FOR PUBLICATION

Centre for Humanitarian Dialogue
Mediation for peace

Third State Consultation on upholding IHL in the use of ICTs during armed conflicts

Geneva, 16 February 2026 (10:00 – 14:00 | See agenda / concept note)

Full statement by the Centre for Humanitarian Dialogue (HD)

SESSION 1: Key observations by the workstream co-chairs and the ICRC towards upholding IHL in the use of ICTs during armed conflicts 10:10–12:00

Thank you, Chair.

I speak today on behalf of the Centre for Humanitarian Dialogue, a Swiss-based non-profit organisation guided by the principles of humanity, impartiality, and independence that works to prevent and resolve conflicts through dialogue. In recent years, we have expended our work into the cyber domain, particularly in contexts where there is a high risk of unintended escalation due to cyber operations, whether in situations of armed conflict or heightened interstate tensions.

As many have highlighted, cyber operations can generate significant humanitarian risks, and they also carry serious risks of escalation. These often stem from uncertainty: uncertainty about intent, uncertainty about attribution, and uncertainty about thresholds. Even limited misunderstandings in such contexts can amplify political and military tensions.

We welcome key observations by the workstream co-chairs and the ICRC. We believe that when states clarify their positions on the application of international law, including international humanitarian law, in cyberspace, it can further enhance predictability and stability. Clear positions help set shared expectations, reduce the risk of miscalculation, and support constructive engagement. These are outcomes that even adversary states have a strong interest in promoting.

As states continue this process, we see equal importance in investing in practical measures that reduce risk. In our experience, structured engagement between cyber authorities and mechanisms to clarify incidents can serve as effective steps toward reinforcing stability.

Legal clarity, dialogue, and confidence-building should be understood as mutually reinforcing components of a broader effort to protect civilians and maintain international stability in the digital domain.

We look forward to continuing to support constructive engagement in this area.

Thank you

SESSION 2: Key observations by the workstream co-chairs and the ICRC towards upholding IHL in the use of ICTs during armed conflicts (cont'd) 12:30–13:55

Thank you, Chair.

The Centre for Humanitarian Dialogue, a Swiss-based non-profit organization guided by the principles of humanity, impartiality, and independence, facilitates confidential dialogue to prevent and resolve conflicts. In recent years, we have expanded our work into the information domain, contributing towards building the cooperation mechanisms urgently needed to address information-based warfare.

We welcome the key observations presented and propose two areas for deeper dialogue and legal clarity.

First, greater precision is needed regarding thresholds: when do coordinated information operations amount to incitement of IHL violations or acts whose primary purpose is to spread terror among the civilian population? How should IHL address cumulative harms, such as polarization, dehumanization, or erosion of trust in humanitarian actors as a result of online information operations, where individual posts may not rise to the level of a violation, but in the aggregate may create conditions for future harm? Clarifying these issues is essential to both ensuring accountability and upholding protection "in all circumstances".

Second, further discussion is needed on state responsibility for proxy actors, including "disinformation-for-hire" actors, particularly as similar debates evolve regarding civilian hackers.

From our experience, additional safeguards and dialogue-based approaches could support efforts to better protect civilians and other protected persons and objects from risks in the information domain.

First, states could consider non-binding voluntary confidence-building measures in the information domain, including crisis communication channels to prevent unintentional escalation, akin to existing cyber diplomacy protocols.

Second, greater integration of IHL and the information domain into military doctrine, training, and joint exercises is essential to translate legal obligations into operational practice in accordance with the current evolving capabilities and realities in the information domain.

Finally, expanded engagement between humanitarian actors and technology companies can help to develop meaningful safeguards related to risks in the information space. This may include tabletop exercises to further awareness of risks to both civilians and humanitarian actors and to develop meaningful safeguards, such as rapid response mechanisms to mitigate risks resulting from online content targeting civilians, protected objects, or humanitarian operations. These measures can also help build a meaningful case for the alignment of platform policies with the requirements of IHL.

Information manipulation is now a systemic risk to civilians, humanitarian action, and international stability. In today's multipolar world, diplomatic engagement in the information domain - grounded in prevention, confidence-building, and respect for IHL - is essential to protect civilians and safeguard peace and security.

Thank you.