Remarks by the delegation of Ukraine
during the second state consultation on upholding IHL in
the use of ICT during armed conflicts (Workstream 6)
under the Global Initiative to Galvanize Political Commitment
to International Humanitarian Law
(24 November 2025, Geneva)

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

In exercising its right to self-defense against the foreign aggression, Ukraine relies on a full arsenal of available means and methods to protect its nationals, sovereignty, independence, and territorial integrity.

This arsenal includes activities in information-communication networks. In doing so, Ukraine remains committed to the rule of law, including international humanitarian law. It is also our strong conviction that IHL must be observed even when confronting an adversary who blatantly disdains the very idea of law and humanity.

At present, there exist no norms of IHL that would directly regulate the use of ICTs for military purposes as a means of warfare or the attacks against the ICTs of the adversary. Nevertheless, Ukraine believes that the general principles of IHL apply as provided by Article 1 of Additional Protocol 1, which states that in cases not covered by international agreements, civilians and combatants remain under the protection and authority of the principles of international law, principles of humanity, and dictates of public conscience. These are well-known principles of humanity, distinction, and proportionality. Ukraine is deeply committed to these principles in conducting all its operations, including operations in ICTs and against the ICTs of the adversary.

In the ongoing international armed conflict, to which my country is a party, military actions in ICTs take the form of cyber operations. Ukraine fully understands the destructive power of cyber operations conducted by the adversary, as well as the potential of cyber operations in countering armed aggression.

Therefore, the Command of Communications and Cyber Security has been created as part of the Armed Forces of Ukraine. This enabled centralization of cyber operations and ensured rigorous legal control over such operations. Such a control is exercised by a group of legal advisors, who are a part of the Command and who have specific expertise in the legal aspects of cyber operations. No cyber operation can be initiated without prior legal expertise. The group also serves as a center of excellence, which accumulates best practices and solutions resulting from practical experience.

The Command of Communications and Cyber Security is not the only body running cyber operations on behalf of Ukraine. State bodies, which are not a part of the Armed Forces, for example, the State Security Service of Ukraine, have their own cyber units. To ensure proper coordination, Ukraine has created the National Coordination Cyber Security Center. It operates within the Council of the National Security and Defence, which is the Ukraine's top decision-making body on issues of national security and defence. The National Coordination Cyber Security Center pays due attention to ensuring IHL education and training for officers engaged in cyber operations.

Ukraine continues to explore the avenues for legal regulation of cyber operations by means of IHL. The Ministry of Defence plays a key role in these efforts. The Ministry is in the process of developing a Green Paper on the legal regulation of cyber operations, which reflects the experience obtained during the international armed conflict, as well as the best national and international practices, like the Tallinn Manual on the International Applicable to Cyber Warfare. Furthermore, a section on the legal aspects of cyber operations has been added to a new edition of the comprehensive Instruction on Compliance with International Humanitarian Law in the Armed Forces of Ukraine, which is currently under development.

Finally, we would like to emphasize the crucial role of organizational and legislative measures for ensuring compliance with IHL in cyber operations. We look forward to sharing our practical experience and learning from the experience of other states.

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

As we already stressed during the first session, Ukraine believes that, before more specific international legal regulations are developed, strict and rigorous compliance with IHL principles is a key to safeguarding civilians and other protected persons and objects against the danger arising from ICT activities during armed conflict.

In running its military operations, Ukraine takes into account the interconnection of ICTs and that a cyber attack or physical destruction of one ICT element might cause a chain reaction with potentially unpredictable consequences.

Therefore, to ensure compliance with the principles of distinction, proportionality and humanity, as well as to safeguard protected persons and objects in best possible manner, Ukraine refrains from any ICT operations, that

have a potential of causing physical destruction or rendering useless certain elements of ICTs, that may be vital for the survival of the civilian population. Furthermore, Ukraine refrains from attacking any elements of civilian ICTs, even if they are used for the direct support of military operations.

Another aspect are precautions against the effects of attacks on the civilian population taken by Ukraine in the spirit of Article 58 of Additional Protocol I. At this point, our delegation once again underlines that Ukraine faces an adversary committing flagrant IHL violations, including attacks on civilian infrastructure aimed at creating unbearable living conditions for the civilian population. This includes cyber attacks against information and communication networks, like the key mobile operators. In order to mitigate the consequences of such attacks for the civilian population, Ukraine implemented several measures including:

1. Physical protection of the civilian infrastructure against kinetic armed attacks;

2. Doubling the relevant ICT capabilities, for example, by ensuring that in case of a failure of one mobile operator, its users can immediately switch to another one;

3. Reserve power supply lines for critical civilian ICTs.

As our experience suggests, cyber operations and kinetic operations against ICT infrastructure jeopardize civilian populations, and precautions in defence against such attacks must be taken simultaneously.

* * *