

Joint Statement on Protecting Human Rights Online and Preventing Internet Shutdowns in Times of Armed Conflict

We, the undersigned Members of the Freedom Online Coalition (FOC), affirm the importance of a global, free, open, secure, and interoperable Internet and other digital communications services in times of armed conflict.

Building on its previous Joint Statement on State-Sponsored Network Disruptions, the undersigned Members of the FOC express deep concern that Internet shutdowns and restrictions to digital communications services during situations of armed conflict:

- **Exacerbate grave humanitarian crises**, with potentially life-threatening consequences for individuals and communities. Shutdowns hinder crisis-affected populations' access to life-saving information, protection mechanisms, vital services and humanitarian assistance. Furthermore, they hinder independent reporting and reduce international oversight of armed actors' behaviour.
- **Amplify vulnerabilities and inequalities**, due to the effect on those without support networks or resources, perpetuating instability and prolonging dependence on temporary solutions.
- **Disrupt the integrity of the most essential digital communications services and the wider information ecosystem**, which is at risk of being affected or exploited by warring parties. As the FOC [already recognised](#)¹, building and sustaining information integrity online is a complex but imperative endeavour.
- **Exacerbate or facilitate human rights violations and abuses**. Of particular concern is the disconnection of whole areas, or full communication blackouts, which may result in international crimes and other violations or abuses of human rights and humanitarian norms, perpetrated in the dark. Affected communities are unable to seek protection, and the international community remains unaware until it is too late.

Global, free, open, secure, and interoperable access to the Internet is essential during armed conflict, allowing people to request, access, or deliver aid and obtain or share vital information and early warnings. This access also enables humanitarian actors to coordinate operations and distribute information and aid, and is equally crucial for post-conflict restoration and peacebuilding.

The undersigned Members of the FOC fully support the UN Secretary General's view in the [Roadmap for Digital Co-operation](#) that '*special attention should also be given to ensuring connectivity in times of crisis and in humanitarian operations*' and that connectivity is '*a foundation to ensure the continuation of critical services*'. The undersigned Members of the FOC also welcome the commitment in the Global Digital Compact to '*refrain from Internet shutdowns and measures that target internet access*'.

¹

<https://freedomonlinecoalition.com/wp-content/uploads/2024/03/FOC-Joint-Statement-on-Information-Integrity-Online-and-Elections.pdf>



We call on States to:

1. Comply with International Humanitarian Law (IHL), during times of armed conflict, as well as International Human Rights Law (IHRL), as applicable.
2. Advocate for and uphold a global, free, open, secure, and interoperable Internet and other digital communications services during times of armed conflict.
3. Promote and protect information integrity online during times of armed conflict, in a manner that supports the right to freedom of opinion and expression, which includes the freedom to seek, receive, and impart information, including online, in a manner consistent with applicable IHL and IHRL.
4. Protect civilian infrastructure, which is critical to the provision of essential services and the delivery of humanitarian assistance. In times of armed conflict, refrain from directing attacks against civilian objects, including Internet, energy, and telecommunications infrastructure, in accordance with applicable IHL, as well as directing attacks against telecommunication employees and technicians and other civilian actors working to provide or maintain communications and connectivity to affected communities, unless, and for such time as, they are taking a direct part in hostilities.
5. Refrain from imposing policies that may impede connectivity, degrade bandwidth, or render civilian telecommunications systems non-operational in conflict-affected areas, where prohibited under IHL, or human rights law, as applicable - including imposing arbitrary restrictions or bans on the transfer and installation of internet and telecommunications equipment and/or materials necessary for the operation, maintenance, and repair of civilian telecommunications infrastructure in conflict zones.
6. In cases of disruption of connectivity and communications, advocate for and adopt an inclusive, community-driven, multistakeholder approach to efforts that support, protect, and facilitate unrestricted access to and installation of any communications systems, components, and equipment necessary for restoring and maintaining connectivity for life-saving facilities such as hospitals, water and electricity utilities, and shelters, as well as for humanitarian actors and impacted communities themselves.

We urge online platforms and the broader tech industry to:

1. Combat malicious efforts to undermine access to information via the Internet and digital technologies, to humanitarian aid, and to protection during times of armed conflict.
2. Conduct human rights due diligence, in continued and close collaboration with the multistakeholder community, to assess, mitigate, and remedy any adverse human rights and humanitarian impacts of their policies, products, and services.
3. Work collaboratively with the wider multistakeholder community to develop and implement transparent and human rights-based crisis preparedness protocols, including around maintenance and restoration of connectivity and repairs to infrastructure in situations of armed conflict.

To view the list of signatories, please visit the [FOC website](#).

