Submission to the Third Substantive Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes

ICC United Kingdom welcomes the opportunity to submit our views to the Third Substantive Session of the Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

These considerations build upon our previous submissions and interventions, especially that prepared for the second session, available here. We also support the submission of Microsoft, to be found here.

Our recommendations on these sections are based upon a few fundamental principles:

1. **Dual criminality must be the starting place for international cooperation on cybercrime.** Experience with transboundary crime cooperation has clearly shown that it is frustrated where the act is not recognised as criminal in all the concerned jurisdictions. It is not enough for the convention to provide that all crimes under the convention will be treated as if they are criminal acts for the purposes of cooperation by Parties. The acts themselves must be recognised as crimes at the national level as prior experience shows that cooperation is likely to be declined if that is not the case. A dual criminality threshold is important not just for effective cooperation to take place - it is also an essential guarantor that human rights will be protected effectively.

2. **Where it is valuable to draw commitments from existing instruments priority should be given to those, particularly the Budapest Convention and its Protocols, that specifically address cybercrime**, over broader international agreements addressing crime. This is important for many reasons, amongst them being that the likelihood of unanticipated negative consequences will be reduced, and the prior experience in application of such provisions to cybercrime can be better leveraged.

3. **The Convention should be silent on the liability of third parties, given its complexity and rapidly evolving nature at the national level globally.** Simply repeating provisions from instruments developed decades ago to address entirely different areas of criminal activity risks unanticipated negative consequences to society - particularly but not only

human rights - and the economy when applied in this domain under today's circumstances. If a consensus emerges that such a provision is necessary, the model should be that of the Budapest Convention.

4. **The provisions in the key areas being discussed at this session should be focused on addressing serious crimes as, if this Convention fails to do so, it will be seen as a failure.** Far too often, major cybercrimes do not attract sufficient consequences to deter further similar acts, which is leading to very significant escalation in the volume, severity and impact of cybercrime globally. This trend must be reversed, and a focus on serious crime is the prudent way to do that especially given the existing constraints on international cooperation on transboundary crime due to rapidly increasing volumes of requests and their associated complexity in the digital environment.

I. International Cooperation

The convention should foster and develop international cooperation on investigation and prosecuting cybercrime, both between governments and law enforcement agencies, and between national law enforcement agencies and their stakeholders. These should be accompanied by strong safeguards protecting human rights and fundamental freedoms, should be based on existing tested and proven mechanisms.

- **The provisions in international cooperation should include a strong opt-out mechanism where dual criminality does not exist.** This will act as an important human rights safeguard to ensure users are not prosecuted on the grounds of political offences, race, religion, gender, or other protected characteristics.
- **The convention should be aligned with existing tried and tested mechanisms, particularly the Budapest Convention and its Additional Protocols**. This will save valuable time instead of 'reinventing the wheel' and will reduce the likelihood of establishing conflicting rules that raise barriers in international criminal cooperation.
- **The provisions should foster trust on a multi-sectoral basis and avoid being overly state-centric.**
- **To the extent there is a consensus for the international cooperation provisions to apply to crimes outside of the direct scope of the Convention they should be limited to serious crimes only and strictly subject to dual criminality.** There is already a global lack of capacity at the national level to address cybercrime; increasing the volume of requests in each jurisdiction just to address the crimes directly covered by this convention will be challenging enough.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

- **With respect to access to and requests for data** we refer you to our comments on this subject for the second session, available here, and add the following specifics relevant to this section of the Convention:
    - Whenever possible, digital evidence should be obtained from the entity most directly offering the service, or closest to, the data subject. As both public and private entities move their digital information to the cloud and use cloud-based infrastructure to deliver applications and services, governments often have multiple sources for the same digital information. In many cases this will not be the cloud provider themselves. Going directly to the entity that is the data controller can often be done without negative consequences to investigations, just as was the case before the organisation moved its data to the cloud - and the controller may have better access and context to the data sought in any case, improving the value of what is provided to governments.
    - Regarding the real-time collection of information, the convention should embed principles of proportionality and necessity to ensure it does not (a) ignore the particularly intrusive nature of real-time surveillance; and (b) represent a significant expansion of terms used in current mutual legal assistance treaties (MLATs). The convention should also create a right of refusal to cooperate, in particular when the protection of human rights might be at stake, and it should recognise that not all types of access are technically possible for all types of information or in all jurisdictions.
    - The Convention should specifically address personal data protection, obligating that a state party transmitting, or holding, personal data must do so in compliance with domestic and international legal obligations regarding its protection, particularly those relating to the jurisdictions to which a data subject belongs. While this introduces complexity, it is of fundamental importance to ensuring effective cooperation. Systematic failure by a party to effectively protect personal data that it has requested over time should be grounds for refusal of future requests as well.
- **Avoid establishing conflicting rules that raise barriers for international criminal cooperation, and explicitly recognise that conflicts of laws situations will arise.** Data flows are global, yet national rules vary considerably and are not always compatible across jurisdictions. Because compliance costs from conflicting rules are enormous, governments should ensure that legislation provides maximum flexibility and creates the least risk of conflict. Examples of these types of policy issues include, data localization or access laws, data retention laws and data protection laws. The private sector already has to deal with situations where one country's laws can create

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

significant conflict when responding to lawful demands around the world, where complying with one request in one jurisdiction would breach laws in another. The convention needs to recognise this explicitly and ensure that such a request can be denied on such grounds, referring the requesting state to the jurisdiction where the legal problem has arisen.

II. Technical Assistance and Capacity Building

ICC United Kingdom believes that the Convention's commitments in this area are of fundamental importance as many states do not have the technical capacity to effectively tackle cybercrime. This Convention cannot succeed if its Parties do not have the means to effectively implement it in practice, and that will require a considerable increase in the level of resourcing available globally to facilitate legal, policy, and human capacity at the national level in every country as otherwise criminals will simply migrate their activities to jurisdictions where they are less likely to face negative consequences for their actions.

A universal minimum capacity at the national level is required to effectively tackle this truly global issue in a range of key areas. We see these listed in many submissions for this session of the Committee. We therefore suggest the following:

- **The Committee should dedicate time, through intercessional meetings specific to the subject, to quantify what the minimum national elements of law, policy, and human capacity are in order to effectively implement the Convention when it is concluded.** These discussions should capture the expertise and experience of international organisations and stakeholders with specific expertise in the subject. The results of those deliberations can then be included in the Convention, alongside measures intended to ensure these minimums can be met, with an overall increase in the capacity of states' law enforcement and judicial systems within an overarching framework of international human rights law.
- **The provisions in this section should be technologically neutral** so they stand the test of time.

III. Preventive Measures

Preventive measures - such as cybersecurity education, raising awareness, and increasing public-private partnerships - are an effective tool to counter cybercrime. However, it is not the role of this convention to address such subjects, which have their own fora and processes and

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

requisite expertise. Rather, it should concentrate on dealing with cybercrime and cybercriminals.

- The Convention should not create mandates for industry regulation, principles, or standards. These are all best left to the national level and existing standards development processes.
- Provisions on preventive measures should reflect the importance of partnerships. The private sector, academia, and civil society can and do provide important expertise.

IV. Mechanism of Implementation

- **Ensuring robust multi-stakeholder participation in the mechanisms for implementation is of fundamental importance.** Stakeholders are integral to reducing cybercrime, and the private sector in particular is indispensable given that investigation and prosecution of cybercrime generally requires private sector cooperation in evidence gathering in particular.
- **The body responsible for implementation of the Convention should have, as one of its specific tasks, ensuring that the level of capacity building and technical assistance required actually is available and proving effective**. Without the necessary resources and implementation capacity this Convention risks being far less effective than the times require. It will not be enough simply to ratify the Convention; implementation requires continual effort as criminals adapt to the development in technology and officials and stakeholders have to adapt to meet new challenges.
- **The body responsible should specifically be mandated to address, at a technical level, any common issues found at the practical level in implementation of the provisions of the Convention**, and such processes must involve stakeholders in order to be successful. As the saying goes, the devil is in the details - past experience in addressing transboundary cybercrime shows us that the agreement that facilitates cooperation is the tip of the iceberg; the ongoing work to facilitate cooperation day-to-day is indispensable.

V. Preamble and Final Provisions

The preamble and final provisions will set the raison d'être of the treaty. As many states have agreed, while we are not drafting a new human rights treaty, protecting users from malicious

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

crimes in cyberspace is in itself a human rights issue; ensuring their rights are protected in doing so is of fundamental importance and the Convention's provisions should ensure that this is the case. Finally, drafting of these provisions will be greatly facilitated by first agreeing the operative contents of the Convention and then tailoring these provisions to them, and not the other way around.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk