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

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

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

MONDAY, 24 NOVEMBER 2025
9:00–18:00 (UTC+1)

FORMAT: IN PERSON (ICRC HUMANITARIUM IN 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 conflict, 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, particularly Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent, titled "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict". This workstream is part of an ongoing

effort to develop a shared understanding of the limits that IHL imposes on ICT activities during armed conflict, with a view to safeguarding civilians from harm.

The first consultation on this workstream was held on 15 May 2025. It focused on identifying legal and humanitarian issues and concerns arising from the unique characteristics of ICT activities in armed conflict, and on exploring how they should be addressed – with a view to upholding the protection that IHL affords to civilians and civilian objects, and other protected persons and objects, during armed conflict. This second consultation will advance that discussion. It will be held, in a hybrid format, on 24 November 2025 in Geneva.

For further details on the issues addressed in this workstream, participants are invited to consult the **background paper** attached to this concept note.

Objectives

The second consultation will build on the discussions that took place in the first consultation and on key takeaways from that consultation. It will focus on deepening the discussion of legal and humanitarian issues arising from the use of ICTs during armed conflict. The consultation will aim to advance shared understanding and identify potential legal and practical recommendations to ensure better protection for civilians and civilian objects in digitalized warfare.

The consultation will pursue the following objectives:

- **provide an update on the workstream and its progress**:
    - brief participants on the findings of the first consultation reflected in the progress report and on insights gained from subsequent supporting events
    - outline the next steps towards identifying the workstream's final recommendations.
- **deepen discussion of identified legal and humanitarian issues to advance a shared understanding thereof:**
    - facilitate in-depth exchanges on issues identified during the first consultation for further consideration, such as:
        - implications for IHL of ICT operations that result in non-physical effects, such as the loss of functionality of the targeted system
        - protection, under IHL, for civilian and other data from, for example, being tampered with, damaged or deleted, or extracted and published
        - specific protection under IHL of persons, objects and activities from the effects of ICT activities during armed conflict, including their data and digital infrastructure
        - limits imposed by IHL on information spread through ICT activities
        - implications for IHL of the military use of civilian ICT infrastructure and civilian involvement in ICT activities in the context of an armed conflict, and measures grounded in IHL to mitigate the associated risks of harm for civilians and essential civilian services
        -
    - strengthen practical measures to ensure IHL compliance and mitigate civilian harm.

Next steps

A third state consultation is planned for early 2026 to further advance the discussions of the first and second consultations and shared understandings emerging therefrom. These consultations will lay the groundwork for the workstream's recommendations. Feedback for the workstream's recommendations will be sought from all interested states in the second quarter of 2026, and the recommendations will be further considered in future state consultations.

State consultations will be complemented by regional discussions and other supporting events, which will be announced on the Humanity in War website.

Participants

- The consultation will be held primarily in person in Geneva. Online participation is also possible.
- The consultation is **open to all interested states**. There is a strong preference for capital-based government officials specializing in IHL, cybersecurity, or military cyber operations, as well as representatives from permanent missions in Geneva.
- Other representatives with specific expertise in the subject matter (e.g. members of international organizations, civil society and academia) will also participate upon invitation.
- Kindly register no later than 15 November 2025, using this link: https://forms.office.com/e/LuDKik93vY.

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 requested to consider the **guiding questions** provided in the agenda below. Some guiding questions are accompanied by **illustrative scenarios** that should be read together with the questions. An updated **background paper**, to help frame and facilitate the discussion, is attached to this concept note.
- 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 21 November 2025, via email to ihlinitiative@icrc.org, with "ICT workstream second 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 Conflict (ICT Workstream) Second Round of Consultations

9:00–18:00, 24 November 2025
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	8:30–9:00
Opening of the meeting and introduction	9:00–9:30
Panel discussion: Key legal and humanitarian issues arising from the use of ICTs during armed conflict	9:30-10:30
Session 1: Practical measures to ensure compliance with IHL and protect civilians in the use of ICTs during armed conflict	10:30–11:30
Guiding questions 1. What legal and operational measures has your state adopted, or is considering adopting, to ensure compliance with IHL and prevent or mitigate civilian harm when conducting ICT activities during armed conflict? How do these measures – because of the specific characteristics of ICT operations – differ from those applied to kinetic operations, and how can these characteristics be addressed? 2. What measures does your state take, or has considered taking, to prevent and suppress IHL violations committed through or related to ICT activities? 3. What forms of capacity-building or international cooperation would be most useful for supporting states in strengthening compliance and sharing practical measures in this area?	
Coffee break	11:30–12:00
Session 2: Safeguarding civilians and other protected persons and objects against the dangers arising from ICT activities during armed conflict	12:00–13:00
Guiding questions 1. What are the human costs and the IHL implications of ICT operations that result in non-physical effects, such as disabling the targeted system? Consider an ICT operation, conducted in the context of an armed conflict, against a civilian object, for example the server of a transport provider, an internet service provider or a bank. At the time of the operation, this server is not being used in a manner that would qualify it as a military objective. As a result of the	

operation, the targeted object no longer provides the service it normally does; however, it is not physically damaged. How does your state assess the lawfulness of the ICT operation? Would your assessment change if physical damage took place as a result of the foreseeable direct or indirect effects of the ICT operation? 2. How do you address the protection, under IHL, of civilian and other data against, for example, tampering, damage, deletion, or extraction and publication without authorization? Does your state distinguish between different categories of data (medical, biometric, financial, etc.) when assessing their protection under IHL? Consider an ICT operation, conducted in the context of an armed conflict, to delete civilian data (such as medical data, social-security data, bank accounts, tax records, or client data of civilian companies). How does your state assess the lawfulness of such ICT operations? What IHL rules limit tampering with, damaging or destroying civilian or other protected data in times of armed conflict? What protection does IHL provide against the unauthorized copying, seizing and potential publication of civilian or other protected data? 3. What IHL rules safeguard civilians and civilian objects from ICT operations that do not qualify as an 'attack' under IHL? For example, what practical measures must be taken when carrying out ICT activities to implement the obligation to take constant care to spare the civilian population, civilians and civilian objects in the conduct of military operations?	
Lunch (not provided)	13:00–14:00
Session 3: Operationalizing specific protections for persons, objects and activities against the effects of the use of ICTs during armed conflict	14:00–15:00
Guiding questions 1. What practical measures does your state take, or is considering taking, to ensure that ICT activities during armed conflict do not damage or disrupt the functioning of medical services, humanitarian activities or objects indispensable for the survival of the civilian population, including their ICT systems and data? And what precautions does your state take, or is considering taking, to protect these specifically protected objects against harm, including harm caused through ICT activities? 2. Regarding the specific protection for medical facilities and personnel, consider an ICT operation, in the context of an armed conflict, by a party to gain access to the servers of a medical facility in an adversary's territory. The party concerned collects medical data of members of the armed forces treated there, and then encrypts all patient files, making them unavailable to medical staff. To what extent does the specific protection of medical facilities encompass the confidentiality, integrity, and availability of the data they access, collect, process, and store for their operations? Similarly, how does such protection apply to the data accessed, collected, processed, and stored by humanitarian personnel and objects used for humanitarian operations?	

3. What specific risks arise from ICT activities with respect to the prohibition of sexual violence and/or the unlawful recruitment or use of children in hostilities? What practical measures has your state adopted, or considered adopting, to prevent and respond to such unlawful acts?	
Session 4: Safeguarding civilians, and others protected under IHL, against information spread in violation of IHL during armed conflict	15:00–16:00
Guiding questions 1. What limits does IHL impose on the spread of information through ICT activities during armed conflict? Consider, for example, an information campaign by a party to an armed conflict that entails: • posting online images of prisoners of war and their treatment • fabricating, and disseminating on social-media platforms, messages that inflame tensions between local communities, increasing the risk of violence. What safeguards or oversight mechanisms has your state established, or considered establishing, to prevent ICT activities from exposing persons deprived of their liberty to public curiosity? And how does your state determine whether ICT-enabled information operations constitute prohibited incitement or encouragement of IHL violations, or spreading terror among the civilian population? 2. How does your state address the risk that ICT-enabled spreading of disinformation could obstruct medical services or humanitarian operations during armed conflict? Consider an online campaign circulating fabricated images and fake social-media posts that falsely claim that a hospital is a combatant stronghold. This disinformation provokes distrust in the local population and disrupts access for medical staff; in addition, staff entering the facility become the objects of growing incitement or intimidation. What IHL rules protect medical services and humanitarian operations against digital disinformation? What legal or operational measures has your state adopted, or considered adopting, to address these risks? 3. What other measures has your state taken, or considered taking, to prevent the use of ICTs, including through social media, to spread information in violation of IHL?	
Coffee break	16:00–16:30

Session 5: Addressing the risk of harm arising from the military use of civilian ICT infrastructure, and from the involvement of civilians in ICT activities, during armed conflict	16:30–17:30
Guiding questions 1. What are the human costs and the IHL implications of the military use of civilian ICT infrastructure, and what measures grounded in IHL need to be taken to mitigate the associated risks of harm to civilians and essential civilian services? Consider a commercial data centre, on the territory of a state party to an armed conflict, hosting military data and applications as well as data of civilian populations and applications used in the provision of essential civilian services. • How does your state apply IHL principles and rules such as distinction, proportionality and precautions when assessing an ICT operation against such ICT infrastructure? If a particular part of the ICT infrastructure, such as a cloud server, becomes a military objective, how should the effects on its civilian uses be considered when planning and conducting an ICT operation against it? • What precautionary measures can and should the state conducting the ICT operation take to protect civilian populations and essential civilian services relying on the ICT infrastructure being targeted? • What precautions can and should the state that is home to the data centre take to protect the civilian population and civilian objects under its control from the effects of ICT operations against the data centre? • What precautions can and should the company that owns or operates the data centre take to prevent civilian data from being affected by ICT operations directed against the military data and applications hosted in the same facility? 2. How might civilians be endangered by their involvement in ICT activities during armed conflict, and what measures grounded in IHL need to be taken to mitigate the risks to them? Consider civilian hackers on the territory of one of the belligerents conducting ICT operations, in the context of an armed conflict, that are designed to disrupt military communications or damage the ICT infrastructure of private companies, in order to weaken the enemy state's economy and lower morale among its people. • What legal obligations, under IHL, do civilian hackers have to fulfil when conducting any of these ICT operations? • What measures may the affected state take against these ICT operations? 3. What practical measures has your state taken, or considered taking, to ensure that civilians within its jurisdiction or under its control – such as civilian hackers, hacker groups or tech company employees conducting ICT activities related to an armed conflict – are aware of IHL and comply with it, and are aware of, and protected to the maximum extent possible against, the risks associated with their actions?	
Concluding remarks	17:30–18:00