ICC Key Messages on the UN Cybercrime Convention Negotiations

1. ICC, has been engaged throughout the process of discussing the Cybercrime Convention, and continues to support a treaty that strengthens the fight against cybercrime. However, based on how the text stand at the current state of negotiations, a number of amendments are required to prevent the Convention from being abused to criminalize everything from protected free expression to the activities of good-faith cybersecurity researchers, enabling sweeping new transboundary surveillance powers, and expansion of cross-border government access to personal data without meaningful due process safeguards.

2. Convention that would enable any government to request and obtain the personal information of citizens of other countries, without robust, explicit jurisdictional limitations or sufficient procedural safeguards, in secret and in perpetuity, is not consistent with the rule of law. This Convention must have reasonable transparency provisions that empower persons whose data has been transferred to know this has taken place, provided such notice and transparency does not prejudice ongoing investigations or prosecutions. It must also allow providers to object to requests for data in certain circumstances, such as where they would have to violate the law in one jurisdiction to comply with a request from another.

3. We understand the logic behind copying and pasting provisions from other crime treaties, such as the Budapest Convention, into this Convention. However, we urge policymakers to carefully consider whether this will produce a similar framework when applied in domestic legislation as part of this Convention. The Budapest Convention was adopted with a 60-page Explanatory Report specifying the additional checks and balances and rule of law-based environment that parties should have underpinning its provisions. The Budapest Convention also has a review mechanism which provides that its Secretariat regularly publishes evaluations of whether States Parties have implemented the provisions as intended with respect to both the text and the Explanatory Report. This Convention has neither.

Our concerns fall into six main areas:

1. Protecting national security by preventing abuses of the powers of the Convention
2. Ensuring the private sector can cooperate effectively and more quickly with law enforcement by preventing known conflicts of law issues from blocking cooperation (Articles 18, 22, and 24);
3. Ensuring the Convention's legitimacy is not undermined through permanently secret personal data transfers and ensuring the ability of providers to object to requests in specific circumstances
4. Ensuring the Convention does not weaken global cybersecurity (particularly by ensuring cybersecurity researchers are not put in legal jeopardy by the Convention's provisions.
5. Strengthening dual criminality provisions throughout the Convention to help expedite cooperation requests between states and between states and service providers
6. Restoring the scope of the Convention to focus on cyber-dependent serious crime and avoid potential abuses

ICC has submitted detailed views on these topics, and more ahead of the 6th session of the Ad Hoc Committee that recently concluded in New York and are happy to provide also red-line edits and textual proposals on these points, if of interest.

International Chamber of Commerce Sweden
Storgatan 19, 114 51 Stockholm
+46 (0)8 440 89 20 | **icc.se**