*[ADD RECIPIENT NAME*

*ADD RECIPIENT DESIGNATION*

*ADD RECIPIENT ADDRESS]*

*[ADD DATE AND LOCATION]*

**Subject: Global business views on a future Convention on cybercrime**

Dear *[ADD NAME(S)]*,

In today’s hyper-connected world, cybercrime has emerged as a pervasive and highly sophisticated threat, transcending national borders and affecting individuals, businesses, and governments alike. The ongoing work of the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC) has the potential to establish a unified framework for collaboration among nations, enabling them to address the challenges posed by cybercrime, harmonize legal approaches, and foster effective cross-border cooperation in combating this global menace.

At the same time, if negotiators fail to take account of the intricacies of practical international cooperation on crime of this kind, the Convention runs the risk of being operationally deficient. It also risks bringing further complexity and confusion into this space, if its provisions duplicate or contradict existing frameworks.

As Member States move to finalize the wording of the future Convention, I am writing on behalf of the International Chamber of Commerce (ICC) to share perspectives of the *[YOUR COUTNRY NAME]* private sector, developed in close collaboration with global business. Driven by the firm conviction that a secure and stable cyberspace is critical for fostering innovation, economic growth, and international trade, ICC has been actively participating in the work of the AHC since its inception to contribute the expertise and insights of the private sector.

We hope that our contributions help shape a Convention that provides a more predictable environment for businesses to operate in, reducing the complexities of dealing with cyber incidents that cross national borders, as well as a Convention that strikes a balance between effective cybercrime prevention, detection and prosecution and safeguarding data protection, privacy and human rights.

Please find attached a paper detailing our positions and recommendations on the draft text of the future Convetnion. In particular, we hope to have your delagtion’s support on the following considerations:

1. The core objective of the Convention should be to **enable, increase and strengthen international cooperation to reduce the incidence of serious cyber-dependent criminal activity**. To enable effective cooperationthe Convention’s provisions should be based on **dual criminality**, focusing on criminal acts that are similarly defined across jusrisdictions, while avoiding overly prescriptive provisions that may lead to conflicting rules and barriers to cooperation. Focusing on elements that are defined and understood similarly not only facilitates consensus in elaborating the text of the Convention, but also helps ensure its implementation and incentivizes cooperation.

To ensure cooperation, the **scope of the Convention must be clearly and narrowly defined and include appropriate safeguards** to ensure robust independent oversight and redress mechanisms, minimize and avoid conflicts with existing laws, create mechanisms to prevent conflicts, and resolve disputes that might arise.

1. The **scope of the Convention** should be narrowly defined to focus on **cyber-dependent serious criminal offenses**. The Convention’s criminalization chapter should concentrate on cyber-dependent serious criminal offenses, avoid treating traditional crimes as cybercrimes, and not duplicate offenses covered by other conventions. In the same vein, and to safeguard end-users against potential abuse of executive authority, the scope of application of all procedural measures need to be exclusively limited to crimes set forth in the Convention.
2. **Human rights and safeguards must be a core commitment in the Convention**, with protection for freedom of expression, access to information, and privacy. In particular, on matters of data access and sharing, the Convention should include **principles and provisions to ensure clarity and predictability in government access to digital information**. The Convention should embrace **transparency** as the general rule of thumb, taking into account that except in narrow circumstances, the public has a right to know how, when, and why governments seek access to their data. Furthermore, **real-time collection of traffic data and interception of content data are considered as significant invasion of privacy** and references to such practices should be removed from the Convention.
3. **Precise terminology and alignment with established definitions** are crucial to ensure future-proof and adaptable legislation. In particular, we recommend using the term **“cybercrime”** over “use of information and communications technologies for criminal purposes” throughout the Convention. For the purposes of this Convention, the term can be self-defining, under which we understand the crimes covered by the criminalization section
4. The Convention should **not create liability for third parties**, but encourage and permit the production of timely mitigation measures in case of detection of vulnerabilities. In particular, the Convention should **not seek to increase cyber resilience through the introduction of industry regulation.** Other means of regulating industry exist, and these should not be conflated with cybercrime policy through being included in this Convention.

Last, but not least, we wish to thank your delegation’s openness to the input of industry, and count on your support for the Convention to recognize the expertise of the private sector in preventing, detecting and fighting cybercrime, including by ensuring the meaningful participation of business and other stakeholders in any follow-up mechanism to the Convention.

We would be delighted to discuss these points with your delegation either in advance of, or during the upcoming meeting of the AHC in New York on 21 August – 1 September. Should this be of interest, please do not hesitate to contact me or [Timea Suto](mailto:timea.suto@iccwbo.org), ICC Global Digital Policy Lead at your earliest convenience.

We count on the continued leadership of *[ADD YOUR COUNTRY NAME]* to guide the drafting of a Convention that fosters a safer digital environment and bolsters international cooperation in the fight against cyber threats.

Yours sincerely,

*[ADD YOUR NAME]*

*[ADD YOUR DESIGNATION]*