Humanity In War

Under the Global Initiative to Galvanize Political Commitment to International Humanitarian Law (Global IHL Initiative), **Ghana, Luxembourg, Mexico, Switzerland and the International Committee of the Red Cross (ICRC)** are pleased to present the:

WORKSTREAM 6

THIRD STATE CONSULTATION ON UPHOLDING INTERNATIONAL HUMANITARIAN LAW IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES DURING ARMED CONFLICTS

For government representatives specializing in IHL, cybersecurity or military cyber operations in capitals, as well as representatives from permanent missions in Geneva

MONDAY 16 FEBRUARY 2026

10:00–14:00 (UTC+1)

FORMAT: IN PERSON (GENEVA) AND ONLINE (ZOOM)

Background

The growing use of information and communication technologies (ICTs) during armed conflicts raises significant humanitarian and legal questions. While it is generally accepted that international humanitarian law (IHL) imposes limits on the use of ICTs in armed conflicts, the specific characteristics of the ICT environment give rise to complex questions regarding the implementation of IHL. States have recognized the need to continue discussing these questions.

The ICT workstream of the Global IHL Initiative builds on the global discussions on the use of ICTs and the progress achieved to date, including reports of the United Nations Open-ended Working Group on Security of and in the Use of Information and Communications Technologies and of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of

International Security, national and common positions on cyber and international law, and Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent, entitled "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict". It complements the ongoing multilateral discussions, including the forthcoming Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs. This workstream is part of an ongoing effort to develop a shared understanding of the limits that IHL imposes on ICT activities during armed conflicts, with a view to safeguarding civilians from harm.

The first and second state consultations of the ICT workstream, held on 15 May and 24 November 2025 respectively, recognized the significant human consequences that the use of ICTs during armed conflicts may generate and underscored the imperative to protect people and safeguard human dignity. They reaffirmed that IHL remains the core legal framework for protecting civilians and other protected persons and objects from the dangers arising from the use of ICTs in both international and non-international armed conflicts.

Across both consultations, participants examined the humanitarian and legal implications of the use of ICTs in armed conflicts and explored practical measures to ensure compliance with IHL and strengthen the protection of civilians in this context.

The third consultation will build on these discussions and the key observations emerging from them, with a view to further advancing a shared understanding of how to uphold IHL in the use of ICTs during armed conflicts, with a view to safeguarding civilian populations from harm.

Objectives

This consultation aims to:

- **Consolidate emerging understandings** on how IHL principles and rules protect civilians and other protected persons and objects from the dangers arising from ICT activities in armed conflicts. While states broadly reaffirmed the need to uphold and strengthen such protections, some issues require further discussion in order to foster a shared understanding. The key observations prepared by the co-chairs and the ICRC in line with the objective of the workstream to safeguard civilian populations from harm in the digital age are intended as a basis to guide discussion, invite further inputs, and help assess practical pathways to build a shared understanding of the limits IHL places on the use of ICTs during armed conflicts.
- **Gather national perspectives and practice** on legal, operational and policy measures taken or considered to ensure compliance with IHL in the use of ICTs during armed conflicts, including through legislation, military practice, IHL dissemination, engagement with the technology sector and measures to prevent and suppress IHL violations.
- **Identify areas for further reflection and engagement**, in anticipation of preparing draft recommendations for consideration by states, and ultimately for inclusion in the broader outcome of the Global IHL Initiative.

Next steps

Following the three rounds of consultations, the co-chairing states and the ICRC will formulate concrete recommendations, which will be presented to all states for further discussion:

- On **1 April 2026**, the first versions of the recommendations for all workstreams will be sent to all Permanent Missions in Geneva and published on the Humanity in War website.
- The **fourth round of consultations** will be held between **4 and 6 May 2026**, in a **hybrid format**. During this round, all states will be invited to share comments on the first versions of the recommendations for each workstream, which will be discussed sequentially.
- On **1 June 2026**, the second versions of the recommendations for all workstreams will be sent to all states and published on the Humanity in War website.
- The **fifth round of consultations** will be held between **22 and 26 June 2026**, in a **hybrid format**. All states will be invited to provide final comments on the recommendations. Following this round, the co-chairing States and the ICRC will finalize the recommendations for each workstream, which will be presented to all states in the second part of 2026.

Participants

- The consultation will be held in a hybrid format with participation in person and online.
- The consultation is open to all states that are interested. There is a strong preference for capital-based government representatives specializing in IHL, cybersecurity or military cyber operations, and for representatives from permanent missions in Geneva.
- Other representatives with specific expertise in the subject matter (e.g. members of international organizations, civil society, academia as well as representatives from the technology sector) will also participate upon invitation.
- Please register no later than Friday, 13 February 2026, using the registration link.

Procedure

- The working languages will be **Arabic, Chinese, English, French, Russian and Spanish**, with simultaneous interpretation.
- We ask states to kindly limit their statements to **four minutes** to ensure sufficient time for all participants to take the floor. At the end of each session, and after all participating entities that wish to contribute have done so, states and other participants will be given an opportunity to discuss ideas proposed by others.
- When preparing their statements, participants are kindly invited to take into account the **key observations by the workstream co-chairs and the ICRC towards upholding IHL in the use of ICTs during armed conflicts** and the **guiding questions** provided in the agenda below. The workstream's background paper is also available for reference, to help frame the scope of the discussion.

- Given the technical challenges of hybrid meetings, we encourage delegations who are in the room to make their statements in person and in all cases to give their full attention to delegations speaking online.
- The **inclusive, constructive, non-politicized and solution-oriented** nature of the discussions will be maintained throughout the consultation. While participants are encouraged to refer to their state's domestic practice during the consultations, they are asked to kindly refrain from discussing specific contexts or the practice of other states.
- To facilitate interpretation, we invite participants to share a copy of their statements by Friday, 13 February 2026, via email at ihlinitiative@icrc.org, with "ICT workstream third consultation" in the subject line. We also encourage participants to send their full written statements by email after the meeting. **Unless confidentiality is explicitly requested, these statements will be published on the Humanity in War website.**
- The consultation will be recorded, but the recording will not be made public.

Agenda

Upholding International Humanitarian Law in the Use of Information and Communication Technologies During Armed Conflicts (ICT Workstream) Third Round of Consultations

10:00–14:00, 16 February 2026
ICRC Humanitarium, 17 avenue de la Paix, 1202 Geneva

** Depending on the number of statements given, all times set out below are subject to change.*

Registration and coffee / Login and connection	9:30–10:00
Opening of the meeting and introduction	10:00–10:10
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
Key observations Recognizing the human cost of ICT activities during armed conflict and the damage and disruption they can inflict on societies, and underscoring the imperative of protecting civilian populations and preserving human dignity, it is essential to uphold and reinforce respect for IHL in the use of ICTs during armed conflict. States and parties to armed conflict will take practical measures, individually and collectively, to mitigate risks to civilian populations and to help ensure that ICT activities conducted in the context of armed conflict remain consistent with the protections afforded by IHL. **Protection of civilian populations, civilians and civilian objects against the dangers arising from ICT activities during armed conflicts** In the conduct of ICT activities associated with an armed conflict, compliance is required at all times with IHL, including the principles of humanity, military necessity, distinction, proportionality and precautions. ICT operations expected to cause death or injury to persons, or to result in damage or destruction of objects, including by disabling them, amount to attacks under IHL, and must be conducted in accordance with all IHL rules and principles on the conduct of hostilities, including the prohibitions of direct attacks against civilians and civilian objects, indiscriminate attacks and disproportionate attacks, and the obligation to take all feasible precautions to avoid or at least minimize incidental civilian harm. The principle that a party to an armed conflict may only resort to those means and methods of warfare that are necessary to weaken the military forces of the enemy, the obligation to take constant care to spare the civilian population, civilians and civilian objects in the conduct of military operations, and the rules protecting property from seizure and destruction, offer additional protections against the dangers arising from ICT activities. **Protection of data** Data lie at the heart of the digitalization of the world and is central to the functioning of essential civilian services. The way data is handled during armed conflict may affect people's lives and dignity. Under IHL, data is protected by:	

- the principles and rules governing the conduct of hostilities, including distinction which requires that military operations be directly only against data that qualifies as a military objective and prohibits attacks that affect civilian and military data without distinction, as well as the principles and rules of proportionality and precautions,
- the principle that a party to an armed conflict may only resort to those means and methods of warfare that are necessary to weaken the military forces of the enemy,
- the obligation to take constant care to spare the civilian population, civilians and civilian objects in the conduct of military operations, and
- the rules protecting property from pillage, seizure and destruction.

Information-gathering activities per se are not prohibited under IHL, including when they involve accessing data.

Civilian ICT infrastructure used for military purposes

States and parties to armed conflict need to be aware of and minimize the risk of civilian harm arising from the military use of civilian ICT infrastructure during armed conflicts.

Where such use turns civilian ICT infrastructure, or parts thereof, into military objectives, any attack against such a military objective remains subject to the prohibitions on indiscriminate and disproportionate attacks and the obligation to take all feasible precautions.

In assessing the lawfulness of such operations, all foreseeable direct and indirect incidental effects on civilians and civilian objects, including the civilian uses of the ICT infrastructure, must be taken into account. All feasible precautions need to be taken to spare civilian populations and essential civilian services that rely on ICT infrastructure. All feasible precautions must be taken in the choice of means and methods of warfare with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects. This includes aiming to affect only the components or functions of ICT infrastructure used for military purposes and not those serving civilian purposes.

States and parties to armed conflict must, to the maximum extent feasible, take all necessary precautions to protect the civilian population and civilian objects under their control from the dangers arising from military operations. This includes, wherever feasible, physically or technically separating the components of ICT infrastructure used for military purposes from those serving civilian functions.

Civilian involvement in ICT activities during armed conflicts

Civilians, including hackers and technology company employees, must respect IHL when acting in the context of and associated with an armed conflict.

States must ensure respect for IHL by civilians whose ICT activities during armed conflict are attributable to them, make IHL known to civilians over which they exercise authority, including hackers and technology company employees, and take necessary measures to inform them of the legal and practical risks of conducting ICT activities in the context of an armed conflict. States must exercise due diligence to prevent violations of IHL committed by civilians through or facilitated by ICT activities, and must suppress such violations if they occur. They must not encourage, aid or assist civilians to violate IHL, including through ICT activities.

States and parties to armed conflict should avoid, to the extent feasible, involving civilians in ICT operations amounting to direct participation in hostilities, so as to protect them against the dangers resulting from military operations. Where such participation

nevertheless occurs, those civilians should, to the extent feasible, be integrated into the armed forces. Children must not be allowed to take part in hostilities. **Technology companies' products and services in armed conflicts** Technology companies provide a range of civilian ICT products and services on which civilian populations, governments and humanitarian organizations rely, including during armed conflicts, and such civilian objects, as well as the civilian employees providing these ICT services, are protected under IHL. Technology companies should be mindful that providing ICT products and services to parties to armed conflict carries both legal and practical risks. They should understand, assess and take measures to minimize the risks of harm to civilians and civilian objects, whether as staff in or property of these companies, or due to their physical proximity, digital connection to, or dependence on the relevant infrastructure or services. This includes, to the extent feasible, physically or technically separating their services and products used to support military operations from those used for civilian purposes. Technology companies are expected to take measures to prevent their personnel from engaging in or becoming complicit in violations of IHL, including through the provision of ICT products or services to parties to armed conflict, and to take appropriate measures should any such acts occur. ***Guiding questions for discussion*** 1. Do you have any comments on the above key observations? Are there any issues that require further discussion? 2. Are there other elements or safeguards that should be considered to better ensure the protection of civilians and other protected persons and objects against the dangers arising from ICT activities during armed conflict?	
Break	12:00–12:30
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
Key observations **Protecting medical services, humanitarian activities and other specifically protected persons, objects and activities** Medical personnel, units and transports, as well as humanitarian personnel and objects, must be respected and protected at all times, in accordance with IHL, including against the effects of ICT activities. ICT activities during armed conflicts must not unduly disrupt the functioning of medical services and humanitarian activities, including their data, ICT and communication systems. The confidentiality of medical and humanitarian data must be respected as required by IHL. This protection is critical to preserve trust in the work of medical services and impartial humanitarian organizations. States and parties to armed conflict must also take feasible measures to prevent medical services and humanitarian activities from being harmed, including through ICT activities by third parties such as cyber criminals and other non-state actors not attributable to a party to an armed conflict. In the digital environment, as in the physical world, it is important that the specific protection afforded under IHL to medical services and humanitarian activities be clearly	

identifiable and visible, so that this protection can be respected. One means of signalling this protection is a "digital emblem", currently under development. States and other relevant stakeholders are encouraged to continue engaging with the ICRC to explore legal, technical and diplomatic avenues for its implementation.

The specific protection accorded to objects indispensable to the survival of the civilian population, works and installations containing dangerous forces, cultural property and civil defence must be respected, including when conducting ICT operations during armed conflicts. This includes both their data and the ICT infrastructure indispensable to their functioning.

IHL prohibits sexual violence and the recruitment and use of children in hostilities, including when such acts are committed through, encouraged or facilitated by ICT activities.

Information spread in violation of IHL

States must refrain from, and take all feasible measures to prevent, the use of ICTs to spread information in violation of IHL. This includes spreading information that incites or encourages IHL violations, exposes persons deprived of liberty to insults or public curiosity, or has the primary purpose to spread terror among the civilian population. States and parties to armed conflict should not spread information that dehumanizes the adversary or propagates hatred against civilian populations, including through ICTs.

Medical services and humanitarian activities must be protected from ICT-enabled disinformation aimed at obstructing their work during armed conflicts, as such acts are unduly interfering and incompatible with the obligation to respect and protect medical and humanitarian personnel and their activities.

Measures to ensure compliance with IHL

States must adopt national measures to ensure compliance with IHL in the use of ICTs during armed conflict. This includes disseminating IHL knowledge within armed forces and among the wider population, particularly those who may be involved in ICT activities, and integrating IHL principles and rules and their application to ICT activities into national legislation, military doctrine, operational procedures, rules of engagement and training as appropriate. Dedicated legal advice should be available to military units and commands responsible for ICT activities when necessary. In accordance with states' obligations under international law, in the study, development, acquisition or adoption of ICT capabilities that function as a new weapon, means or method of warfare, determination must be made whether their employment would, in some or all circumstances, be prohibited by international law.

Integrating gender- and age-sensitive approaches into national frameworks contributes to fulfilling IHL obligations, including for addressing ICT-related risks.

To protect civilians and other protected persons from the spread of information in violation of IHL, engagement with relevant actors, including the technology sector, can help ensure compliance with applicable law. This includes encouraging technology companies to adopt safeguards and practices that reduce the risk of online platforms or other ICT services being used to incite, encourage or facilitate violations of IHL, or to otherwise harm civilians and civilian objects.

It is essential for each state to adopt all necessary legislative, regulatory and other measures, including, where appropriate, criminal sanctions, to prevent and suppress IHL violations committed through or facilitated by ICT activities by persons or on territory under its jurisdiction or control.

Transparency, trust-building and shared understandings can be further enhanced through the development and public sharing of national views and positions on how international law, including IHL, applies to the use of ICTs, and through the exchange of lessons learned and good practices to minimize the risk of ICT activities harming civilians. Where possible, efforts will be made to support capacity-building at the bilateral, regional and global levels to strengthen states' capacity to faithfully implement and apply IHL to ICT activities. ***Guiding questions for discussion*** 1. Do you have any comments on the above key observations? Are there any issues that requires further discussion? 2. Are there other elements or safeguards that should be considered to better ensure the protection of civilians and other protected persons and objects against the dangers arising from ICT activities during armed conflict?	
Concluding remarks	13:55–14:00