AHC 6th session: ICC Statement on groups 6 to 10

Thank you, Madam Chair,

Thank you, for the opportunity to share some brief comments on behalf of the International Chamber of Commerce, the institutional representative of 45 million companies in over 100 countries.

We align with the statements by the US Council for International Business, Microsoft and the Cybersecurity Tech Accord. I would like to focus my intervention on the articles related to criminalization in the Convention.

First, as we noted previously, we caution against unnecessarily expanding the scope of the Convention.

For the Convention to be effective, the technology industry and data custodians must have a clear understanding of what constitutes a cybercrime, so that they are able to respond appropriately to government requests for electronic evidence.

Therefore, the Convention should **focus on criminalizing only cyber-dependent offences**, and language in subsequent chapters should refer to *"offences set forth in this Convention"* so as to avoid expanding the scope of procedural and international cooperation measures to other crimes merely because a computer was involved.

We appreciate the efforts already made to tighten the text in this respect.

Second, given the large variety in domestic laws on cyber-related crimes and means of establishing jurisdiction over them, we urge states to maintain strict dual criminality requirements for all crimes and law enforcement measures covered by this Convention to avoid any unintended consequences and jurisdictional disputes.

Third, we encourage states to focus on *"serious crimes"* and **explicitly refer to *"offences committed with criminal intent"*** not simply *"offences committed intentionally"* as a prerequisite for exercising any powers over crimes included in this convention.

The Convention should use precise terminology and clearly defined terms and avoid the unqualified use of terms such as *"unlawful" (Article 10)* or *"dishonest" (Articles 11 and 12)*, which can carry various meanings across different jurisdictions and are generally used to refer to activity that is illegal, but not necessarily criminal.

Furthermore, such terms risk creating situations where acts carried out with beneficial intent, such as penetration testing and cybersecurity research might be criminalised. This increases the likelihood of prosecuting individuals for unintentional behaviour or behaviour that did not cause harm.

It may also increase the risk that companies offering cybersecurity solutions will be less willing to do so in jurisdictions where there is increased legal risk.

I believe this is all I could fit into my time, I thank you, Madam Chair.