Second state consultation on compliance with IHL in the use of information and communication technologies (ICT) during armed conflict

Statement by France

24 November 2025

Session 1 – Practical measures to ensure compliance with IHL and protect civilians in the use of ICTs during armed conflict

- *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?*
- *What measures does your state take, or has considered taking, to prevent and suppress IHL violations committed through or related to ICT activities?*
- *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?*

France would like to thank the ICRC and the States co-chairing this group – Luxembourg, Mexico, and Switzerland – for holding this second state consultation. We also wish to thank the ICRC in particular for the significant work done in drafting the progress report, which captures the depth of our discussions.

As we mentioned during the session of May 2025, France considers that international law and international humanitarian law during armed conflict apply fully to cyber space. We also wish to commend once more the work carried out by the ICRC during its 34th International Conference, in October 2024, which recalled that the rules and principles of IHL help protect civilians and persons protected from the risks of ICT activities. Nonetheless, the use of cyber capabilities during armed conflict and the characteristics of the environment necessarily require an interpretation of IHL in order to adapt it to the specificities of cyber space.

As such, France, and in particular the Ministry for the Armed Forces, has fully incorporated cyber capabilities into the operational manoeuvre with the creation in 2017 of the cyber defence command (COMCYBER), which reports directly to the Armed Forces Chief of Staff.

COMCYBER is specifically responsible for designing, planning and carrying out military operations in cyber space. It streamlines these actions with the various operational staffs (joint forces, land, naval, air and special forces) and the intelligence services. The general officer for cyber defence command is permanently supported by a legal adviser trained in IHL in order to ensure that the law is fully incorporated into the planning and conducting of cyber operations.

Cyber operations are carried out by specialized units, whose expertise ensures that technical risks are analysed and in particular that collateral effects are controlled. The action of these specialized units is fully incorporated into the manoeuvre of the armed forces, directly in the terrain or remotely.

Furthermore, the use of cyber capabilities to support the operational manoeuvre requires lengthy planning specific to cyber space, so that all phases of a cyber operation are subjected to the principles of distinction, precaution and proportionality to respond to the obligation to limit collateral effects on protected persons and objects.

Thank you.

Session 2 : Safeguarding civilians and other protected persons and objects against the dangers arising from ICT activities during armed conflict

- *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?*

- *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?*

- *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?*

To begin, we would like to commend the method chosen by the ICRC and the organizing States for this session. Situational exercises and practical case studies are very useful to reflect on the concrete application of IHL to information and communication technologies.

Next, we wish to raise several points.

The first, is the importance of respecting the law of armed conflict, and particularly its cardinal principle of distinction. Applying this principle, cyber attacks must never be directed against information systems used by schools, medical establishments or any other exclusively civilian service. Also forbidden are indiscriminate cyber attacks, meaning those that are not directed against a determined military objective or where the effects cannot be limited.

Secondly, for France, cyber space operations in a context of armed conflict and in relation to that conflict which, without creating physical damage, result in the disabling of systems, can be qualified as attacks under Article 49 of Additional Protocol I to the Geneva Conventions. We consider that a cyber operation constitutes an attack when the targeted facilities or systems no longer provide the service for which they were installed. This applies whether the result is temporary or definitive, reversible or irreversible. If the effects are temporary or reversible, the attack shall be determined as such when an intervention by the adversary is necessary to render the infrastructure or system operational once more. This intervention can take several forms: equipment repair, replacement of parts, network reinstallation, etc.

Thirdly, we believe that data may constitute military objectives, if they fulfil the definition set out in Article 52 of Additional Protocol I. If they do not, they shall be considered as civilian objects, and therefore protected. In addition, the special protection enjoyed by certain objects (such as medical units or goods necessary for the survival of the civilian population) extends in our opinion to the data necessary for the functioning of their computer equipment and information systems.

Lastly, we wish to conclude by reiterating that both the direct and indirect effects of a material or immaterial attack must be assessed in advance in order to avoid or minimize collateral damage to protected objects and persons. However, we consider that only reasonably predictable indirect effects have to be taken into account. As such, the armed forces should not be required to predict, or be held liable for, "cascading" effects of an attack that were not reasonably predictable as they were too far off, notably in time or space.

Session 3 : Operationalizing specific protections for persons, objects and activities against the effects of the use of ICTs during armed conflict

- *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?*

- *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?*

- *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 ?*

It is undeniable that attacks using conventional means and cyber attacks may violate international humanitarian law and therefore have harmful impacts on civilians and medical and humanitarian personnel employed in their service.

As mentioned in previous sessions, France recognizes the full applicability of international humanitarian law to information and communication technologies. As such, operations in cyber space must also take into account the special protection that certain objects (and their information systems) enjoy, such as medical units, cultural property, the natural environment, goods essential to the survival of the population, humanitarian emergency supplies and installations containing dangerous forces.

We are increasingly seeing the use of the notion of critical, or essential infrastructure. This expression does not currently have any basis in positive law. It is therefore not possible to deduce or conclude on any particular protective regime in the law of armed conflict from the use of these terms. In addition, we are convinced that while certain objects enjoy special protection, such as those mentioned previously, this is not the case for all infrastructure deemed "critical" or "essential". It is important to us in that regard to maintain the distinction between what might be everyday language and what is part of an identified legal category.

Thank you.

Session 4 : Safeguarding civilians and other protected persons under IHL, against information spread in violation of IHL during armed conflict

- *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?*
- *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?*
- *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?*

France wishes first and foremost to reiterate its full support to the humanitarian organizations whose work is impeded by the dissemination of false information on the Internet and on social media. The questioning of their neutrality and the spreading of false information designed to weaken the protection that they lawfully enjoy affect humanitarian personnel and their work on the ground. We remain convinced that States must refrain from conducting information attacks against humanitarian organizations.

Secondly, while influence operations conducted via social media may tangibly fulfil military needs, particularly by sharing messages, said messages must not, either in form or in substance, lead to a violation of the rules of IHL.

As such, it is expressly forbidden to encourage the commission of crimes (including violations of IHL) such as threats of reprisals or that no quarter will be given. Simultaneously, draft messages aimed at influencing the civilian population must be carefully verified, in order to avoid messages designed to spread terror among the population, for example messages encouraging the population to leave an area or else face mistreatment.

France attaches particular importance to raising awareness about these issues within the armed forces. As an example, information sessions with legal experts from the ministry have been held, focusing on the issue of exposing prisoners of war to public curiosity in the era of ICTs and social media.

Lastly, should, however, the consequences of such operations lead directly or indirectly to the neutralization of a target, the process specific to kinetic targeting must be applied.

Thank you.

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

- 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?*
- *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?
- 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?

First of all, thank you for these questions which encourage us to reflect on identifying the nature of a target. It is true that, particularly in the cyber space field, an object that could legally be a lawful military objective, may provide a service to civilians or be used by civilians. This means assessing, with the highest standards and strictness, the effects of its destruction or neutralization on civilians, especially considering the intrinsic specificities of cyber space. These effects must not be disproportionate in relation to the concrete and direct military advantage anticipated.

It would be useful, then, to recall that it is not because an object fulfils the two cumulative conditions of Article 52 of Additional Protocol I, and may be considered a military objective as regards distinction, that it would be lawful to attack it in application of the principles of precaution and proportionality.

Secondly, as we mentioned in the previous session, while no provision expressly forbids States from inviting or inciting the adult civilian population to take part directly in hostilities, this practice can create a climate conducive to creating confusion between civilians and combatants, and thereby weaken the protection that civilians are entitled to. Furthermore, in application of Article 72.2 of Additional Protocol I, the States Parties must take every measure so that children under 15 do not participate directly in hostilities.

We believe it is fundamental that the population fully understand the effects of such participation. As such, training in IHL, in peacetime, and for a broad audience (both military and civilian) is essential. Training in IHL is a priority for the French authorities, with the adoption of a new humanitarian strategy for the French Republic for the years 2023-2027, which aims to promote and strengthen compliance with IHL.

Thank you.