Access Now's Submission to the First States Consultation on the ICT workstream to inform the Global Initiative to Galvanize Political Commitment to International Humanitarian Law

15 June 2025

Full written version of oral statement

Excellencies,

Dear chairs,

Access Now welcomes this opportunity to contribute its input to the ICT workstream of the Global Initiative to Galvanize Political Commitment to International Humanitarian Law, on the human cost of ICT operations and on the spread of harmful information during armed conflict, and more broadly on emerging digital issues in the protection of civilians in armed conflict,[1] and expresses its full support to the ICRC and the States promoting this important endeavor.

Access Now routinely engages with the international community in support of our mission to extend and defend digital rights of people and communities at risk around the world.[2] As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights, such as in situations of conflict and violence.

[1] See reference material: United Nations Security Council, *Protection of civilians in armed conflict,* 14 May 2024, UN Doc. S/2024/385, available at: https://docs.un.org/S/2024/385

[2] About Us, *Access Now* (2025), available at: https://www.accessnow.org/

We welcome the broad consensus on the fact that "cyber operations during armed conflicts, or cyber warfare, are regulated by IHL – just as is any weapon, means or methods of warfare used by a belligerent in a conflict, whether new or old,"[3] and that human rights persist during war.

But as we have seen during the debate, several points of contention between various policies and visions related to the role and status of ICT in conflict remain.

Access Now is a firm believer in the life-saving and rights-enabling power of digital technologies. We are also aware of the harms that these can and do generate, when used against or outside of protective normative frameworks such as human rights and humanitarian norms and principles.

The devastating humanitarian consequences of ICT-related activities are often defined as potential. Indeed, we cannot ignore the potential risks and threats posed by emerging technologies in warfare, such as lethal autonomous weapons systems, and we welcome and support the ongoing efforts to ban and regulate some of their uses.

However, we must first and foremost recognize the existing impact of ICT-related threats already faced by civilians globally, often facilitated by gaps in applying humanitarian norms or principles to technology. More digital technologies in conflict is resulting in additional harms for civilians: the response cannot and should not only be "more technology will fix this".

For example, biometric surveillance and automated targeting through data-driven cloud systems should purportedly help in better implementing the principle of distinction, but the catastrophic human impacts of today's tech-enabled conflicts clearly contradict this claim.

By their very nature and function, automated target generation systems used for military purposes are rarely disclosed to the public– let alone audited. These systems are known to make mistakes, which in the case of armed conflict are very likely to have lethal and irreversible consequences. Opacity in ICT systems design, development, deployment, and oversight makes the concept of accountability ring increasingly hollow.

In the legal debate over the existence and definition of attack in an ICT-enabled world, we testify that communities experiencing loss of functionality or control over essential assets or systems due to ICT or ICT-related activities definitely feel under attack, even when they suffer no physical impact.

This explains the many and often unexpected ways in which harms are generated, enabled or amplified through ICT-related activities, such as the denial of access to essential digital services, or emerging ICT-enabled forms of ill-treatment or torture.[4] Those States that have already suffered from ICT-related activities against their core services such as hospitals or power plants, have seen those harms hit their citizens in a clear and unambiguous way, even without a kinetic event.

[3] Laurent Gisel, Tilman Rodenhauser and Knut Dormann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts* (2021), available at: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf

[4] Owen Bowcott, *UN warns of rise of 'cybertorture' to bypass physical ban*, The Guardian (2020), available at: https://www.theguardian.com/law/2020/feb/21/un-rapporteur-warns-of-rise-of-cybertorture-to-bypass-physical-ban

But not all unfriendly ICT activity is an act of war, or a military attack, or direct participation in hostilities. We stress the importance of protecting civilian ICT systems from the concerning trend of repurposing or abusing them for military purposes, and the mirroring reflex of labeling any unfriendly ICT-related activity as direct participation in hostilities. Civilian ICT infrastructure and civilian data systems are not dual use objects, but rather civilian objects essential to the survival of the civilian population and should be protected as such.

The normalization of ICT-related harms is nowhere as visible as in the dramatic increase in blanket shutdowns imposed by warring parties and other third-party actors[5] within and across borders through the tampering and outright destruction of civilian ICT infrastructure, regardless of any assessment of distinction and proportionality.

Shutdowns have several causes:[6] states ordering ISPs to interrupt services, sabotage by hackers, airstrikes against infrastructure, or depriving data centers or towers of energy or fuel. We know the activities that lead to shutdowns, but we have no agreed framework to define responsibility for protecting or restoring the digital lifeline, and accountability for those undermining it.

Today, conflict is by far the leading trigger for shutdowns globally[7] and the resulting harms are punishing and immediate, but can also last for months to years,[8] impacting nearly every aspect of modern life.

Shutdowns prevent civilians from receiving early warnings, block their access to critical and life-saving emergency services and medicine,[9] and hinder humanitarian coordination and response by aid groups, including in areas also impacted by natural disasters.[10] Shutdowns create a shroud of darkness for accountability,[11] and can enable war crimes and atrocities.[12]

Parties to conflict, third-party actors, oversight bodies, and all other stakeholders must ensure by all means necessary that civilians in conflict affected areas, as well as those fleeing, refugees, and the displaced, maintain reliable access to ICT infrastructure and essential communications platforms at all times.

Just like shutdowns, the spread of harmful information generates mistrust and forces already vulnerable communities into information vacuums with no access to reliable life-saving information, with staggering consequences: mass displacement, collapse of protection mechanisms, inter-community violence, mistrust of humanitarian actors hindering their response

[5] Access Now, *Lives on hold: internet shutdowns in 2024* (2025), available at: https://www.accessnow.org/internet-shutdowns-2024/

[6] Access Now, *Ending Internet Shutdowns* (2025), available at https://www.accessnow.org/issue/internet-shutdowns/

[7] Access Now, *Lives on hold: internet shutdowns in 2024* (2025), available at: https://www.accessnow.org/internet-shutdowns-2024/

[8] Access Now, *Stranded, suffocated, and in pain: 15 stories from Tigray's internet siege* (2023), available at: https://www.accessnow.org/15-stories-from-tigrays-internet-siege/

[9] Access Now, *The Sudan conflict: how internet shutdowns deepen a humanitarian crisis* (2024), available at: https://www.accessnow.org/the-sudan-conflict-how-internet-shutdowns-deepen-a-humanitarian-crisis/

[10] Access Now, *Joint statement: Myanmar must lift internet restrictions following devastating earthquake* (2025), Available at: https://www.accessnow.org/press-release/call-for-lifting-of-internet-restrictions-myanmar/

[11] Access Now, *Evading accountability through internet shutdowns: Trends in Africa and the Middle East* (2023), available at: https://www.accessnow.org/wp-content/uploads/2023/03/Evading-accountability-through-internet-shutdowns.pdf

[12] Access Now, *Legal explainer: Internet and telecommunications shutdowns in the assessment of international crimes* (2024), Available at: https://www.accessnow.org/wp-content/uploads/2024/02/Shutdowns-and-ICL-Legal-Explainer.pdf

or threatening their safety.[13]

Finally, ICT-related attacks raise jurisdictional challenges for victims as the geographical concepts of frontlines and warzones loses its centrality: remote systems, cyberattacks, doxxing, and smear campaigns generate conflict-related vulnerabilities in faraway communities, and conflict-related harms can be caused by perpetrators in non-conflict areas.

I thank you all for your attention and the organizers for their work, and I remain available to discuss in further detail these complex issues.

[13] Access Now, *Content and platform governance in times of crisis: applying international humanitarian, criminal, and human rights law* (2023), Available at: https://www.accessnow.org/wp-content/uploads/2024/01/Content-Governance-and-Platform-Accountability-in-Times-of-Crisis-update.pdf

Consolidated responses to guiding questions and recommendations

Which ICT activities during armed conflict pose a threat or risk of harm either directly or indirectly to civilians and civilian objects?

Any weaponization or targeting of civilian ICT objects and systems inevitably results in forms of harm to civilian and civilian objects, either through enhanced exposure to a protection risk, by suspending their protected status, or by infringing upon key human rights in conflict.

A clear example can be attributing an alleged dual use nature of civilian ICT infrastructure in order to legalize and normalize their indiscriminate and wanton destruction by stripping it of its protected status as an essentially civilian object. Over the past two years, conflict has been by far the leading trigger for shutdowns globally and the resulting harms are punishing and immediate, but can also last for months to years,[14] impacting nearly every aspect of modern civilian life.

Shutdowns prevent civilians from receiving early warnings, block their access to critical and life-saving emergency services and medicine,[15] and hinder humanitarian coordination and response by aid groups,[16] including in areas also impacted by natural disasters.[17] Shutdowns create a shroud of darkness for accountability, can enable war crimes and atrocities,[18] as have been proven to accompany - instead of deterring - escalations of violence.[19]

Just like shutdowns, the spread of harmful information generates mistrust and forces already vulnerable communities into information vacuums with no access to reliable life-saving information, with staggering consequences: incitement to violence and atrocity crimes, mass displacement, collapse of protection mechanisms, inter-community violence, mistrust of humanitarian actors hindering their response or threatening their safety.

There is then the harm generated by the active use of the ICT system as part of the means and methods of warfare, the most immediate and evident example being the concerning frequency of

[14] Access Now, *Stranded, suffocated, and in pain: 15 stories from Tigray's internet siege* (2023), available at: https://www.accessnow.org/15-stories-from-tigrays-internet-siege/

[15] Access Now, *The Sudan conflict: how internet shutdowns deepen a humanitarian crisis* (2024), available at: https://www.accessnow.org/the-sudan-conflict-how-internet-shutdowns-deepen-a-humanitarian-crisis/

[16] Yassmin Abdel-Magied, *Sudanese People Don't Have the Luxury of Hating Elon Musk*, New Lines Magazine (2025), available at: https://newlinesmag.com/spotlight/sudanese-people-dont-have-the-luxury-of-hating-elon-musk/

[17] Access Now, *Joint statement: Myanmar must lift internet restrictions following devastating earthquake* (2025), available at: https://www.accessnow.org/press-release/call-for-lifting-of-internet-restrictions-myanmar/

[18] Access Now, *Evading accountability through internet shutdowns: Trends in Africa and the Middle East* (2023), available at: https://www.accessnow.org/wp-content/uploads/2023/03/Evading-accountability-through-internet-shutdowns.pdf

[19] Hertie School, *Anita Gohdes discusses her new book on Digital Repression on Elliott School's POMEPS Podcast* (2024), available at: https://www.hertie-school.org/en/news/allcontent/detail/content/anita-gohdes-discusses-her-new-book-on-digital-repression-on-elliott-schools-pomeps-podcast

cyber threats of all sorts and nature impending on most humanitarian[20] and human rights actors engaged in life-saving activities.

Cybersecurity experts working for humanitarian organizations are facing increasingly uphill battles trying to protect their share of the humanitarian data ecosystem, as it is reflected in the threats reports generated by their teams and partners. In addition to the onslaught of incidents and hostile events, there is a shared perception across the sector of not being neither equipped to fully protect their sensitive assets, nor to be able to openly flag the extent of their problem.

Some of these threats come from state affiliated actors, while some alerts are provided confidentially by state-affiliated intelligence agencies: in both cases, speaking up about their real threat experience would compromise their perceived neutrality in the humanitarian space and further increase their risk exposure.

The danger posed by the hacking of civilian data goes well beyond the databases, devices and systems controlled by humanitarian actors. Civil society organizations, local community groups and civilians on the individual level are also increasingly threatened by sprawling surveillance practices, sometimes with the unwitting contribution of aid groups trying to assist them. As shown by the discussions during the first states consultation, there is still a lingering feeling that people’s data are not inherently civilian but could hide useful information which might justify monitoring and possibly intrusion into their systems under pretext of ascertaining their status and more accurately inform any military targeting.

We believe that this interpretation of the principle of distinction and precaution to be unfounded in both norms and customs, and to represent a slippery slope towards abusive universal surveillance practices outside of any oversight or recourse mechanism. The burden of running the assessments required under IHL and LOAC should fall on the warring parties, without devolving into a sort of constant duty to prove its innocence by civilians.

The introduction and normalization of mass surveillance practices is also facilitated by the steady push towards the use of invasive practices such as the use of biometric identification and verification tools, officially under the pretext of fighting corruption and diversion of aid or ensuring access to services. In practice, these algorithmic surveillance systems are precursors and enablers of harmful emerging tech processes such as the automation of targeting through data-driven AI systems. By their very nature and function, automated target generation systems used for military purposes are rarely disclosed to the public– let alone audited. These systems are known to make mistakes, which in the case of armed conflict, are irreversible.

How can information spread through ICT activities in armed conflict – in particular through social media platforms – cause, or contribute to physical, lasting psychological, economic and societal harm?

[20] Tilman Rodenhäuser, *Hacking Humanitarians? IHL and the Protection of Humanitarian Organizations against Cyber Operations*, EJIL: Talk! (2020), available at: www. ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyberoperations/

Propaganda has historically been considered part and parcel of a war. The advent of digital communication and the internet has somehow maintained some of the challenges linked to propaganda but also acted as a force multiplier, without the limits that derive from international legal frameworks applicable to the conflict. As a result, disinformation operations have been used as a pretext to allow and justify the targeting of protected civilian objects and groups such as medical facilities and personnel, or humanitarian actors.

For example, in some cases online information operations suggesting that a hospital or medical facility is allegedly used as a military base by a warring party have been exploited by the opposing party to conduct potentially unlawful attacks against such a facility, obfuscate facts, and possibly evade accountability. In some cases, commonly available messaging apps such as WhatsApp and Telegram have been reportedly used to coordinate attacks against civilians[21] as well as humanitarian actors.[22]

Disinformation operations targeting humanitarian actors are also increasingly recurrent outside of the tactical theater of engagement, often with the aim to disrupt their work or undermine their neutrality or impartiality, their support, and acceptance. This has been happening in various ways including through official statements, influence operations using fake accounts, targeted advertisement,[23] causing direct harm to these actors including compromising their financial support or putting their staff at risk.[24]

In some cases, the harm against a community or a collectivity might also be the result of the manipulative use of truthful information. Some warring parties have made use of social media or other communication channels to issue evacuation orders to civilian populations in a way that undermines its main protective function, and actually generates psychological and physical harm.[25] This can for example happen when evacuation instructions are designed to generate stress and confusion in the community, when they are provided without leaving reasonable enough time or adequate instructions to reach safety, or sometimes when purposely generating unfounded expectations of safety about an area that is or might still be a combat area. In quite a few cases, warring parties have used evacuation orders as part of a forced displacement strategy.[26]

Despite the many tragic examples from the recent past, social media is also often used by warring parties to publicly and directly incite to genocide, dehumanize an entire ethnic or religious group/population, call for their collective punishment, or encourage those under their control to commit such crimes. Unfortunately, tech companies have repeatedly proven to lack the

[21] Emmanuel Maiberg, 'Burn Their Homes': Israeli WhatsApp Groups Are Organizing Attacks on Arabs, Vice (2022), available at: https://www.vice.com/en/article/burn-their-homes-israeli-whatsapp-groups-are-organizing-attacks-on-arabs/

[22] Loveday Morris, Far-right Israeli settlers step up attacks on aid trucks bound for Gaza (2025), The Washington Post (2024), available at: https://www.washingtonpost.com/world/2024/05/26/west-bank-aid-trucks-gaza-settlers/

[23] Paresh Dave, *Israel Is Buying Google Ads to Discredit the UN's Top Gaza Aid Agency*, Wired (2024), available at: https://web.archive.org/web/20250417033117/https://www.wired.com/story/israel-unrwa-usa-hamas-google-search-ads/

[24] *UNRWA: Stop Israel's Violent Campaign Against Us* (2024), available at: https://www.unrwa.org/newsroom/official-statements/unrwa-stop-israel%E2%80%99s-violent-campaign-against-us

[25] *Lebanon: Israel's evacuation warnings have been 'misleading and inadequate',* Amnesty International, (2024), available at; https://www.amnesty.org.uk/press-releases/lebanon-israels-evacuation-warnings-have-been-misleading-and-inadequate-new-analysis

[26] *Forced Displacement Orders - Debunking the Myth of Humane Attack* (2024), Oxfam, Actionaid. Available at https://actionaid.org/sites/default/files/publications/Forced%20Displacement%20Orders%20-%20Debunking%20the%20Myth%20of%20Humane%20Attacks.pdf

commitment needed to implement the solutions flagged by civil society groups[27] to prevent, mitigate, and remedy these harms.

Surveillance and information manipulation can also result in harms against civilians, their families, or other protected categories such as prisoners of war, soldiers hors-de-combat, or even humanitarian personnel even in the absence of a kinetic event, through emerging ICT-enabled forms of harassment, ill-treatment, torture,[28] cruel or inhuman treatment, and outrages upon their personal dignity.[29]

The countless ways in which this behaviour has been documented, including by broadcasting and spreading the desecration of religious sites, the invasion of civilian homes, the abusive and degrading public display of intimate or gender-related items, showing detainees or prisoners naked and possibly abused, are aimed at fuelling feelings of indignity, oppression, and inhumanity in the broader communities impacted in some way by the conflict.

Similarly to the past, even people outside of the contested areas can be impacted by the spread of harmful information spreading broad conspiracies and accusations against whole ethnic, religious, national or minority groups in the diaspora. The digital dimension, however, introduces an additional layer of harm due to the sudden possibility of singling out individuals and driving coordinated hostile campaigns against them. Doxxing and smear campaigns targeting individuals for their political views or humanitarian advocacy have resulted in their arrest, losing their employment, being stripped of their residence permits, or being expelled by their university or school, or even attacked on the street.

In conclusion, we stress how all these harmful behaviours do not happen isolated or in a vacuum. The decision by warring parties to manipulate narratives during armed conflict creates confusion[30] for residents seeking safety, a state of extreme distress that is further worsened when parties impose blanket internet shutdowns[31] as a means of information control, forcing them into total information vacuums with no access to reliable life-saving information and making them prey of harmful information campaigns or fraudulent humanitarian service providers. Restricting access to information endangers lives, hinders delivery of humanitarian aid and makes it extremely difficult for the documentation of perpetrators of human rights abuses and even atrocities.

Recommendations

[27] Access Now, *Content governance in times of crisis: how platforms can protect human rights* (2022), available at: https://www.accessnow.org/publication/new-content-governance-in-crises-declaration/

[28] Owen Bowcott, *UN warns of rise of 'cybertorture' to bypass physical ban*, The Guardian (2020), available at: https://www.theguardian.com/law/2020/feb/21/un-rapporteur-warns-of-rise-of-cybertorture-to-bypass-physical-ban

[29] *Article 13 - Humane treatment of prisoners*, Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-13/commentary/2020

[30] Ange Kasongo Adihe et Valdez Onanina, Report from the DRC – The difficulty of accessing reliable information: how disinformation and media censorship have made communities more vulnerable to insecurity, Balobaki (2025), available at: https://balobakicheck.com/en/report-from-the-drc-the-difficulty-of-accessing-reliable-information-how-disinformation-and-media-censorship-have-made-communities-more-vulnerable-to-insecurity/

[31] Access Now, #KeepItOn: authorities must restore access in Goma and across the DRC (2025), available at: https://www.accessnow.org/press-release/keepiton-drc-goma/

For all these reasons, we call on all States and parties involved in the Global Initiative on IHL to:

1. Reaffirm and clarify the status of civilian connectivity and telecommunication systems as protected objects under IHL, essential to the survival of the civilian population and for the full and unimpeded delivery of humanitarian protection and assistance.

2. Act in accordance with International Humanitarian Law (IHL) with regard to ICT infrastructure and systems, including adhering to the principles of humanity, necessity, proportionality and distinction, during times of armed conflict, as well as International Human Rights Law (IHRL), as applicable.

3. Advocate for and uphold a global, free, open, secure, and interoperable Internet and other digital services during times of armed conflict and violence.

4. Promote and protect information integrity online during times of armed conflict and violence, in a manner that supports the right to freedom of expression, which includes the freedom to seek, receive, and impart information online, in accordance with applicable IHL and IHRL.

5. Take active steps to protect civilian infrastructure, which is critical to the provision of essential services and the delivery of humanitarian assistance.

6. Demanding commitment from parties to a conflict to refrain from directing attacks against civilian internet, energy, and telecommunications infrastructure, in accordance with 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, and who are not taking direct part in hostilities.

7. Refrain from imposing restrictive measures and policies that may impede connectivity, degrade bandwidth, or render civilian telecommunications systems non-operational in conflict-affected areas, where prohibited under IHL, including imposing 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.

8. 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.

9. Develop comprehensive guidelines and standards for the ethical and human rights compliant use of AI in military operations, emphasizing the importance of human oversight, accountability, and compliance with international human rights and humanitarian law.

10. Establish an international monitoring mechanism to investigate and report on the use of AI technologies in conflict zones, with a focus on their impact on civilian populations and potential violations of human rights.

11. Establish international cooperation frameworks to address the ethical and human rights implications of AI in warfare, including efforts to ban or strictly regulate lethal autonomous weapon systems (LAWS) and semi-autonomous weapon systems (semi-LAWS).

12. Call on the private sector to conduct thorough enhanced human rights due diligence and impact assessments before providing AI technologies, cloud services, or other digital infrastructure to governments, especially in conflict situations, to ensure these technologies are not used to commit or facilitate human rights abuses.

13. Call on the private sector to develop and implement robust policies, oversight mechanisms, and safeguards to prevent the misuse of consumer products and services (such as facial recognition features in photo apps) for mass surveillance or military targeting purposes.