The Global Initiative to Galvanize Political Commitment to International Humanitarian Law

WORKSTREAM 6: ICT

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

24 November 2025

Statements by Finland

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

We thank the ICRC and the co-chairs for these very useful consultations. I wish to reiterate Finland's commitment to upholding IHL, and its faithful interpretation, at a time when both far too permissive interpretations of IHL, and blunt indifference to its requirements, are prevalent in armed conflicts. Finland joined the global IHL initiative early this year and consider the initiative to provide an important forum to discuss and promote respect for IHL. While it is clear that IHL applies to ICT operations conducted in the context of an armed conflict, there have been calls for greater clarity on *how* IHL applies in practice.

We wish to once again emphasize that IHL fully applies in cyber space. IHL applies to cyber operations when such operations *are part of or amount to* an armed conflict, whether international or non-international in character. Cyber means and methods of warfare must be used consistently with IHL, including the principles of distinction, proportionality and precautions, as well as the specific rules flowing from these principles.

Already in our national position, issued in 2020, Finland stated that when assessing the capacity of cyber means and methods to cause prohibited harm, their **foreseeable direct and indirect effects** shall be considered. It was underlined that constant care shall be taken to ensure the protection of civilians and civilian objects, including essential civilian infrastructure, civilian services and **civilian data**. In other words, civilian data shall be protected as a civilian object in accordance with IHL. This statement has not been further elaborated, which means that it applies to all civilian data, understood as a civilian object. We agree with the statement in the background paper that no distinction should be made between civilian data stored in digital files and that in paper documents. Both are entitled to protection under IHL.

The IHL rules prohibiting attacks against objects indispensable to the survival of the civilian population are also relevant here. In addition, it must be remembered that the duty to take continuous care to spare civilians and civilian objects from the harms of warfare also covers cyber operations that do not constitute an attack under IHL.

The special protections under IHL, for instance, for medical personnel, units and transports and humanitarian personnel and objects shall be respected also in cyberspace and that includes their data.

As highlighted in the background paper, ICT operations that severely disrupt civilian infrastructure and interrupt the delivery of essential services, constitute one of the most important ICT risks for

civilians during armed conflict. The question of whether loss of functionality can **constitute an attack under IHL** was discussed already during the first round of consultations. In the modern world, essential services largely depend on ICT and the **loss of functionality** in the targeted systems can cause serious consequences. In this context, the loss of functionality that requires physical action such as reinstallation of software, may be considered an attack under IHL. The purpose of IHL is to limit the effects of armed conflict and to protect those not taking part in hostilities and to restrict the means and methods of warfare. When applying the existing rules in cyber context, our focus should be on protecting civilians and civilian objects, including civilian infrastructure, from the real risks that the use of ICT means and methods of warfare may cause. In the Declaration on a common understanding of the application of international law to cyberspace, the EU and its Member States made clear that international law, including IHL, is fit for purpose in the digital age. It was also stated that cyber activities may amount to attacks within the meaning of IHL whether in offence or defense.

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

States have an obligation to disseminate IHL among the civilian population. This obligation is even more important in the digital age. Advising civilian hackers of the risks they may encounter, as well as condemning IHL violations, when they occur, increases general awareness of the rules and principles of IHL and of the prohibition of encouraging or inciting IHL violations.

There are considerable risks of civilian involvement in cyber operations, including the risk that such action may not be consistent with IHL, risks to the security of civilians and those close to them if they are seen to directly participate in hostilities, and the general risk that such action may blur the distinction between civilians and combatants.

In the Declaration on a common understanding of the application of international law to cyberspace, the EU and its Member States underlined the applicability of the definition of military objective under IHL, according to which military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. The declaration noted that in the cyber context specific consideration may be required, since ICT infrastructure is often used for both civilian and military purposes. It is, however, clear that whenever an ICT system, network or infrastructure does not constitute a military objective, it enjoys the protection as a civilian object.

ICT infrastructure is often used for both civilian and military purpose, but as was highlighted on the first round of the consultations, this applies to also other types of infrastructure. And not all military use of a civilian object turns it into a military objective under IHL. It must also be reiterated that the principle of distinction applies irrespective of whether a cyber-attack is conducted in an offensive or a defensive context. In addition, the principle of proportionality and the special protection enjoyed by certain objects gain importance when cyber means are used in armed conflict.

In our national position, Finland has also emphasized that while IHL is *lex specialis* in an armed conflict, it does not override other areas of international law, such as human rights law.