Excellencies, colleagues,

At the outset we would like to express our gratitude to the ICRC as well as to the co-chairs of this workstream (Luxemburg, Mexico and Switzerland) for organising this discussion.

The impact of the use of ICTs on the modern battlefield and the related human cost is indeed a matter of growing urgency. All over the world, we have observed the increasing use of ICTs in both international and non-international armed conflicts. Worryingly, the effects of cyberattacks can sometimes spill over to countries that are not involved in an armed conflict. Poland has experienced such negative consequences from a malicious cyber operation carried out in the context of an armed conflict in a neighbouring country.

The international community seems to have taken notice of the issue at hand. On 31 October 2024 the International Conference of the Red Cross and Red Crescent adopted, by consensus, the first humanitarian ICT resolution. The resolution was an unprecedented achievement, addressing a number of crucial issues regarding the application of ICT in the context of IHL. Unfortunately, we have yet to see a similar progress on the subject in other fora.

Now I will turn to the first two guiding questions proposed in the background document.

With regards to ICT activities during armed conflict that pose a threat or risk of harm to civilians and civilian objects, let me start with stressing that the use of cyberspace as a new domain of warfare has serious implications for civilians.

Malicious ICT activities may undermine the functioning of critical infrastructure on which civilian populations are increasingly dependent. Cyberattacks on electrical grids, water purification systems, or hospitals can have direct consequences for civilians and may violate core principles of distinction and proportionality. Targeting communication systems may limit access to basic services and humanitarian aid.

Moreover, continuous and widespread cyberattacks may lead to the breakdown of social order in the targeted area which may expose civilians to further violence and deprivation, not directly caused by cyberattacks.

It must be noted that the dual-use nature of many digital infrastructure blurs the lines of lawful targeting under IHL and poses a challenge for application of this branch of international law in the cyber domain.

Now moving to the detrimental impact of information spread through ICT activities in armed conflict. We would like to begin with noticing that social media platforms, in times of armed conflict, can be a fertile ground for disinformation, hate speech, incitement to violence, and propaganda.

Spreading false information – for example, regarding evacuation orders or planned attacks can lead to panic and displacement. It can be a means of wearing down the targeted population physically and psychologically. Fear-mongering and hate speech may lead to violence against vulnerable groups.

Recording and sharing images and videos of mistreatment of civilian or prisoners of war can be a cause of recurring trauma, especially when the content is humiliating for the victims.

Disinformation during armed conflict may be a means of warfare in itself, undermining the trust in political or military leadership, spreading defeatism, or eroding trust in institutions. It may also prolong conflicts by derailing ceasefire attempts, feeding resentment and building mistrust between conflicting parties. Moreover, it can delegitimize humanitarian actors, disrupt aid delivery, and fracture the social fabric needed for post-conflict recovery.

To conclude undoubtedly IHL applies fully to ICT activities during armed conflict. Yet, it is important to remember that ICTs are only tools – they do not lead to violations of IHL by themselves. Whether ICTs are used to uphold or undermine IHL is, at the end of the day, a question of political will of parties to the armed conflict. Unfortunately, in recent years we have witnessed a waning attachment to the principles of IHL, both online and offline, in too many places.

At the same time, we should not overlook the role of private sector. Technology companies should step up their efforts in content moderation and use algorithms that, instead of amplifying hate speech and disinformation, promote peaceful efforts. This is particularly relevant during armed conflicts.

Lastly, it is important that the discussions on the nexus between use of ICTs and IHL involve a variety of stakeholders, including international organizations, civil society, technical community and academia. On this note, we would like to commend the organizers for ensuring a rich and diverse representation here today.

I thank you.