International Chamber of Commerce

Industry Perspectives Ahead of the Reconvened Concluding Session of the UN Ad Hoc Committee on Cybercrime

In our increasingly interconnected world, cybercrime stands as a pervasive and highly sophisticated threat that transcends national borders, affecting individuals, businesses, and governments on a global scale. Cybercriminal activities frequently extend beyond territorial boundaries, emphasizing the imperative need for robust international collaboration at the heart of effective prosecution. Collaboration at this scale and on such a sophisticated matter can only be efficient if founded on a shared comprehension of cyber offenses among all involved parties.

The establishment of the United Nations Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes offered an opportunity to build a comprehensive and robust international framework that defines the scope, sets the objectives, and describes the mechanisms of such cooperation. An international framework that would not only facilitate cooperation across all states and relevant stakeholders, but also bring a common understanding to developing national legislations in harmony, that collectively tackle cybercrime.

However, as negotiations progressed, it became increasingly clear that the Convention, based on the current draft, will fall short of these ambitions. Concerns of the global private sector remain that the Convention continues to contain serious flaws, allowing its provisions to be potentially misused to compromise cybersecurity, data privacy, and online rights and freedoms.

Human Rights Impact

As currently written, the Convention risks undermining human rights, particularly privacy, freedom of expression, and access to information. Its overly broad and vague provisions could enable intrusive cross-border data collection, infringing on individuals' rights and preventing them from challenging arbitrary data access.

The Convention's proposed mechanisms on sharing electronic evidence on serious crimes, without adequate safeguards, could empower governments with tools to demand and obtain sensitive data. The Convention also allows states to keep all data access requests secret indefinitely and lacks due process protections or mechanisms for providers to appeal against overbroad requests. Furthermore, the Convention's provisions could enable the prosecution or coercion of individuals to subvert technical access controls, undermining cybersecurity and exposing individuals to risk. This

lack of transparency and accountability in data access requests prevents individuals from challenging such actions and protect their privacy.

Additionally, the Convention's provisions on the application of human rights and safeguards are qualified to correspond with domestic law, which in numerous cases would mean little to no protections as obligations under international human rights law are unevenly implemented across jurisdictions.

Read together, these provisions show the absence of meaningful safeguards and oversight mechanisms that would likely result in the misuse of procedural powers, limiting fundamental rights and freedoms.

Economic Development Impact

Economic development relies heavily on a predictable and secure business environment. A flawed treaty may impose conflicting national rules, leading to substantial 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.

The Convention, in its current form, would make it increasingly difficult for providers to appeal against overbroad requests or resist extraterritorial requests for data from law enforcement. This could particularly impact the safety of industry employees in jurisdictions where staff who refuse to provide data may be subject to arrest as accessories to the crime for which data is being sought.

Under such unpredictable and uncertain circumstances, commercial activities may suffer, reducing the potential to invest and innovate in digital services. Economic growth could be stifled, which is especially alarming at a time when socio-economic development fuelled by digitalization is a priority for countries worldwide.

The risks posed by a flawed treaty could hinder progress in creating a stable and secure environment necessary for thriving economic development.

National Security Impact

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.

Unchecked data collection, including from traveling company employees, government officials or government contractors, could lead to sensitive information being exposed or misused, increasing the risk of security breaches and unauthorized access to critical information.

Furthermore, the provision on compelled assistance (article 28, paragraph 4) could be interpreted to order people who have knowledge or skills in breaking security systems to help law enforcement break those systems. This must be removed, lest the power could even be interpreted to include compelled disclosure of vulnerabilities, private keys, or proprietary information.

Additionally, an unpredictable legal environment might deter critical security research, allowing malicious actors to exploit digital weaknesses.

The lack of clear definitions and robust safeguards could hinder effective cybersecurity measures, leaving nations exposed to sophisticated cyber threats. The potential for overbroad or extraterritorial data requests could strain international relations and cooperation, further complicating efforts to combat cybercrime on a global scale.

Recommendations for an Effective Convention

To mitigate these risks, the Convention should:

1. Focus narrowly on cyber-dependent serious criminal offenses and keep the scope of all provisions of the Convention on offences established by the Convention:
   - *Remove references that could broaden the scope of the Convention and its procedural provisions, such as article 23, paragraph 2 (b) and article 35, paragraph 1 (c), as well as references to other crimes in article 23, paragraph 2 (c), article 40, paragraph 1, and article 47, paragraph 1 (a);*
2. Avoid provisions that can lead to jurisdictional disputes or broad extraterritorial claims:
   - *Remove article 22, paragraph 2 except for subparagraph (b);*
   - *Remove article 27, paragraph 1 (b);*
   - *Remove article 28, paragraph (4);*
3. Include robust safeguards to protect human rights, ensuring transparency, accountability, and judicial oversight in data access:
   - *Support the inclusion of article 6 and article 24, with strengthened language not limiting the granting of safeguards to domestic law alone;*
   - *Include language in articles 25 to 28 to:*
     recognize that, except narrowly defined circumstances, the public has a right to know how governments may access their information and under what circumstances third parties may be obliged to provide it to public authorities;
     allow technology providers an opportunity to challenge demands for data on behalf of their customers, including those based on potential conflicts of law;
     ensure legally binding remedies are available to data subjects in the event of a breach by the government of the access, use, and retention rules;
   - *Remove articles 29 and 30 and related references, such as Article 40 paragraph (3), subparagraphs (e) and (f);*
4. Align definitions with those of the Budapest Convention;
5. Support legitimate cybersecurity research and protect good-faith researchers from criminal prosecution.

In summary, 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, necessitating a cautious approach from the international community.