15.05.2025

Session 1: Protecting civilians and other protected persons and objects from the dangers arising from ICT activities during armed conflict

First of all, also in this workstream, Germany would like to commend the ICRC, BRA, CHN, FRA, JRD, KAZ and ZAF for launching the Global Initiative to Galvanize Political Commitment to International Humanitarian Law and thank LUX, MEX and CHE. We express our sincere appreciation to the ICRC, not only for hosting todays ICT Workstream, but also for its ongoing effort to protect civilians and other protected persons in armed conflict, including through its important work on cyber related challenges.

Turning to the substance of today's discussion, I would like to reiterate that Germany reaffirms that international humanitarian law applies in its entirety to cyber operations conducted in the context of an armed conflict.

The specific characteristics of cyber operations must under no circumstances diminish the protection afforded by IHL to civilians, civilian objects, and specifically protected persons and entities.

Accordingly, IHL prohibits attacks against civilians and civilian infrastructure, whether carried out by kinetic or cyber means.

Germany has consistently emphasized the applicability of IHL to cyber operations in armed conflict, including in the UN Open-ended Working Group.

As a member of the Cross-Regional Group on IHL in Cyberspace, we co-supported a discussion paper on this topic for the February session 2024. Furthermore, in partnership with the ICRC we have launched the Cyber in Conflict event series to promote a continued dialogue on this question.

15.05.2025

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

Regarding the first guiding question. Let me start by referring to our national position on the application of international law in cyberspace, which Germany published in 2021.

In this paper, a cyber attack in the sense of IHL is defined as an act or action initiated in or through cyberspace to cause harmful effects on

1. communication, information or other electronic systems

2. on the information that is stored, processed or transmitted on these systems or

3. on physical objects or persons.

For us, the occurrence of physical damage, injury or death to persons or damage or destruction to objects comparable to effects of conventional weapons is not required for an attack in the sense of Art 49 of the First Additional Protocol to the Geneva Conventions.

However, we do not consider the mere intrusion into foreign networks and the copying of data as an attack under IHL.

Based on this understanding, a cyber operation that disables civilian objects without causing physical damage could, according to Germany, still qualify as an attack in the meaning of IHL.

This brings me to the lively discussed question whether data can qualify as an object in the sense of IHL.

If civilian data is understood as an object, then operations aimed at deleting or damaging such data would fall under the core IHL principles, including the principle of distinction which prohibits attacks against civilian objects.

Consequently, attacks directed against civilian data would be prohibited. In its national position on the application of international law, Germany addressed this issue indirectly:

By defining an attack as an act or action initiated in or through cyberspace to cause harmful effects on the information stored, processed or transmitted on electronic systems, we have implicitly recognised that information stored on electronic systems, meaning data, must be protected in the same way as civilian objects.

In this regard, we share the ICRC's view that the digitalization of essential functions, such as public health services or other data related to critical infrastructures, must not diminish the protection that International Humanitarian Law affords to the information stored in the data.

Finally, we strongly support the ICRC's view that the special protection granted under IHL to medical services and humanitarian activities must also be upheld in the cyber domain.

We therefore welcome the ICRC's initiative to explore the use of a digital emblem and look forward to engage in further discussions on its legal, technical and practical feasibility.

Thank you.

15.05.2025

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

Germany would like to make three brief comments on the issues raised in this session.

First. On military use of civilian digital infrastructure: In our 2021 position paper on the application of international law in cyberspace, as well as in numerous subsequent statements, Germany has emphasized that the principle of distinction must fully apply to cyber operations during armed conflict. This is especially true in light of the increasing “dual-use” nature of civilian digital infrastructure, also for military purposes.

To quote our position paper: A civilian object like a computer, computer networks, and cyber infrastructure, or even data stocks, can become a military target, if used either for both civilian and military purposes or exclusively for the latter. However, in cases of doubt, the determination that a civilian computer is in fact used to make an effective contribution to military action may only be made after a careful assessment. Referring to Article 52 paragraph 3 of the First Additional protocol our position paper states, that should substantive doubts remain as to the military use of the object under consideration, it shall be presumed not to be so used.

Furthermore, we emphasize that in our understanding the loss of protection of civilian object, digital or otherwise, does not affect the continued applicability of the principles of proportionality and precaution. This is true whether the operation is conducted by cyber or kinetic means

Second, on the involvement of civilians in cyber activities during armed conflicts. Germany is concerned about the increasing role of civilian hackers in armed conflicts and the risk this poses to the effective application of the principle of distinction. For this reason, Germany has explicitly raised this issue in the context of our Cyber in Conflict Dialogue series, which we organize together with the ICRC.

Third and finally, Germany strongly reaffirms that States have an obligation to respect and to ensure respect for IHL. When civilians engage in cyber activities, the rules of State responsibility apply.

Thank you.