High-Level Launch Event on the Progress Report for the Global Initiative to Galvanize Political Commitment to IHL

Thursday 16 October 2025, 3:00 to 5:30 pm

Palais des Nations, Geneva

Draft Elements: Presentation of the Progress Achieved in Workstream 6 - Upholding International Humanitarian Law in the Use of Information and Communication Technologies During Armed Conflict

Excellencies, distinguished delegates, colleagues,

It is an honour to present this report today on behalf of the co-chairs Switzerland, Luxembourg, Mexico, and Ghana.

[Importance of the ICT-Workstream and topic]

- The increasing use of information and communication technologies (ICTs) during armed conflicts raises pressing humanitarian and legal questions.
- The ICT workstream was established precisely to address them: to foster a shared understanding on (i) how IHL applies to ICT activities in armed conflict, and (ii) how IHL can help ensure that civilians and civilian infrastructure are safeguarded from harm.
- The workstream builds on years of multilateral discussions and State's positions on the application of international law to ICTs, as well as on Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent just last year.
- It is designed to complement existing processes, without duplicating them, by providing a focused space to explore how IHL can respond to the humanitarian consequences of digitalized warfare.

[Activities & consultations so far]

- Let me briefly address our findings so far and lay out the next steps.
- The first State consultation took place in Geneva on 15 May of this year, in a hybrid format to allow for a global participation, open to all States.

- Over 200 participants, from over 80 states and 14 organizations, were in the room or dialled in, and more than 80 substantive contributions were made, underscoring the high level of engagement and the recognition of the relevance and urgency of the questions at hand.
- The following key findings have emerged, so far.
    - ICT operations in armed conflict may lead to serious humanitarian consequences.
    - States confirmed that IHL remains the relevant framework for protecting civilians and civilian objects from these dangers, while one state cautioned against the automatic applicability of IHL in cyberspace.
    - There was a strong call for greater clarity on how existing IHL rules apply in practice to ICT operations.
    - Let me highlight three specific questions addressed:
        - first, on the notion of "attack": how do we extend the notion of "attack" to ICT operations? Must there be a physical effect? How do we treat an impact that result in non-physical effects, such as the loss of functionality of systems?
        - Second, on distinction: what are the risks when civilian ICT infrastructure is used for military purposes? How do we treat civilians, including private companies, individuals, or hacker groups, when they become involved in ICT operations? In these cases, civilians and civilian services risk being exposed to attacks. We need to explore the legal implications and identify measures grounded in IHL to mitigate these risks.
        - And third, the spread of harmful information through ICT activities. What do we mean by this? For instance, incitement to IHL violations, public exposure of detainees, or threats designed to instil terror in civilian populations. Participants emphasized the need for continued dialogue to refine the limits that IHL imposes on such activities.
    - Throughout, States highlighted and restated their commitment to the baseline: protecting civilians, civilian objects, and infrastructure essential to civilian survival as well as medical services and humanitarian operations.

[Next Steps]

- Looking ahead, the second State consultation will take place on 24 November, once again in a hybrid format. Invitations, a concept note and an updated background paper have been circulated.

- We will build on the discussions so far, work to enhance our common understanding, and aim at identifying concrete legal and practical recommendations to ensure IHL compliance and mitigate civilian harm from digital threats during armed conflict.
- A panel of distinguished experts will help frame the debate as an introduction. The discussions will then focus on key issues such as:
    - The implications of ICT activities that cause non-physical effects;
    - The protection of civilian and other data under IHL;
    - The limits IHL imposes on the spread of harmful information; and
    - The risks and legal implications of military use of civilian ICT infrastructure and civilian involvement in ICT activities, and
    - we will exchange on measures grounded in IHL to mitigate the associated risks of harm for civilians and essential civilian services.
- Further, we intend to reach out to technology companies from different regions to include them in a first round of discussions towards the end of the year.
- Excellencies, colleagues. We count on your continued constructive engagement in this workstream, and we look forward to building together a clearer and stronger understanding on legal and humanitarian issues arising from the use of ICTs during armed conflict and how to address them.

Thank you

Nasty Questions/Situations:

1) Process: This topic should be discussed in the Global Mechanism (follow-up forum of the OEWG) in New York

   ➔ The application of international law, including IHL, to ICT activities has been the subject of multilateral discussions for nearly two decades. This includes the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE), which noted by consensus that "international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognized the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict."

   ➔ The Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021–2025 echoed this conclusion in its progress reports.

   ➔ Building on this momentum, in October 2024 the 34th International Conference of the Red Cross and Red Crescent (34IC) adopted the resolution "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" (ICT Resolution). The resolution also recognized that the specificities of the ICT environment raise questions on how principles and rules of IHL apply to ICT activities and that there is a need for further discussions.

   ➔ This workstream responds to this need and provides a dedicated space for focused and in-depth exchanges. It does so in a complimentary way [and without prejudice] to other fora, such as the OEWG and its successor.

2) Contextual or politicized Statements

   ➔ Recall the rules of the game. The objective of the workstream is to foster shared understandings on the limits that IHL imposes on ICT activities in armed conflict to safeguard civilians from harm in a depoliticised and decontextualized manner.

   ➔ Kindly ask Delegations to respect this format.

3) IHL does not apply

   ➔ Take note

   ➔ Acknowledge that it is important to understand each other's points of view of how IHL protects against dangers of ICT activities during armed conflict.