits shutdowns or attacks, while international humanitarian law provides little or no mechanisms to limit such attacks in a specific setting.
    - There is a gap in the understanding of how both legal frameworks intersect and relate.
    - There is a need to work on a more systemic integration of both legal frameworks.

    - Human rights impacts should be explicitly considered within a proportionality analysis, and within proper humanitarian law

14. Protection of Critical Information Infrastructure - the public core of the Internet
    - International humanitarian law provides little protection for critical infrastructure, largely because the proportionality principle is very stretchy.
    - The ‘public core of the Internet’ concept encompasses core Internet protocols and infrastructure.
    - The protection of critical Internet resources and infrastructure that should be exempted from state interventions has been debated since 2015.
    - The public core is a negative norm (‘thou shall not’-norm). It represents a political commitment, yet implementation of negative norms is hard and traditional frameworks for norm implementation offer little support. The public core focuses on the large scale and transnational disruption of the Internet. (The AFRINIC case fits under the public core framework, whereas human rights lays seems a more appropriate framework for conflicts such as in Gaza and Syria.)
    - The central public core idea of ‘how to protect the integrity and availability of the global Internet’ has since surfaced in various discussions and fora. (UN, EU policy, OEWG, and more). The 2020 GGE report was the first acknowledgement by diplomats and states of the notion of a ‘transnational critical infrastructure’, a remarkable step given that critical infrastructure is typically regarded a strictly national prerogative.
    - Protecting the public core of the Internet is situated at the three layers of the Internet:
        - Physical / Technical infrastructure layer
            - Debates on the public core increasingly encompass cable and satellite infrastructure, though expert discussions caution against hype (attacks on cables happen, but are still rare) and for many stakeholders the issue feels novel (a Columbus Fallacy), despite substantial existing policy frameworks.
        - Logical / Protocol layer
            - Internet protocols were not originally designed with security in mind, leaving them vulnerable, yet significant efforts within the technical community have since sought to address these weaknesses.
        - Organisational / Governance layer
            - A politically grounded gentlemen's agreement assured that the organisation responsible for the core Internet functions are relatively free from sanctions.
            - In the context of the Russia/Ukraine war, ICANN and RIPE defended their role of ‘caretaker of network continuity’ and did not intervene.

They were exempt from sanctions, based on a so-called Internet carveout (G7, EU).
A similar reasoning was not followed in the case of Syria.

- The final outcome of the AFRINIC case will be interesting. If a decision were made to relocate the organisation to another country, it would signal that organisations managing the Internet's key resources are essentially moveable, and this potentially opens a new debate.

How does the multistakeholder community cope with situations of conflict and crises?

15. Norms and international relations are human processes, they involve human beings and organisations.
    - Ten years ago, cybersecurity was largely viewed as a technical problem requiring technical solutions. Today it is recognised that cybersecurity is a far broader challenge. Similarly, with regard to the public core of the Internet, attention should extend beyond the technical and institutional capacity and include the people within the organisations responsible for the maintenance of the public core.

16. The Multistakeholder Internet Governance Model is intended to protect and safeguard the public core. If it fails to function as intended, an urgent and honest discussion is needed about what can and should be changed.
    - In the three examples, Russia/Ukraine war, Gaza, AFRINIC, there is a risk of interference in the public core from both state and non-state actors, or even individuals (in the AFNIC case). The multistakeholder community, however, is responding differently:
        - Ukraine/Russia
            - Challenge to the public core is predominantly focussed on software protocols and services.
            - The MS model functioned well : RIPE & ICANN were articulate in their responses, and there was a public debate.
        - Gaza
            - Challenge to the public core predominantly through the hardware
            - There hasn't been a clear response from the MS community.
            - The MS community seems unprepared or unable to respond in this context and to promote the protection of the public core.
            - Moreover, prior to the current conflict and destructions, Gaza was already wholly or significantly dependent on Israel, which had the power to destroy the physical infrastructure, block repair, or prevent alternative solutions to connect. This situation has never been remedied by the Multistakeholder community.

17. There is an expectation that the Multistakeholder model would play a significantly more pro-active role in protecting the public core.
    - This raises the questions:
        - Is the MS community willing and/or able to respond in context like Gaza?
        - If so, how should it respond? What should happen that hasn't happened?
        - If not, then who is responsible and should act? (The Gaza case demonstrates that there is a gap in situations like this.

How can the IGF Best Practice Forum help advance these issues?

18. Be conscious of today's environment that is increasingly indifferent to rule-based international cooperation and compliance with existing frameworks, and support the protection of international law and of the institutions that protect international law (UN, International Criminal Court, etc.).

19. Explore the intersection with Internet resilience and examine key questions such as:
    - What could go wrong? What preventive measures and risk mitigation strategies can be adopted? Who is responsible to fund and invest in them?
    - How can local actors be empowered to technically and diplomatically respond in situations of crisis?

20. Establish a multistakeholder mechanism for emergency and rapid response to crisis:
    - The Internet has become a lifeline and live saving tool. A multi-stakeholder mechanism, that includes states, private sector, and civil society, should have the purpose to mobilise funding, equipment, political leverage (e.g. on warring parties to allow equipment to enter) in case of a crisis situation in a country or region.
    - As armed conflicts tend to be cyclical in nature, increasingly intractable, or open-ended, the multistakeholder mechanism should think beyond rapid response, and contribute to the rebuilding of resilient and independent infrastructure that would help communities to stay connected when the Internet becomes a weapon of war.

21. Further the discussion on the gap between Human Rights law and Humanitarian law frameworks and explore how missing links can be established. Also explore the role of corporate power in this context.

22. Evaluate and evolve the role of the Internet Multistaleholder community in a changed world:
    - Changed context for the MS model: for example, geopolitical changes

- Changes within the MS community: for example, concentration of corporate power and ownership of key infrastructure
- How do these changes affect the MS model?
- What can and what cannot be expected from the MS model ?
- How to strengthen the MS model, including its governance and operations, to ensure that it continues to serve its key purpose of enabling a functioning open and interoperable Internet?

Annexe, **Session description and draft agenda**

IGF 2025 Schedule https://sched.co/24FKt
Session Recording https://www.youtube.com/watch?v=evZNOL7MtaE

This main session is examining the **importance of securing Internet access and protecting core Internet resources in contexts of conflict and crisis situations** and is organised by the IGF Best Practice Forum on Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises, one of the IGF intersessional activities of the 2025 cycle. The session at the IGF serves as a cornerstone for the BPF's activities that span beyond the annual meeting in June.
The session is driven by the draft problem statement that **there is a clear and pressing need to clarify applicable norms, and the roles and responsibilities of different parts 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.**
Session objectives

- discuss and gather stakeholder input to **complete and refine the problem statement**
- examine **applicable norms and normative frameworks**, as well as any gaps or missing links
- identify next steps and inform the direction of **future actions under the BPF**

Call for written input : Stakeholders and invited to provide written feedback on the draft problem statement. Details are in the Call for written input.
Session outline

1. Opening and setting the scene
    1. Welcome and introduction
    2. Presentation of the BPF, the BPF 2025 topic and Objectives of the session

3. Message of the UN Office on Disarmament Affairs
4. Presentation of the BPF's draft problem statement and initial community feedback

2. Case studies
    1. Brief case studies will cover examples of destruction of infrastructure and disruption of access in conflict context, caused by natural disaster, and disruption in the management of core resources.
3. Discussion round 1: Normative Frameworks
    1. Reflecting on the different cases, what existing norms apply to the context of securing access and protecting core Internet infrastructure? Are they sufficient? Is there a need for adapting norms? Are there gaps to be filled?
    2. Does the existing work on the norm to protect the public core apply to this context? If so, how?
    3. Do Human Rights norms and International Humanitarian Law provide another angle to look at this context?
4. Discussion round 2: Accountability Frameworks and the Role of Stakeholders
    1. What accountability frameworks would support compliance with the relevant norms? Which institutions have a role in this contexts? What is the role of different stakeholders?
5. Next Steps and future actions under the BPF
6. Wrap up

Moderation, topic leads, panel

- Dennis Broeders, University of Leiden
- Madeline Carr, University College London
- Chantal Joris, Article19
- Jalal Abukhater, 7amleh
- Marwa Fatafta, Access Now
- Pablo Hinojosa
- Valeria Betancourt, MAG Member, BPF co-facilitator, remote moderator
- Anriette Esterhuysen, BPF co-facilitator, session moderator
- Wim Degezelle, BPF consultant, IGF Secretariat