My delegation would like to reaffirm that international law, especially the UN Charter in its entirety, international human rights law, and international humanitarian law apply to State conduct in cyberspace, and also that the imminent and outstanding question is not whether we need a new treaty, but how we can clarify the application of law in a uniform manner. Absence of a treaty simply cannot be an excuse.

We share the view that the current Ukraine situation reinforces the importance of international humanitarian law. We recognize that cyberattacks often take place in a hybrid format alongside conventional military operations. Nonetheless, our adherence to IHL must be consistent, not hybrid. My delegation believes it is imperative that IHL be part of the applicable law and also part of our discussion. As such, we suggest that we have a dedicated workshop or meeting in which experts or the IRC provide briefings.

Several delegations expressed interest in discussing what constitutes an armed attack in the cyber context. I believe that *jus ad bellum* is still a premature topic which can risk polarizing and diverting our attention without any prospect of convergence. Instead, we should focus more on the urgency of protecting and saving civilians with IHL.

My delegation would like to highlight two areas of international law
pertinent to ICT: the peaceful settlement of disputes and State responsibility. As I mentioned when we considered the previous agenda item, we can frame the application of law from the perspective of a targeted State.

The current international law on peaceful settlement does not just impose an obligation of resolving a dispute peacefully, but also provides us with a variety of procedural options, including fact-finding ones. The law of State responsibility too can be read in this way as a process of addressing an alleged breach, rather than merely apportioning blame. Thus, we can seek to expound on procedural guidance as to how a State can best address an alleged breach, step by step, in relation to other States. I believe that this could also constitute an important element of capacity building, including for those States exposed to cyber threats and attacks.

With regard to the issue of attribution, my Government takes a principled position that a sufficient level of confidence is needed for attribution. In real-life scenarios, this issue of attribution can be elusive and complicated, but this cannot be an obstacle to laying out what our cooperative obligations are when a cyber-incident occurs.

Lastly, my delegation lends its support for the proposals to make UNIDIR’s Cyber Policy Portal a repository for national views and the National Survey of Implementation. We also find the proposal to engage the ILC interesting, but only after a full and thoughtful discussion of what to ask.

Thank you. /END/