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

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?

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

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?*

Germany thanks GHA, LUX, MEX, CHE and the ICRC for hosting this second consultation. It is global consensus that international law and thereby international

humanitarian law, fully applies to State conduct in cyber space and especially to cyber operations in the context of an armed conflict.

On the first guiding question, where a cyber operation in the context of an armed conflict is directed against a civilian object and results in the targeted object no longer providing its normal service, without being physically damaged.

Germany may consider such an operation an attack within the meaning of Article 49 paragraph 1 Additional Protocol I.

Germany interprets “violence” in Article 49 (1) to cover not only violent means but also violent effects. Accordingly, a cyber operation qualifies as an attack, when it is reasonably expected to cause harmful effects on communication, information or other electronic systems, on the information that is stored, processed or transmitted on these systems or on physical objects or persons. This includes the loss of functionality of the targeted object meaning the situation where a system is rendered incapable of performing its intended function, even if no physical destruction occurs. This is because, functionally disabling the server of a transport provider, an internet service provider or a bank, is clearly damaging to the targeted object, potentially requires repair and impacts its civilian users. Therefore, such effects must be considered equally to other forms of violence to safeguard civilians and civilian objects in line with IHL’s object and purpose.

Accordingly, where a civilian object is targeted in such a way, this would violate the principle of distinction and the related prohibition of attacking civilian objects which are both norms of customary international law in IACs and NIACs.

On the second question: Germany is of the view that data qualify as objects under Article 52 Additional Protocol I and respective customary international law. Consequently, cyber operations expected to damage or destroy civilian data must be treated as a prohibited attack on civilian objects, unless the data meets the criteria of a military objective under Article 52 (2) Additional Protocol I. Today, digital data often serves the same function as their physical predecessors e.g. in the case of medical records, tax files, electoral rolls or banking data. Also, with the growing use of AI in our societies, which rely on data, the importance of data for civil societies will grow even further. Deleting or corrupting such data can disrupt essential services and cause humanitarian harm that may even exceed that of attacks on purely physical objects. To deny protection in this case would create a significant gap in the protection of civilian populations, contrary to the object and purpose of Part IV of the Additional Protocol I. Germany does not draw distinction between categories of civilian data in this regard

On the third question: Germany recalls that under Article 57 (1) of Additional Protocol I according to which constant care shall be taken to spare the civilian population, civilians and civilian objects in the conduct of military operations. This customary obligation of conduct applies to all weapons, means and methods of warfare, including to cyber operations not amounting to attacks in both international and non-international armed conflict. Parties to a conflict must take all feasible measures to avoid or at least

minimize incidental harm to civilians and civilian objects, for example by segmenting military from civilian cyber infrastructure wherever feasible.

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

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?

Germany recalls that medical units, humanitarian relief operations and objects indispensable to the survival of the civilian population enjoy specific protection under treaty and customary international humanitarian law. This protection extends to any protective activities of these actors in cyberspace. In Germany's view, data qualifies as objects, in the sense of international humanitarian law. Consequently, harming protected data related to such specifically protected actors and actions is prohibited by the very same legal rules.

Germany is also open to continued work with the ICRC and other States on digital emblem solutions to help with technical identification of protected medical units and humanitarian relief operations. We duly note the encouragement given to this exploration in the first cyber related Resolution at the 34th International Conference of the Red Cross and Red Crescent from 2024.

In the scenario given in guiding question 2, where a party to the conflict gains access to the server of a medical facility in an adversary's territory and then encrypts all patient files making them unavailable to medical staff. Germany would assess that such behavior which renders a system incapable of performing its intended function, as it is the case, when medical data is unavailable for the medical unit, would constitute an attack in the sense of international humanitarian law. Targeting a medical unit with such an attack would therefore be prohibited by international humanitarian law. The

same logic applies when data of humanitarian relief personnel and material involved in a humanitarian assistance is being targeted. As a further remark, Germany would like to add that international humanitarian law does not only prohibit attacks against medical units and humanitarian relief operations, but any other cyber operation to the detriment of such actors.

Germany is deeply concerned about violations including by cyber means of international humanitarian law with respect to the prohibition of sexual violence and the unlawful recruitment or use of children in hostilities.

We continue to engage in discussions such as this one to exchange on effective measures to prevent such activities from happening.

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

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?

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

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?

At the outset, Germany would like to outline, that both the military use of civilian cyber infrastructure and the involvement of civilians in cyber activities during armed conflict

pose serious challenges to the principle of distinction and increase risks for the involved civilians and civilian objects.

Regarding the first guiding question on the military use of civilian cyber infrastructure: Under international humanitarian law, civilian cyber infrastructure is a civilian object and enjoys protection unless and for such time as it meets the criteria of a military objective in the sense of Article 52 para. 2 Additional Protocol I, which reflects customary international law in both international and non-international armed conflicts.

In situations such as in the example where a data centre is used for both, civilian and military purposes, Germany considers that any determination that a specific object within that infrastructure has become a military objective must be made with great caution and on a case-by-case basis. Germany recalls, that according to Article 52 (3) Additional Protocol I, "*in case of doubt whether an object which is normally dedicated to civilian purposes […], is being used to make an effective contribution to military action, it shall be presumed not to be so used*".

When planning and conducting a cyber operation against such an object, the principles of proportionality and precautions must be observed and the expected effects on civilian objects must be factored into the proportionality assessment of an attack.

With respect to the principle of precautions by the party conducting a cyber operation, Germany emphasizes that Parties who plan or decide upon an attack must among others

- Do everything feasible to verify the nature, use and dependencies of the targeted infrastructure, e.g. by mapping networks and understanding its function for the civilian population and civilian objects.
- Adapt means and methods of cyber warfare to minimise civilian harm, for example by using tailored tools with features such as "system- or geo-fencing" or automatic deactivation mechanisms and strict control of propagation and by avoiding inherently indiscriminate tools such as self-replicating malware.
- Reassess, adapt or cancel operations, where the expected incidental loss of civilian life, injury of civilians, damage to civilian objects or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

The State that is home to the data centre must according to Article 58 of Additional Protocol I in an international armed conflict, to the maximum extent feasible, take the necessary precautions to protect the civilian population and civilian objects under their control against the dangers from military operations, including cyber operations. This includes

- Isolating military from civilian networks and avoiding, as far as possible, the conduct of military operations through civilian infrastructure.
- Enhancing the cyber resilience of civilian systems to the highest possible standard e.g through up-to-date security measures, timely security patches and backups.
- The ongoing work on a possible “digital emblem” led by the ICRC could also play a role here.

While international humanitarian law binds States and Parties to a conflict, private companies operating data centres play an important role. They can support compliance with those feasible precautionary measures by implementing robust isolation of civilian and military data and strong encryption and backup measures, which all help in limiting civilian harm.