Internet Governance Forum

BEST PRACTICE FORUM

ON SECURING ACCESS TO THE INTERNET AND PROTECTING CORE INTERNET RESOURCES IN CONTEXTS OF CONFLICT AND CRISES

November 2025

Disclaimer:

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

BEST PRACTICE FORUM
ON
SECURING ACCESS TO THE INTERNET
AND
PROTECTING CORE INTERNET RESOURCES
IN
CONTEXTS OF CONFLICT AND CRISES

United Nations Internet Governance Forum (IGF) Secretariat

Best Practice Forum on Cybersecurity

For questions regarding this publication, please contact*:* *igf@un.org*

Designed and produced by:

IGF Secretariat

Department of Economic and Social Affairs

United Nations

INTERNET GOVERNANCE FORUM

The Internet Governance Forum (IGF) is a global multistakeholder platform that facilitates the discussion of public policy issues pertaining to Internet governance. The IGF was one of the most important outcomes of the United Nations World Summit on the Information Society (WSIS). The Tunis Agenda, adopted on 18 November 2005, mandated the UN Secretary-General to convene a new forum for multistakeholder policy dialogue. The convening of the IGF was announced by the Secretary-General on 18 July 2006, with the inaugural meeting of the Forum held from 30 October to 2 November 2006.

The existing mandate of the IGF, as set out in paragraphs 72 to 78 of the Tunis Agenda, was extended for a further ten years in a resolution adopted by the UN General Assembly on 16 December 2015 (70/125), which served as the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society.

In between the two annual meetings, the intersessional work of the IGF is conducted in a community-centred, open, inclusive, cooperative, and collaborative, bottom-up manner. The intersessional work takes different forms, such as Best Practice Forums, Policy Networks, Dynamic Coalitions, capacity development activities, and close cooperation with the national, regional, and youth IGF initiatives, which continue throughout the year.

Institutionally, the IGF is supported by the IGF Secretariat, which is administered by the UN Department of Economic and Social Affairs (UN DESA). The programme of the annual IGF meeting is developed by its Multistakeholder Advisory Group (MAG), whose members are appointed by the UN Secretary-General. An IGF Leadership Panel, with members also appointed by the Secretary-General, has supported IGF strategic improvements since 2022.

So far, twenty annual meetings of the IGF have been held, nineteen hosted by governments and one conducted fully online due to the COVID-19 pandemic.

EXECUTIVE SUMMARY

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. The *BPF on Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises*, part of the IGF 2025 intersessional activities, explores the roles and responsibilities of the multistakeholder Internet community in maintaining civilian access to the Internet and ensuring the protection of the public core of the Internet during times of conflict and crisis.

The BPF consulted the community on the draft problem statement that *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.* The consultation indicated that concepts such as civilian access during crisis, core Internet resources, and the multistakeholder community, would benefit from additional refinement to help advance the discussion. It was further suggested that work on the topic include the perspective of the people directly impacted by loss of Internet access, explicitly reference the human rights dimension, and address pre-crisis prevention and preparedness, as well as active crisis management and post-crisis recovery.

A review of recent and ongoing conflicts and crisis situations lead to the following key observations:

- Internet shutdowns and disruptions have severe humanitarian and economic consequences, including loss of life, livelihoods, and access to essential services.
- International human rights (IHRL) and humanitarian law (IHL) provide a framework for protecting Internet access and core Internet resources, but there is a need for a better understanding of how these legal frameworks intersect and complement one another, to enable a more systemic integration of both approaches.
- Stakeholder engagement is essential to addressing the complex and multifaceted challenges related to securing access and protecting core resources in conflict contexts. The lack of clarity regarding roles and responsibilities hinders the multistakeholder Internet community's ability to respond to conflicts and crises.

The BPF identified and conceptualised three work areas for advancing the securing of civilian Internet access and the protection of core Internet infrastructure in crisis and conflict contexts. These work areas are:

1) Explore the scope, role, and objectives of a **multistakeholder emergency connectivity mechanism** that engages governments, humanitarian agencies, technical experts, private-sector providers, and civil society, to deploy, restore, and maintain emergency Internet access for civilian populations.

2) Engage stakeholders in a **normative discussion** to develop a shared understanding of how International Humanitarian Law (IHL) and International Human Rights Law (IHRL) interact and complement each other in imposing limitations on restrictions to Internet access, identifying where their obligations intersect, diverge, or require interpretive guidance - and to what extent they impose obligations on private entities.

3) Develop a shared understanding of the roles and responsibilities of the multistakeholder Internet community in protecting the public core of the Internet and maintaining civilian access during conflicts and crises. Promote and strengthen a **holistic multistakeholder governance approach** encompassing preparedness, prevention, protection, and recovery, and recognizing the interdependencies between technical, social, and economic factors.

The IGF community is encouraged to take forward the findings of this report, and to work together to develop and implement effective solutions for securing access to the Internet and protecting core Internet resources in contexts of conflict and crises.

LIST OF ACRONYMS

AFRINIC	African Network Information Centre
AU	African Union
AUC	African Union Commission
BPF	Best Practice Forum
DNS	Domain Name System
EU	European Union
ETC	Emergency Telecommunications Cluster
FOC	Freedom Online Coalition
G7	Group of Seven
GCSC	Global Commission on the Stability of Cyberspace
GGE	Group of Governmental Experts (UN GGE United Nations Group of Governmental Experts on developments in the field of ICTs in the context of international security
HRC	Human Rights Council (UN Human Rights Council)
ICCPR	International Covenant on Civil and Political Rights
ICANN	Internet Corporation for Assigned Names and Numbers
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IHL	International Humanitarian Law
IHRL	International Human Rights Law
ILO	International Labor Organization
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
MAG	Multistakeholder Advisory Group (IGF MAG)
NIS2	Directive on Security of Network and Information Systems 2 (EU NIS2 Directive)
NRIs	National and Regional IGF Initiatives
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-ended Working Group on ICTs in the context of international security

OHCHR	Office of the United Nations High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
PN / PNs	Policy Network(s) (IGF Policy Networks)
PPP	Public–Private Partnership
RIR	Regional Internet Registry
RIPE NCC	Réseaux IP Européens Network Coordination Centre
UDHR	Universal Declaration of Human Rights
UN	United Nations
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society

ACKNOWLEDGEMENTS

The Best Practice Forum (BPF) on Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crisis is an open multistakeholder effort conducted as an intersessional activity of the Internet Governance Forum (IGF). **This BPF output is the product of the collaborative efforts and valuable insights of the many contributors who participated in BPF webinars and the BPF main session at the IGF 2025 in Lillestrøm, Norway, or provided input via the mailing list and requests for feedback.**

We extend our gratitude to all participants of the BPF webinars and main session for their valuable contributions. Special thanks to the esteemed discussants and panelists to the BPF's main session at the IGF 2025 annual meeting, **Ms Chantal Joris**, ARTICLE 19, **Mr Dennis Broeders**, University of Leiden, **Mr Jalal Abukhater**, 7amleh, **Ms Madeline Carr**, University College London, **Ms Marwa Fatafta**, Access Now, and **Mr Pablo Hinojosa**. We wish to acknowledge **Mr Jochen Michels,** Kaspersky, **Ms Chantal Joris**, and **Ms Marwa Fatafta** for their significant contribution to the development of the three concept areas for further work.

The BPF activities were prepared and coordinated by a BPF Coordinating team consisting of **Ms Valeria Betancourt**, IGF MAG Member and BPF co-facilitator, **Ms Anriette Esterhuysen**, BPF co-facilitator, **Mr Wim Degezelle**, BPF consultant, IGF Secretariat.

CONTENTS

1. Introduction

1.1 IGF Best Practice Forum

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.

BPFs were introduced in 2014. Their objective is not to develop new policy or practices, but rather to collect existing good practices, share positive and negative experiences, and identify challenges that warrant further multistakeholder dialogue or the attention of policymakers, including within relevant decision-making bodies.[1]

BPFs operate on an annual cycle which starts with the selection and confirmation of their topic and focus by the IGF Multistakeholder Advisory Group (MAG). Since 2014, BPFs have addressed a broad range of topics and areas. An overview of the BPF outputs is available on the IGF website.

1.2 Topic Selection and Rationale

1.2.1 IGF 2024 Thematic Main Session

'Enhancing the digital contribution to peace, development, and sustainability' was one of the four thematic areas that structured the programme of the 19th annual IGF meeting, which was held in Riyadh at the end of 2024. The corresponding thematic Main Session, titled '*Protecting Internet infrastructure and general access during times of crisis and conflict'*, underscored the need 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 context of crisis and conflict.

This Main Session was organised at a time when the world had witnessed a series of events where access to the Internet and core Internet resources were either deliberately disrupted in the context of conflict, or destroyed as a result of natural disasters. The session was particularly interested in how the Internet multistakeholder community, which is committed to preserving an open and interconnected Internet to uphold the full enjoyment of human rights, is responding in such situations. The discussion revealed the absence of a coherent or consistent response across the cases that were analysed during the session.

The conclusions emerging from the Main Session called upon all stakeholders to collaborate to ensure the protection of essential telecommunications and Internet infrastructure, even in times of crisis. It further emphasized that technical bodies responsible for Internet governance must remain neutral in order to continue to be able to function effectively. They must be free from sanctions as

[1] IGF Best Practice Forums. Definitions, Procedures, and Modalities. https://www.intgovforum.org/en/filedepot_download/3405/2270

well as protected from misuse of legal processes and from unlawful or coercive pressures. It was also stressed that efforts should be undertaken across all major forums and institutions responsible for the maintenance of international peace and security to ensure open and secure access to telecommunications infrastructure and the protection of the public core of the Internet.

Participants of the Main Session suggested that the IGF Best Practice Forums could examine the roles and responsibilities of the multistakeholder community in ensuring the protection of the public core of the Internet and maintaining access during times of conflict and crisis.

1.2.2 IGF Messages

The Riyadh IGF Messages, which are sourced from the sessions held during the IGF 2024 annual meeting and finalised after the meeting following a period of community review, confirmed the Main Session's finding and stated that '*International peace and security forums and institutions must prioritize open, secure access to telecommunications infrastructure and the protection of the public core. The UN Security Council should monitor telecommunications in the conflicts, while peace and justice institutions ensure accountability for disruptions affecting fundamental rights and security. Collaboration among all stakeholders is essential to safeguard critical telecommunications and Internet infrastructure, even during crises. To advance the Global Digital Compact guidance discouraging Internet shutdowns, multistakeholder working groups and enhanced IGF Best Practice Forums should define the community's roles in protecting the public core and ensuring access during conflicts and crises.*'

The Kyoto IGF Messages from 2023 noted that *'The information space plays an increasing role in conflicts. Digital risks and restrictions on the free flow of information can harm civilians in conflict zones. Digital companies have become important actors in conflict and often find themselves in extremely challenging circumstances, having to ensure safety of staff and deal with demands made by belligerents. Alongside their responsibility to respect human rights and humanitarian law, they should be guided by the principle to minimise harm during conflict.'*

1.2.3 BPF Proposal for the 2025 Cycle

The IGF Multistakeholder Advisory Group (MAG) selected *Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises* as a topic for a BPF during the IGF 2025 cycle (BPF proposal, 14 April 2025). The proposal indicated that the BPF would undertake an analysis of the overall topic, assess key issues, challenges and needs from the perspective of various role players and stakeholder groups. It would assess work done, identify good practices and gaps, and set a forward-looking agenda for protecting the public core and securing access in conflict and crisis contexts. The BPF would adopt a holistic approach encompassing preparing for crisis, prevention, protection through legal frameworks, strengthening resilience, mitigation of impacts, rebuilding and recovery.

The initial step in the work plan was to gather stakeholder input on the topic and synthesize their perspectives, providing a foundation for the BPF's work. After that, the received input was reviewed and validated during the BPF Main Session at the IGF 2025 annual meeting in Norway in June, and the BPF examined priority areas for continued work for the remainder of the 2025 cycle and beyond.

1.2.4 BPF Scope

The BPF seeks to clarify the **roles and responsibilities** of the multistakeholder Internet community and the institutions that are part of it regarding the **assurance of civilian Internet access and the protection of core Internet resources in contexts of conflict and crisis**. This entails assessing the key issues, challenges, and needs from the perspectives of various relevant actors and stakeholder groups. This work requires adopting a holistic approach that addresses preparedness for crisis, prevention and protection under legal frameworks, resilience, impact mitigation, and rebuilding and recovery.

The **BPF does not address uses of the Internet in conflicts** that contravene international law, as could be the case for certain cyber or information operations.

Also, **the BPF does not address the lack of basic infrastructure** often resulting from socio-economic inequality. However, examining how pre-existing connectivity gaps exacerbate vulnerability when a conflict breaks out or crisis occurs, and affect both efforts to protect core Internet infrastructure and to assure or restore civilian Internet communication, is considered to be in scope.

2. Problem Statement

2.1 Draft problem statement

The work of the BPF is framed by a 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 core Internet resources and ensuring civilian access to the Internet during conflicts and crises."

The draft problem statement was developed during the BPF's kick-off call on 6 May 2025 and draws on the discussions held at IGF 2024, which are outlined above. Participants confirmed the scope of the BPF and viewed the draft problem statement as an appropriate starting point for the BPF's work cycle.

It was further agreed to provide the wider community with an opportunity to comment on the draft statement and to offer suggestions to complete or refine it. To this end, the draft problem statement was published on the BPF's webpage and circulated through its mailing list, inviting the community to review the text and submit feedback.

2.2 Unpacking the draft problem statement - community feedback

This section unpacks the draft problem statement in light of the feedback received from the community. It synthesises comments and observations expressed during the various BPF online meetings, as well as those raised during the BPF Main Session at the IGF 2025 annual meeting in Lillestrøm, Norway, and incorporates the written contributions submitted in response to the call for written feedback on the problem statement.

The feedback on the draft problem statement is organised around the key concepts of the statement, along with additional suggestions provided.

Civilian access

It is important to clarify the scope of "civilian access during a crisis". For instance, the focus may be on maintaining access to certain essential digital services and communications. In that case, ensuring access during a humanitarian crisis or armed conflict further requires a shared understanding of which infrastructures are essential for providing these services, as well as clarity on how they are governed across jurisdictions.

When seeking to conceptualise the notion of ensuring civilian access to the Internet, a number of questions arise that can help to clarify and further refine the concept. For example: could a state legitimately argue that a reduction in access and connectivity without shutting down the Internet is permissible? And if so, what are boundaries or minimum requirements that should apply? Recent cases suggest that reduced connectivity should not be regarded as more permissible than shutdowns. Throttling mobile connectivity to 2G, for instance, forces users onto unencrypted

networks, where they are more exposed and easily vulnerable to surveillance. Or, when in a conflict area 80% of the infrastructure is destroyed, the situation for the majority of the users equals a continuous shutdown.

Several States invoke certain use or abuse to justify shutdowns and destruction of infrastructure for reasons of public safety or citing national security risks. This raises the question whether and to what extent the notion of access to the Internet, and the infrastructure that enables it, can be decoupled from how that access is used.

Conflicts and crises

It should be acknowledged that "conflicts and crises" encompass both localised incidents and global disruptions, as well as different types of crises, such as armed conflicts and natural disasters, each of which have specific characteristics, particularities, and distinct constellations of parties and stakeholders that are involved.

Perspective of those directly affected

The draft problem statement is missing the perspective of the people who are directly impacted by loss of Internet access. Integrating this perspective would provide an additional justification of the work and bring the discussion to them. There are a lot of local organisations doing important work that lack visibility. Including them would enrich the conversation.

Connectivity or access?

Looking at connectivity in conflict situations through the lens of access rather than solely focussing on the protection of infrastructure may be helpful.

Framing access to connectivity within a multidimensional humanitarian protection framework, which is similar to an approach already applied in other contexts, could provide additional clarity. Within such a framework, access to connectivity could then be broken down into specific dimensions, such as safe access and reliable access, each of which can be clearly defined and operationalised.

Core Internet Resources

What constitutes "core Internet resources" remains a subject of debate and varies depending on the context in which the discussion takes place. More clarity, including through the use of sector-specific examples, would help to define a clear scope of the discussion. 'Some stakeholders view core resources in strictly technical terms—such as the DNS, IP addressing, root zone management, and routing infrastructure—while others take a broader approach, encompassing the socio-technical systems and institutional arrangements that support Internet continuity and resilience. This includes software supply chains, cloud and data service providers, and the underlying dependencies between CI sectors.'

The ambiguity around the definition of what are core Internet resources also hinders the operationalisation of the cyber norms. The lack of a common understanding of what are the core infrastructures and interdependencies between them, makes it difficult to coordinate responses during incidents that impact Internet accessibility.

Although there is no universally adopted definition of core Internet resources or critical information infrastructure, existing legislation and documents developed under the auspices of the United Nations can serve as useful references. For instance, the EU's NIS2 Directive (Annex I) or the report prepared by the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE Report) may provide helpful guidance.

While providing a fixed definition of core Internet resources may be challenging, it would be helpful to recognise that there are varying understandings among different stakeholder communities. This includes both narrowly technical components (e.g. DNS, IP routing) and broader socio-technical systems essential for Internet continuity. Depending on the interpretation of what is considered core Internet or information infrastructure, different stakeholders should be involved in its protection.

Many core Internet resources are inherently transboundary and disruptions can have regional or even global consequences. It is essential to acknowledge that these interdependencies exist to be able to understand the scale and nature of shared risks.

Multistakeholder Internet Community

The term “multistakeholder Internet community" is a familiar concept to the members of the UN IGF, however less familiar to other stakeholder not or not yet part of the IGF community. They, and new members to the IGF, could benefit from explicitly naming the key categories (governments, private sector, technical community, civil society, academia, as well as key actors such as the media and intergovernmental organisations). A precise description of the different stakeholders helps to clarify responsibilities and set expectations. In addition, it is advisable to explicitly refer to the key actors, such as service providers, different branches of the government (executive, legislative, judicial), technical operators, civil society, academia, the open-source community, network operators, technical community organisations (e.g., Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF)), private sector companies, intergovernmental organizations, including the UN and its specialized agencies (e.g. the International Telecommunication Union (ITU), the World Intellectual Property Organization (WIPO), the International Labor Organization (ILO), the World Health Organization (WHO) etc.), the African Union (AU), European Union (EU), etc..

Stakeholder roles

Referring to “stakeholder roles” may give the impression that stakeholders have clearly defined and static responsibilities. It would be more appropriate, and better in line with the distributed nature of both Internet governance and incident response, to emphasise and promote coordinated action and flexible collaboration among stakeholders.

The roles and responsibilities - and the legal obligations of some stakeholders - could be elaborated and clarified through a set of tools, including clear policies and guidelines, stakeholder agreements, regular communication and coordination, established crisis response protocols, as well as capacity building and training.

Moreover, there are different causes and scenarios for losing civilian access to the Internet. For example, the reason for not having access to the Internet may be the unavailability of electricity, a shutdown resulting from a government decision, a kinetic attack on the infrastructure, or a cyber attack. As a consequence, addressing or preventing the loss of Internet access may be context specific, requiring the involvement of different people, organisations and stakeholders.

Temporal scope – prevention & response

The problem statement should explicitly address both prevention and response phases and specify that roles and responsibilities apply during pre-crisis preparedness, active crisis management, and post-crisis recovery.

Human Rights reference

The problem statement would benefit from explicitly referencing the human rights dimension. It should, in particular, underscore the connection between securing civilian Internet access and protecting core resources in conflict and crisis contexts and the right to freedom of expression and access to information.

3. Securing Internet Access and Protecting Core Resources

3.1 Internet Access in Crisis Contexts: Realities & Challenges

This section draws on the examples shared during the BPF Main Session at the IGF 2025 annual meeting in Lillestrøm, Norway. The examples presented are intended to illustrate varying realities of Internet access in crisis situations. They are not intended as full case studies or detailed situation analyses.

Restricting Internet access to control information flows

In Sudan control over connectivity has been emerging as a tool to influence information flows or restrict communications.

The destruction and occupation of critical infrastructure have become deliberate tactics, with, for example, attacks on data centres in territories controlled by opposing forces used to harm civilians. The occupation of data centres and ISP offices has triggered widespread Internet blackouts across the country.

Maintenance of basic infrastructure has turned into both a political and logistical battlefield, as warring parties contest control over essential services. Access to spare parts and other critical components needed for repairs is often banned or heavily restricted. Moreover, essential resources such as fuel and electricity, without which Internet services cannot be maintained, are also limited and further impacting the digital isolation of civilians caught in the conflict.

Destruction of the communication system

The conflict in Gaza has led to the near-total collapse of the communications infrastructure in the conflict area.

Repeated and deliberate Internet blackouts have been reported, alongside the extensive destruction of fixed landline networks. As of June 2025, key fibre routes have been targeted and destroyed, resulting in the loss of network redundancy. The mobile network faces imminent collapse due to shortages of fuel, damage to infrastructure, and the unavailability of spare parts, with repair missions not permitted.

These blackouts have had severe humanitarian and operational consequences: medical agencies struggle to coordinate aid, emergency services are unable to communicate or report, and civilians are left without reliable means to connect or receive critical warnings.

According to World Bank estimates, the damage to Gaza's ICT sector totals $164 million, with additional losses of $736 million.

Restoring access during and after crisis

Fourteen years of conflict have severely damaged much of Syria’s infrastructure, including its telecommunications networks.

The situation is further complicated by the impact of international sanctions, which make it difficult for both public and private telecommunications providers to import the equipment and materials needed to repair, maintain, and operate essential infrastructure. As a result, Internet connectivity across the country remains unreliable and fragmented.

Different areas rely on Internet service providers controlled by various warring parties, leading to inconsistencies in access and service quality. In the northern regions, connectivity depends largely on infrastructure routed through Turkey. These areas experienced complete disconnection when Internet access was temporarily shut down in the aftermath of the 2023 earthquake.

Disruption in the management of core resources

The AFRINIC management crisis shows the risks of disruptions in the management of the Internet core resources.

A well-functioning Regional Internet Registry (RIR) is essential to the stability and security of the global Internet. When an RIR fails to operate effectively, it can undermine trust in routing information and increase the risk of cyberattacks, with consequences that extend beyond regional boundaries.

AFRINIC, the RIR responsible for Africa, has faced more than two years of institutional uncertainty, governance deadlock, and leadership challenges. This situation highlights an important lesson: Internet resilience depends not only on physical infrastructure but also on the strength and stability of the people and institutions that manage its core resources.

Weak governance structures, legal pressures within a specific jurisdiction, and a lack of multistakeholder or community support can all place Internet core resources at risk. The AFRINIC case challenges the long-held belief that non-interference is always the best way to safeguard the Internet. It suggests that, in some circumstances, inaction can be as harmful as interference. To ensure the Internet remains open, stable, and secure, proactive and protective measures are needed to support the organisations and communities that uphold its core functions.

3.2 Normative Perspective

Armed conflict has become the leading trigger of Internet shutdowns worldwide, according to #KeepItOn data. Cell towers, fibre optic cables, switchboards, data centres, ISP offices, and even their maintenance and repair crews, can all come under attack by conflict parties. This can cause considerable harm, cutting civilians off from potentially life-saving information about troop movements and humanitarian corridors and impede medical facilities and humanitarian agencies from operating properly. It can also curtail the documentation of human rights abuses and war crimes. While civil society organisations in many contexts work to secure alternative connectivity, this remains extremely challenging.

The most relevant international law norms to the protection of Internet access and Internet core resources in contexts of conflict and crisis are International Human Rights Law (IHRL) and International Humanitarian Law (IHL) (or the Law of Armed Conflict). In addition, political commitments have been made and soft law developed to support the protection of Critical Information Infrastructure.

3.2.1 International Human Rights Law (IHRL)

The primary norm under IHRL to protect and respect Internet access in times of conflict is the right to freedom of expression. Freedom of expression and the right to seek, receive, and impart information are protected under Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). Importantly, freedom of expression continues to apply during armed conflict, although it may be subject to derogations in line with Article 4 of the ICCPR 'in time of public emergency which threatens the life of the nation' (in practice, derogations under this provision are rarely invoked by states).

Any restriction on freedom of expression and of the right to share and receive information, must meet the tests of legality, legitimacy, necessity, and proportionality (referred to as the three-part test). Even where states apply derogation measures, it must be with due regard to the principles of legality, legitimacy, necessity, proportionality, and non-discrimination, according to the Human Rights Committee (General Comment No. 29). These requirements apply equally to online environments and Internet-based communications.

Based on these criteria, human rights bodies have, for instance, made clear that blanket shutdowns, because of their impact on populations, can never be justified under human rights law (for example, in the Office of the High Commissioner for Human Rights (OHCHR) report to the Human Rights Council on Internet shutdowns, A/HRC/50/55). The UN Human Rights Council has further condemned 'measures to intentionally prevent or disrupt access to or dissemination of information online' in its Resolutions on the promotion, protection and enjoyment of human rights on the Internet (HRC Resolution 32/13 (2016) and 47/16 (2021)). The four mandate holders on freedom of expression stated in their 2015 Joint Declaration that even in times of conflict, 'using communications "kill switches" (i.e., shutting down entire parts of communications systems) can never be justified under human rights law'.

3.2.2 International Humanitarian Law (IHL)

Limitations on connectivity disruptions may also be imposed by IHL. Particularly important are the Geneva Conventions and their Additional Protocols. They contain the most important rules restricting the means and methods of warfare and protecting persons who are not, or are no longer, participating in hostilities.

IHL does not explicitly protect Internet access, nor does it explicitly prohibit restricting Internet Access. Nevertheless, certain rules under IHL impose limitations on disruptions of Internet access. For example:

- The Protection of humanitarian organisations and hospitals (explicitly protected by several IHL rules).

  Example: disruptions to their ability to access and use ICT infrastructure, which enables them to operate effectively, could amount to a breach of the obligation to respect and protect humanitarian operations and medical missions.

- Key rules governing the conduct of hostilities include the principles of distinction, proportionality and precaution.

  For example, rules on attack prohibit attacking civilian objects (principle of distinction) and causing incidental civilian harm which would be excessive in relation

to the concrete and direct military advantage anticipated (principle of proportionality).

- Warring parties need to respect international humanitarian law (Art. 1, Geneva Conventions).
  Example: an Internet shutdown to conceal violations of humanitarian law could amount to an IHL violation.

Communication infrastructure is generally civilian in nature (even if pieces of civilian communication infrastructure can qualify as military objectives if they make an effective contribution to military actions and their neutralisation offers a definite military advantage). Yet, at times, the perception or classification of ICT infrastructure as 'dual-use' can present a challenge and potentially be exploited to legitimise attacks, even if such attacks are not in line with IHL. This places additional importance on the principles of precautions and proportionality which require that attention be paid to the length of the disruption, its scope, geographic reach and impact on civilian life.

A second challenge lies in how these principles are interpreted and applied, as well as how, in specific cases, the assessment of the expected civilian harm against perceived military advantage can vary depending on who carries out that assessment.

A third challenge concerns the extent to which knock-on effects resulting from attacks or shutdowns can be considered, including to the human rights of the affected communities. The full consequences of disrupting telecommunications infrastructure are hard to quantify and might be underestimated or ignored. It is not fully clear how questions such as the impact on people unable to reach hospitals, the psychological toll on affected populations, and the economic losses caused by the interruption of banking and other essential services ought to be factored into decision-making processes.

3.3.3 Complementarity, Intersection and Potential Gaps between IHL and IHRL

Given the above considerations, it is conceivable that an assessment of the legality of an Internet shutdown looking at either IHL or IHRL in isolation could result in different outcomes. In practice, one could be confronted with a scenario in which IHRL prohibits shutdowns or attacks on ICT infrastructure, while an assessment under IHL might be less clear. It also generally seems unclear whether rules under IHL or IHRL might be considered *lex specialis* in a given context concerning Internet shutdowns. Whether the shutdown is imposed in an international or non-international armed conflict, and whether it is actually linked to a military objective or is merely to restrict information for the civilian population can further be relevant in determining which legal framework should take precedence.

There is thus a need to better understand how the two legal frameworks intersect and complement one another and a need for a more systemic integration of human rights and humanitarian law approaches. For example, it is suggested that human rights impacts should be considered within IHL assessments, including proportionality assessments, to avoid contradictory outcomes.

3.3 Protection of Critical (Core) Information Infrastructure

In addition to the protection of Internet access and Internet core resources under binding international law norms, it is relevant to consider how the concept of the *public core of the Internet* has emerged to encompass the essential protocols and infrastructure that underpin global connectivity. Since 2015, the protection of critical Internet resources that should be exempt from state interference has been an active topic of debate. The formulation of the '*Norm to Protect the Public Core of the Internet*' by the multistakeholder Global Commission on the Stability of Cyberspace (GCSC) in 2017 marks a significant milestone.

> *"State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace."*
>
> (Norm to Protect the Public Core of the Internet, GCSC)

The public core represents a negative norm (a "thou shall not" principle) embodying a political commitment to refrain from certain actions rather than prescribing specific positive obligations. However, implementing such a political commitment is inherently difficult, as traditional frameworks for norm enforcement offer limited support. The concept primarily focuses on preventing large-scale and transnational disruptions to the Internet. While the AFRINIC case falls within the public core framework, human rights and international humanitarian law appears more suitable for addressing conflicts such as those in Gaza and Syria.

The central idea of protecting the integrity and availability of the global Internet has gradually gained traction across multiple international fora, including the United Nations, European Union, and Open-Ended Working Group (OEWG). The 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE report) marked a significant milestone as the first formal acknowledgment by diplomats and states of the Internet as a form of transnational critical infrastructure, which was a notable departure from the traditional view that critical infrastructure is a strictly national concern.

Efforts to safeguard the public core of the Internet can be understood across three interrelated layers:

- Physical / Technical Infrastructure Layer
  Recent debates increasingly address the protection of undersea cables and satellite systems. Experts, however, caution against exaggerating threats, noting that while attacks on cables do occur, they remain rare. For many stakeholders, the issue appears novel despite the existence of substantial policy frameworks that already cover much of this ground.
- Logical / Protocol Layer
  Many Internet protocols were not originally designed with security in mind, leaving them vulnerable to exploitation. However, sustained efforts within the technical community have sought to strengthen these protocols and address longstanding weaknesses.
- Organisational / Governance Layer
  A long-standing, politically grounded understanding has ensured that organisations responsible for core Internet functions operate with relative freedom from sanctions. During the Russia–Ukraine war, for example, both ICANN and RIPE NCC upheld their roles as

caretakers of network continuity, benefiting from an “Internet carve-out” under G7 and EU sanctions frameworks..

3.4 The Multistakeholder Community’s Response to Situations of Conflict and Crises

The *Multistakeholder Internet Governance Model* is designed to protect and safeguard the open and interoperable Internet and its public core. Crisis and conflict situations may pose a risk to this openness and interoperability. State and non-state actors may take actions that, deliberately or not, cause interference with the functioning of the Internet and the public core. The examples discussed above, including the situation in Gaza, Ukraine, Sudan, and the AFRINIC case, illustrate such contexts. Naturally, these issues lie at the heart of the multistakeholder model. It becomes interesting to see how the multistakeholder community responds across different situations.

In the context of the war in Ukraine, challenges to the public core have been focussed predominantly on software protocols and Internet services rather than on physical infrastructure. In this crisis, the multistakeholder model demonstrates its functionality. For example, RIPE and ICANN have been articulate about their responses to calls to revoke Russia's Internet domains and IP addresses in February 2022, which would have prevented Russian Internet users from accessing the global Internet. They rejected the requests, noting the importance of their neutrality in geopolitics to ensure the availability of a global Internet to all. In addition, RIPE NCC transparently documents actions it has undertaken in cases involving violations of RIPE policies, for example when IP address space allocated to Ukraine is or was at risk of being taken away from the country. Overall, one can observe that the war sparked a public debate within the multistakeholder community on how to react and the key organisations clarified their respective roles and positions.

In the context of Gaza, challenges to the Internet and its public core have largely stemmed from impacts on hardware and physical infrastructure. Unlike the situation in Ukraine, there has not yet been a coordinated or comprehensive response from the multistakeholder community. Even prior to the current conflict and resulting damage, Gaza’s connectivity relied almost entirely on infrastructure located in, or managed through, external networks. This longstanding dependency made the region particularly vulnerable to disruptions and limited the ability to undertake repairs or explore alternative options for ensuring continuity of service. These structural issues have yet to be fully addressed within the broader multistakeholder community.

While there is an expectation that the multistakeholder model should play a significant and pro-active role in protecting the public core, the situation in Gaza raises the question whether the multistakeholder community is willing and/or able to respond in such contexts, and how it should respond. If the multistakeholder model does not or cannot take on this role, a conversation is needed on who is then responsible and who should act. The current situation in Gaza suggests that there is a gap. An engagement of all relevant stakeholders is invaluable to address the complex and multifaceted challenges related to securing Internet access and protecting the core Internet resources in conflict contexts. The global community should navigate the different challenges in a balanced approach that considers concerns and needs from the various stakeholders, including national security needs, with principles of a global Internet to ensure that it remains a robust, secure, and open resource for all, even in the face of conflict and crisis. If the multistakeholder model does

not fulfill its envisaged purpose, an urgent and honest discussion is needed about what can and should be changed.

4. Advancing the Discussion and Work Areas

4.1 Advancing the Discussion

The BPF explored recent examples of conflict and crisis situations in which access to the Internet is challenged or impossible. It looked at the existing human rights and humanitarian law frameworks, the norm on protecting the public core of the Internet, and the role of the multistakeholder model in relation to protecting Internet access and core Internet infrastructure in crisis and conflict contexts. These discussions lead to the identification of three work areas for the BPF to further the work:

1) Support the establishment of a multistakeholder mechanism for emergency and rapid response to secure or restore connectivity in times of conflict or crisis.
2) Forster a discussion on addressing the gap between human rights and humanitarian law frameworks in the context of safeguarding civilian access to the Internet.
3) Foster a discussion on the role and functioning of the Multistakeholder model when it comes to securing access and protecting core Internet resources.

The three work areas are conceptualised in the sections below, with the intention that they are picked up, as part of a follow-up BPF or elsewhere. The concept notes dedicate special attention to identifying which stakeholders should be engaged in the work.

4.2 Defining three work areas

4.2.1 Multistakeholder Emergency Connectivity Mechanism

Restoring connectivity and providing civilian Internet access in conflict settings involves complex political, regulatory, administrative, and safety challenges. Effective response requires coordinated action, political will, resilient technical solutions, and sustained funding. No single actor can address these needs alone. A multistakeholder approach engaging governments, humanitarian agencies, technical experts, private-sector providers, and civil society, is therefore essential to deploy, restore, and maintain emergency Internet access for civilian populations.

Existing multistakeholder mechanisms for emergency connectivity are limited in mandate, scale, and scope, and do not fully address the growing political and human rights challenges posed by deliberate Internet shutdowns. For example, the ITU's emergency telecommunications programs primarily focus on climate events, natural disasters, and pandemics. The Emergency Telecommunications Cluster (ETC) provides connectivity in active conflict zones but largely prioritizes humanitarian actors rather than mass access for affected civilians. Civil society initiatives that provide circumvention tools and eSIMs, remain small-scale and limited in reach.

To address these gaps and the unique challenges posed by armed conflict, the BPF is well-positioned to explore the scope, role, and objectives of a multistakeholder emergency connectivity mechanism. Such a mechanism would aim to prevent, mitigate, and respond to intentional or incidental Internet

shutdowns in armed conflict by coordinating resources, deploying emergency infrastructure and tools, and safeguarding the digital rights of affected populations. This includes mapping existing mechanisms, assessing their strengths and limitations, defining objectives and operational models for a future mechanism, and identifying stakeholders for consultation. The BPF could convene relevant actors to evaluate needs, challenges, and design options, supporting the development of a detailed concept for how such a mechanism could be established and operationalized.

4.2.2 Normative Discussion

There has been growing momentum in clarifying the extent to which IHL constrains Internet shutdowns and connectivity disruptions. Recent developments include the publication in the July 2025 ICRC blog series examining the humanitarian consequences of connectivity loss and the application of IHL to such disruptions during armed conflict (on the humanitarian consequences of connectivity disruptions and on international humanitarian law and connectivity disruptions during armed conflict), as well as the June 2025 Freedom Online Coalition joint statement on protecting human rights online and preventing shutdowns in conflict situations.

Building on this, it would be of great value to engage relevant stakeholders in further dialogue to develop a shared understanding of how IHL and IHRL interact and complement each other in imposing limitations on restrictions to Internet access, identifying where their obligations intersect, diverge, or require interpretive guidance - and to what extent they impose obligations on private entities, in particular ISPs.

The discussion might also identify a number of underlying questions that manifest in the context of Internet access in conflict and that require additional research. The aim should be to help move the discussion toward a shared normative position that can be promoted to states, international organisations, and other stakeholders, thereby contributing to greater coherence in how civilian access to the Internet, connectivity disruptions, and shutdowns, are evaluated and regulated across different contexts.

The IGF and the BPF are well suited to provide a space to facilitate this work, convene stakeholders, support the discussion, and document and promote its outcomes.

4.2.3 Multistakeholder Governance Discussion

One of the critical areas of discussion, particularly relevant in today's geopolitical landscape, is the protection of core Internet resources and securing access to the Internet in contexts of conflict and crises. This chapter delves into the ongoing discussions to address these challenges and aims to specify the most pertinent issues and determine the different stakeholders that should be engaged.

Introduction to the Challenge

The Internet, by its very nature, is a global network of interconnected systems, relying on a complex infrastructure that includes undersea cables, satellite communications, and a myriad of physical and virtual servers. This infrastructure is critical for the functioning of modern society, supporting everything from communication and commerce to education and healthcare. However, its global and interconnected nature also makes it vulnerable to both physical and digital threats, especially in contexts of conflict and crises.

In recent years, several countries have been developing and implementing new laws and regulations aimed at increasing the resilience of their critical communications infrastructure. These measures are designed to protect against cyberattacks, ensure data sovereignty, and maintain the integrity of the Internet within their jurisdictions. While these efforts are understandable from a national security perspective, they also raise important questions about their potential impact on the global Internet ecosystem.

Global Implications of National Measures

The primary concern with national measures to secure critical infrastructure is their potential to fragment the Internet. When countries implement laws and regulations that affect how data is routed, stored, and accessed within their borders, it can lead to a situation where the global Internet becomes less interconnected. This fragmentation can undermine the very principles of the Internet, which are based on openness, interoperability, and the free flow of information.

Moreover, such measures can have unintended consequences, including the creation of barriers to access for certain groups of people, undermining the efforts to achieve universal and equitable access to the Internet. This is particularly concerning in the context of developing countries, where access to the Internet is already limited, and any additional barriers could exacerbate existing digital divides.

The Role of International Cooperation

Given the global nature of the Internet, addressing the challenges of securing access and protecting core Internet resources in contexts of conflict and crises requires international cooperation. The IGF, with its multi-stakeholder approach, provides a unique platform for such cooperation. By bringing together governments, international and intergovernmental organizations, civil society, the private sector, and the technical community, the IGF facilitates discussions that consider the diverse perspectives and needs of all stakeholders.

Technological Solutions and Considerations

From a technological perspective, several solutions and considerations are being explored to enhance the security and resilience of the Internet. These include the development of more secure protocols for data transmission, the implementation of robust cybersecurity measures, and the use of emerging technologies like blockchain for enhancing the security of critical infrastructure.

However, the adoption of these technologies must be considered in the context of their potential impact on the global Internet. For instance, while technologies that enhance security are welcome, they should not create unnecessary barriers to access or undermine the principles of net neutrality. Furthermore, the development and implementation of these technologies should be guided by international standards and best practices to ensure interoperability and consistency across different jurisdictions.

Proactive Measures for Resilience

To increase the resilience of core elements of Internet infrastructure before a crisis occurs, states, industry, and international organizations can take several proactive measures. States can invest in redundant infrastructure, such as backup servers and diverse routing paths, to ensure that critical Internet services remain available even if part of the infrastructure is compromised. They can also implement robust cybersecurity measures, including regular vulnerability assessments and

penetration testing, to protect against cyber threats. Furthermore, states can develop and implement national cybersecurity strategies that include provisions for the protection of critical Internet infrastructure. The industry, on the other hand, can adopt best practices in cybersecurity, such as implementing secure-by-design principles in the development of Internet infrastructure and services. Technical community and international organizations can play a crucial role by facilitating the development of global standards and guidelines for the security and resilience of Internet infrastructure, as well as providing capacity-building programs for countries to enhance their capabilities in these areas. Additionally, international and intergovernmental organizations can facilitate information sharing and coordination among countries to respond to cyber threats and other crises that may affect the Internet. By taking these proactive measures, the global community can reduce the risk of Internet disruptions and ensure that the Internet remains a stable and secure platform for communication, commerce, and innovation, even in the face of crises.

In the context of international cooperation, organizations such as the ITU, IETF, or ICANN play critical roles. The ITU, for example, works on developing global standards for telecommunications and the Internet, including standards related to cybersecurity and infrastructure resilience. ICANN, on the other hand, is responsible for the global coordination of the Domain Name System (DNS).

Further work

The discussion around securing access to the Internet and protecting core Internet resources in contexts of conflict and crises is complex and multifaceted. As countries continue to develop and implement measures to secure their critical communications infrastructure, it is essential to consider the potential global implications of these actions.

The contributions to these discussions of (i) international organizations like the United Nations (in particular the ITU), Organization for Security and Co-operation in Europe (OSCE), the Council of Europe, the European Union, the African Union and similar organizations in other regions of the world like the African Union Commission (AUC), Smart Africa, (ii) multistakeholder platforms like the IGF and the National and Regional IGF initiatives (NRIs), (iii) cooperation between public and private sector on national, regional and global level (like the Paris Peace Forum), (iv) industry associations on national, regional and global level, (v) cybersecurity industry, (vi) academia, and (vii) civil society, are invaluable, bringing different perspectives, concerns, expertise and experience to the table. As the global community navigates these challenges, an approach that strengthens resilience, protects access to the Internet and upholds international law should be actively pursued. By working together and adopting a multistakeholder, collaborative approach, we can ensure that the Internet remains a robust, secure, and open resource for all, even in the face of conflict and crises.

In the end, the key to success lies in securing access, and the free flow of information in line with international law obligations, and in particular international human rights and international humanitarian law, recognizing that the Internet's strength lies in its global interconnectedness and its ability to facilitate communication and innovation without borders. As such, ongoing dialogue and cooperation at the global level are not just beneficial but essential for the long-term health and viability of the Internet as we know it.

Furthermore, the development of new technologies and the evolution of the Internet ecosystem will continue to present both opportunities and challenges for the security and resilience of the Internet. Emerging technologies like the Internet of Things (IoT), 5G networks, and quantum computing will introduce new vulnerabilities and risks, but they also offer potential solutions for enhancing security

and resilience. The global community must be prepared to adapt and evolve in response to these changes, ensuring that the Internet remains a secure, stable, and open platform for generations to come.

Ultimately, the protection of core Internet resources and the securing of access to the Internet in contexts of conflict and crises require a sustained effort and commitment from all stakeholders. By prioritizing international cooperation, adopting proactive measures for resilience, and embracing a multi-stakeholder approach, we can build a more robust and secure Internet infrastructure that supports the needs of all people, regardless of their location or circumstances. This is a challenging but critical task, as the future of the Internet and its ability to drive economic, social, and political development depend on it.

5. BPF 2025 Takeaways and Way Forward

Internet shutdowns and disruptions have severe humanitarian and economic impacts, which are further exacerbated in contexts of conflict and crisis. Loss of civilian access to the Internet can put people or populations off from vital information and essential services, including health and emergency assistance, and may lead to the loss of life and livelihoods.

A consultation on the BPF's problem statement confirmed the need to clarify the roles and responsibilities of the multistakeholder Internet community, and the institutions within it, in ensuring civilian access and the protection of core Internet resources in conflicts and crisis situations. To advance the discussion, concepts such as civilian access during crisis, core Internet resources, and the multistakeholder community, need clarification and refinement, and it should not be assumed that all stakeholders share the same understanding. It is also important to consider the perspective of the people directly impacted by loss of Internet access, explicitly reference the human rights dimension, and address pre-crisis prevention and preparedness, as well as active crisis management and post-crisis recovery.

Based on a review of the situation of Internet access and disruptions in recent and ongoing conflicts and crisis situations, three concrete areas for further work were identified:

1. Developing a multistakeholder emergency connectivity mechanism to responding to Internet shutdowns and disruptions.
2. Enabling a more systemic integration of the international normative frameworks (IHL and IHRL).
3. Promoting and strengthening a holistic multistakeholder approach to securing access and protecting core resources that encompasses preparedness, protection, and recovery.

The BPF, in this report, developed concept notes for the three work areas, outlining the key questions and challenges, proposing the objectives of the work, and identifying stakeholders, stakeholder groups, organisations and institutions, that should be involved in taking the work forward.

The IGF and BPF are well suited to provide the space to further the work in the three areas, convene the stakeholders, support the discussions, and document and promote the outcomes. The work will require actively reaching out to and engaging of relevant stakeholders, institutions, and organisations, including some that are not regular participants in the IGF community.

For a continuation of the work, it will also be important to intentionally draw on the richness of the IGF ecosystem, in particular the work, insights, and networks of the NRIs, Dynamic Coalitions, and the IGF intersessional work carried out by the Policy Networks. While there is a strong case for advancing the work in three separate and focused streams to allow for deeper analysis, there is also concern that this should not result in the creation of siloed discussions. The BPF, as a focal point, can help ensure that the three different strands of discussion remain connected.

Annexes

Annexe 1 Thematic Overview of Sources of Protection of Civilian Internet Access

The protection of Internet access and core resources in conflict and crisis contexts is a complex issue that involves the interplay of various international law norms. This annex provides a non-exhaustive overview of relevant norms and standards.

International Human Rights Law (IHRL)

Right to Freedom of Expression

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) protects the right to freedom of expression, which includes the right to seek, receive, and impart information through any media. This right is essential for ensuring access to information and promoting transparency and accountability in conflict and crisis situations.

Derogations and Limitations

While states may derogate from certain human rights obligations in times of public emergency, such derogations must be in accordance with the strict requirements of Article 4 of the ICCPR. Any limitations on the right to freedom of expression must be necessary, proportionate, and non-discriminatory.

State Responsibility

States have a responsibility to respect and protect human rights, including the right to freedom of expression, in their own territory and in territories under their effective control. This responsibility extends to ensuring that Internet access is not arbitrarily restricted or disrupted.

International Humanitarian Law (IHL)

Protection of Civilian Infrastructure

IHL prohibits attacks on civilian infrastructure, including communication networks and Internet infrastructure, unless they are being used for military purposes. Even then, attacks must be proportionate and distinguish between military targets and civilian objects.

Principles of Distinction, Proportionality, and Precautions

IHL requires that parties to a conflict distinguish between military targets and civilian objects, use proportionate force, and take precautions to minimize harm to civilians and civilian infrastructure.

Humanitarian Access

IHL requires that parties to a conflict allow humanitarian access to affected populations, including access to communication networks and Internet infrastructure.

Intersection of IHRL and IHL

Complementary Regimes

IHRL and IHL are complementary regimes that provide a framework for protecting human rights and humanitarian law in conflict and crisis situations. While IHRL applies at all times, IHL applies in situations of armed conflict.

Normative Gaps

Despite the complementary nature of IHRL and IHL, there are normative gaps that need to be addressed. For example, IHL does not explicitly protect Internet access, while IHRL may not provide clear guidance on the protection of Internet infrastructure in conflict situations.

Interpretation and Application

The interpretation and application of IHRL and IHL in conflict and crisis situations require careful consideration of the specific context and the principles of international law.

Emerging Norms and Standards

UN General Assembly Resolutions

The UN General Assembly has adopted several resolutions that recognize the importance of Internet access and the need to protect it in conflict and crisis situations.

Human Rights Council Resolutions

The Human Rights Council has adopted resolutions that condemn measures to intentionally prevent or disrupt access to or dissemination of information online.

Industry Standards and Best Practices

The development of industry standards and best practices for protecting Internet access and core resources in conflict and crisis situations is essential for promoting responsible behavior and minimizing harm to civilians.

Annexe 2 Overview of BPF Activities in 2025

BPF Kick-off meeting (virtual) - 6 May 2025

Summary

BPF Meeting II (virtual) - 17 June 2025

Summary

BPF Main Session, IGF 20th annual meeting, Lillestrøm, Norway - 26 June 2025

Session recording

Summary

BPF Meeting IV (virtual) - 3 September 2025

Summary

BPF Meeting V (virtual) - 29 October 2025

Summary

BPF Meeting VI (virtual) - 27 November 2025

Summary

Call for written feedback on the draft problem statement

Call for feedback

Written contributions received: Geneva Dialogue on Responsible Behaviour in Cyberspace, Kaspersky, Dino Cataldo Dellaccio.

Input received on the draft problem statement during the BPF meetings is reflected in the meeting summaries.

FOR MORE INFORMATION

intgovforum.org

x.com/intgovforum

facebook.com/intgovforum

youtube.com/user/igf

instagram.com/intgovforum/

LinkedIn: http://bit.ly/3WAdncR

IGF Internet Governance Forum