Statement by the International Chamber of Commerce to the

2nd Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Good morning, good afternoon, good evening everyone.

Thank you, Chair, 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.

I would also like to once again thank the group for accommodating input from observers, as a recognition of the need for multistakeholder cooperation on these matters.

Let me reiterate three basic principles that we already put forward at the first meeting, and that are seen by the global private sector as the baseline of the work of this Committee, and should be at the focus of the Convention's purpose.

1. Firstly, we recognize that **this instrument is intended to supplement major existing instruments in the field. Therefore, the private sector believes the Convention should be based on existing frameworks, such as the Budapest Convention, and its additional Protocols, for example, and avoid duplication of or including conflicting provisions with instruments already in place.**

   This relates to the definitions, scope and substance of the Convention. The Secretariat's overview of existing international instruments offers good guidance and we should give serious consideration whether there is an explicit need or gap to be filled by including specific issues in this Convention.

2. Secondly, we see **the purpose of the Convention to increase international cooperation to reduce the incidence, especially, of major cyber-dependent criminal activity and to protect the victims of such crimes. Therefore, we strongly urge the Committee to focus on cyber-dependent crimes with a threshold of criminal intent, which have a serious impact, and where the act is understood as a crime in the vast majority of member states.**

   One example of serious criminal activity that could be considered under this convention is the intentional development, spread and use of malicious computer code as cyber offensive tools to attack government systems, critical infrastructures or ICT supply chains. The Convention could consider measures to reduce and disincentivize the proliferation of such offensive cyber capabilities and tools and the broader marketplace that provides various tools and methods to ultimately enable cyberattacks for profit.

   The Convention should **not address traditional crimes, or cyber-enabled crimes simply because a computer or other digital tools were involved in their planning or execution**. This means close examination of what types of crimes can generally be covered by existing other statutes, and what capacity building is

necessary to equip all stakeholders, including law enforcement and the judiciary, to help prevent, detect and prosecute traditional crimes in the online environment. It also means **not including content-related crimes**, especially where there is dispute around the protection of human rights and fundamental freedoms like the freedom of speech and expression, or acts which may be unlawful but for which the state is not responsible for investigation, prosecution, and punishment of offences.

Cyber-enabled crimes should only be included under this Convention where the scale, scope, or speed of the offense is significantly increased by the use of online and digital tools, where the definitions are commonly understood, and where they are already an offense in the vast majority of member states. We suggest that these crimes are only considered after consensus has been reached on cyber-dependent crimes.

3. Thirdly, we understand **the Convention is intended to support efforts, on a cross-society basis, to cooperate in pursuit of a more stable, secure, trusted online environment for socioeconomic benefit of all and to support sustainable development through reducing the incidence of criminal activity online**.
   One example of this is the activities of those who defend networks, and who seek to identify vulnerabilities in systems, so they can be remediated before criminals can exploit them. Those engaged in these activities, including cybersecurity researchers and other professionals, should be specifically protected by the Convention.

And last, but certainly not least, as agreed, **decisions are to be taken by consensus, which is the way to ensure that the outcome will effectively inspire global cooperation.** To help us we should focus on widely understood criminal acts which have common, clear and compatible, definitions in many different legal jurisdictions. This is fundamental as many elements of cross-border crime cooperation are greatly limited or rendered ineffective if the acts aren't similarly understood in all jurisdictions with a role in addressing the incident.

ICC stands ready to work with you and your team, Madam Chair, as with the members of this Committee to offer further details on the role and views of the global private sector and help build bridges for further collaboration.

Thank you.