International Chamber of Commerce

Intervention at the reconvened concluding session of the Ad Hoc Committee on Cybercrime

30 July 2024

Thank you, Madam Chair,

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

The establishment of this Committee offered an opportunity to create a unified framework for collaboration among nations to confront the challenges posed by cybercrime, harmonise legal approaches, and facilitate effective cross-border cooperation in combating this global menace.

However, the Convention in its current form risks falling short of these ambitions.

The global private sector remains concerned that the Convention continues to contain serious flaws, allowing its provisions to be potentially misused to compromise cybersecurity, data privacy, and fundamental rights and freedoms.

We see these flaws in three main areas:

1. As currently written, the Convention risks undermining **human rights**, particularly privacy and freedom of expression. It risks enabling intrusive cross-border data collection, infringing on individuals' rights and preventing people from challenging arbitrary access to their data. Others have spoken at length about these risks, and we especially draw your attention to the analysis shared by the OHCHR.
2. **Economic development** relies heavily on a predictable and secure business environment. A flawed treaty may impose conflicting national rules, leading to substantial legal and regulatory uncertainty, compliance costs and hindering international cooperation. Additionally, the uncertainty created by expansive and vague legal definitions could discourage cybersecurity research and innovation, essential for protecting digital ecosystems, with which the global economy is intertwined, and upon which it depends for growth.
   The Convention, in its current form, would make it increasingly difficult for providers to challenge overbroad requests or resist extraterritorial requests for data from law enforcement.
   Under such unpredictable and uncertain circumstances, commercial activities may suffer, reducing the potential to invest and innovate in digital services, which is especially alarming at a time when socio-economic development fuelled by digitalization is a priority worldwide.
3. **National security** is intricately linked to cybersecurity. The proposed Convention's broad data collection powers, without strong safeguards, may weaken global cybersecurity, making institutions and individuals more vulnerable to cybercrime.

The provision on compelled assistance (article 28, paragraph 4) could be interpreted to enable parties to the treaty to conscript people who have access to or otherwise possess the knowledge or skills necessary to break or circumvent security systems to help law enforcement access data on those networks. This must be removed, as it could even be interpreted to include compelled disclosure of previously unknown vulnerabilities, private encryption keys, or proprietary information like source code.

To mitigate these risks, we suggest the following, and refer you to our written input for specific recommendations:

1. Focus narrowly on cyber-dependent serious criminal offenses, keep the scope of all provisions on offences established by the Convention and remove references that could broaden the scope of the Convention and its procedural provisions
2. Avoid provisions that can lead to jurisdictional disputes or broad extraterritorial claims
3. Include robust safeguards to protect human rights, ensuring transparency, accountability, and judicial oversight in data access.

To conclude, the Convention must strike a delicate balance to support international cooperation between law enforcement while protecting human rights, fostering economic development, and ensuring national security. Without significant revisions, the current draft risks undermining these critical areas.

Thank you, Chair.