The Global Initiative to Galvanize Political Commitment to International Humanitarian Law

WORKSTREAM 6: ICT

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

15 May 2025

Statements by Finland

Session 1: The use of ICTs in today's armed conflict and the human cost

Cyber capabilities have changed the way in which armed conflicts are conducted and there is reason to expect that cyber means and methods will continue to be used also in the future. It is therefore important to recall that IHL applies to cyber operations conducted in the context of an armed conflict, whether international or non-international in character.

Last November, in its Declaration on a common understanding of the application of international law to cyberspace, the EU and its Member States reaffirmed that international law, in particular the UN Charter, international human rights law and IHL, fully applies to cyberspace. This Common understanding complements Finland's national position issued in 2020.

IHL applies to cyber operations when such operations are part of, or amount to, an armed conflict. Most so far known harmful cyber operations have not been launched in the context of an armed conflict or have as such triggered an armed conflict. At the same time, when cyber means are used in the context of a pre-existing armed conflict, as has been the case in many current conflicts, there is no reason to deny the need for the protections that IHL provides.

Cyber operations can disrupt the operation of critical civilian infrastructure and hamper the delivery of essential services to the population. There is particular concern about the potential human cost of cyber operations on critical civilian infrastructure, such as health infrastructure.

In the world of today, essential services largely depend on ICT. Cyberattacks and operations targeting critical infrastructure can have severe impacts on the civilian population, and can take an immense toll on human security, causing harm to affected individuals and communities.

In recent conflicts, cyberoperations have been used, for example, to destroy and exfiltrate data, disrupt critical infrastructure and services, and to control the information space. Mis- and disinformation has been used to influence the information space and limit access to timely and reliable information. Such communication shutdowns also severely impact the delivery of humanitarian assistance, including life-saving assistance.

Information operations are not new methods of warfare but are now being used and spreading harmful information at an unprecedented speed and scale.

States and parties to armed conflicts must allow and facilitate impartial humanitarian activities during armed conflict, and protect humanitarian personnel and objects from undue interference, including by ICT activities.

Policy frameworks, such as the framework for humanitarian digitalization by DG ECHO from 2023, are also valuable. In this framework, two fundamental areas were identified, in which work is required to build an enabling environment for humanitarian digitalization: building trust in digital tools and helping invest in and scale innovation. This will, in turn, require a risk-aware, cybersecure and resilient digital integration from the outset, and thereby effectively implementing, inter alia, the established principle and practice of security-by-design.

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

As already emphasized in our previous statement, IHL fully applies to cyber space. Cyber means and methods of warfare must be used consistently with the principles of distinction, proportionality and precautions, as well as the specific rules flowing from these principles. When assessing the capacity of cyber means and methods to cause prohibited harm, their foreseeable direct and indirect effects shall be considered. Constant care shall be taken to ensure the protection of civilians and civilian objects, including essential civilian infrastructure, civilian services and civilian data.

Violation of these principles, or the specific rules flowing from them may amount to a war crime also when committed by using cyber means. The Office of the Prosecutor of the International Criminal Court has also stated that conduct in cyberspace may in appropriate circumstances amount to war crimes or other crimes under the jurisdiction of the Court.

I also wish to refer to the landmark resolution on ICT, already mentioned by many, approved at the 34th International Conference of the Red Cross and Red Crescent. This resolution contained important language regarding ICT activities in armed conflict, for example, on the protection of civilians, medical personnel, medical units and transports, humanitarian personnel and humanitarian objects as well as on allowing and facilitating humanitarian access.

Let me also highlight in this context that the human cost of the use of ICTs in armed conflict is not limited to that caused by **malicious** activities. Nor do the relevant IHL rules only regulate malicious activities, as violations of IHL may be due to carelessness or insufficient precautions, or a mistake. Our primary focus should be on protecting civilians and civilian infrastructure from the real risks that the use of ICT means and methods of warfare may cause.

The same applies to the protection of humanitarian organizations and humanitarian personnel from ICT activities that might have a negative impact, not only from malicious ones. There are very real and concrete concerns related to the effect of ICT activities on humanitarian action. Humanitarian operations and medical and humanitarian organizations and personnel benefit from several protections under IHL and these should be respected also in cyberspace.

Interference by cyber operations, including information operations, with the work of humanitarian organizations is never acceptable. Mis- and disinformation and hate speech represent a significant challenge for humanitarian space and principled humanitarian action. The issue of data protection and management still requires further attention, particularly regarding data collected on beneficiaries, to ensure accountability to beneficiaries and the do-no-harm principle. This is particularly important when seeking new innovative solutions.

Session 3: Protecting civilians and other protected persons from information spread in violation of IHL during armed conflict

States have an obligation to disseminate IHL among the civilian population. While not ICT specific, this obligation is extremely important in the digital age as knowledge of IHL is a condition of its respect. With more footage shared through social media, including on prisoners of war, it is important to inform the public of the protections provided by IHL for persons deprived of liberty against public curiosity. Clearly stating and condemning IHL violations, when they occur, is important for various reasons, but also to increase awareness of the public on the rules and principles of IHL and the prohibition of encouraging or inciting IHL violations.

Another important factor in advancing general awareness is media literacy. In Finland, media education is present throughout the Finnish education curriculum. "AI literacy" is also quickly becoming a more and more vital skill. The ability to both harness the capabilities of this new technology and critically analyze its outcomes has become increasingly crucial.

We appreciate the innovative ways the ICRC is working to promote awareness, including by seeking to have IHL included in video games.

Session 4: The risk of harm arising from the military use of civilian ICT infrastructure and the involvement of civilians in ICT activities during armed conflict

Regarding the principle of distinction, in the cyber context specific consideration may be required, since ICT infrastructure is often used for both civilian and military purposes. If an ICT system, network or infrastructure does not constitute a military objective it enjoys the protection as a civilian object. The principle of distinction applies irrespective of whether the cyber-attack is exercised in an offensive or a defensive context. Civilians must be protected against attacks, unless they take a direct part in the hostilities including by cyber means, as must be civilian objects.

The issue of civilian hackers, i.e. civilians conducting cyber or information operations in situations of armed conflict, is a timely one. There are considerable risks to such action, including the risk that their action may not be consistent with IHL, risks to the security of the hackers 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.

Early this year, the Ministry for Foreign Affairs published in Finland an information package for those considering volunteering as foreign fighters and for their relatives. The intent was not to recommend or to promote volunteering, but to inform about relevant national and international law, including IHL obligations and ensuing criminal liability for possible breaches of IHL. Similar guidance could be helpful also for civilian hackers.