Submission to the Fourth 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 Fourth 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.

Our submission builds upon our previous submissions and interventions, especially that prepared for the Second Substantive Session, available here. We support the Substantive Considerations on an International Instrument on Cybercrime, developed by the International Chamber of Commerce globally, which will be available soon on the AHC 4th session page. Finally, we also support the statement of Microsoft made to this session.

Comments on the method of working proposed for the Fourth and Fifth Substantive Sessions

We appreciate the need to accommodate informal negotiations on subjects at issue in the forthcoming stages of the process, however, we believe that stakeholders should be allowed to observe these discussions. We add fundamental value to the process and the outcomes will have significant impacts upon us and industry will have an important role to play in the success of the Convention. Our experience in how criminal enforcement works presently, and what can be done to make it more effective, should be welcomed throughout the process of developing the text.

Recommendations on the Consolidated Negotiating Document

We believe the document fairly represents all the proposals made - our comments on it are based upon the fundamental principles below. We follow the principles with recommendations on specific articles.

Criminalisation Chapter

The focus of this Convention should be addressing cyber dependent crime - defined as offences which cannot be committed without ICTs - and those which are serious - for which conviction carries a mandatory period of incarceration. According to estimates the

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

global cost of cybercrime is expected to rise from $8.44 trillion in 2022 to a staggering $23.84 trillion by 2027, an amount larger than the GDP of the world's largest economy[1]. This Convention will be seen as a failure if it does not have a meaningful impact on reducing the incidences of, and impact of, serious cybercrime. Subsequent protocols to the Convention can address additional offences as required.

Far too often, major cybercrimes do not attract sufficient consequences to deter further 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 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. It should be possible for State Parties to require that the conduct described in each article must result in serious harm for it to attract obligations for that party. **Examples of offences that should be included in the Convention are those in Articles 6-10 and 16 of the Consolidated Negotiating Document ("CND"), where modified as we recommend.**

1. **Crimes to be included should have the following additional characteristics:**

    a. **Offences included should already be reflected as criminal acts - not merely unlawful - in national law in a large majority of member-states, and with compatible definitions.** This will have many benefits, including more rapid ratification and entry into force of the Convention, and it increases the likelihood of rapid responses to transborder requests for cooperation in pursuing criminals due to dual criminality being more obviously applicable.

    b. **All offences should require criminal or malicious intent and not intent alone.** Thresholds such as "without authorisation," "without right," and "unlawful" allow prosecution of behaviour which did not intend or result in harm. This is of fundamental importance as otherwise acts which are widely desirable and valuable to modern societies will be at risk due to increased potential risks. Here are three examples:

        i. **Articles 6, 7, and 8 could create criminal liability for journalists and their sources.** Their sources and whistleblowers could also be seen as criminals: both the sources and the journalist *intended* to provide unauthorised material to others and to review that material, respectively, but their intent was not *criminal,* it was, however, both "without authorisation" and "without right" and a statute could even inadvertently include these activities as "unlawful" depending on the drafting.

        ii. **Article 10 as presently drafted could open vendors of an app, as well as app store providers, to criminal charges if an app has a vulnerability that allowed**

[1] Estimates from Statista's Cybersecurity Outlook.

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

the compromised device to be used for criminal activity. Even though neither the vendor or the store had knowledge, nor could they reasonably be expected to know, about the vulnerability and while they certainly had no malicious intentions they did *intend* to make the application available. The present wording could allow this normal commercial behaviour to be criminalised;

iii. **Most of the articles in the criminalisation section would criminalise the work of penetration testers and security researchers**, as by definition their work involves intentional penetration of networks, accessing them, reviewing and retrieving information, and interfering with systems and devices. Their activities, by design, are frequently "without right" and "without authorisation" and depending upon the drafting of statutes they could also be inadvertently caught up if the threshold is "unlawful."

c. **Where there is consensus to include cyber-enabled crimes, these should be strictly limited to those acts where the use of ICTs dramatically increases the scale, scope, and speed of the offence**. The convention should not include offences just because ICTs were used in their commission; criminals communicating online about the commission of theft, fraud, extortion, or other kinetic world crimes does not justify special treatment as cybercrimes. Since provisions to extend the procedural measures and international cooperation chapters of this Convention to criminal activity not directly covered by the Convention are proposed, these acts' online dimensions would have all the procedural and cooperation provisions available to states in any case. **Therefore the articles on forgery (11), fraud (12), theft (13), payments (14), copyright (17), drugs (30), arms trafficking (31), distribution of counterfeit medication (32), money laundering (33), and obstruction of justice (34) should be removed.**

2. **Offences addressing online content should only be included where the offence is not already covered in other international agreements**. **Articles which should be removed for this reason include copyright (17) and genocide (28).**

3. **Further, offences related to content should be excluded except where there is consensus amongst all negotiating states on the definition of the acts and a demonstrable need for them to be addressed as cybercrimes.** Cooperation requires a compatible view of offending content as a crime across all jurisdictions and this is an area where there is very little convergence, and even less on what would rise to the level of criminality. For example, while the non-consensual dissemination of intimate images is noxious, defining what constitutes an infringement relies upon national law and social norms related to sexuality which themselves are subject to very different interpretations. Therefore, including such provisions has considerable risks of unintended

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

consequences to states' obligations in other areas of international law, particularly human rights and at a practical level makes a finding of dual criminality problematic, without which cooperation is frustrated. In the case of subversion, extremist content and terrorism, these acts are dealt with through existing international agreements[2].
Therefore the articles on Encouragement of or coercion to suicide (23), sexual extortion (24), non-consensual dissemination of intimate images (25), subversion (26), extremist content (27), and terrorism (29) should be removed.

4. **The Convention should not criminalise offences related to data protection solely on that basis.** While the motivation behind proposals for inclusion is understandable, data protection legislation is very different globally and is under revision in many jurisdictions. How infractions are dealt with is subtle, complex, and routinely shifting especially with respect to how sovereigns address international dimensions of use of personal data of their nationals and the nationals of other countries[3]. It is also the case that there are existing, lawful and routine situations where personal information is accessed in the normal course of business which would fall within the drafting of this article. Last not least, what constitutes 'personal information' widely varies across the globe, making a finding of dual criminality even more complicated. The risk of unanticipated negative consequences of broad-brush criminalisation, such as proposed in Article 15, is simply too great. **Article 15 should therefore be deleted.**

Procedural Measures Chapter

This Convention is a major opportunity to foster more effective public-private cooperation in reducing cybercrime. One of the most important aspects of this is in how evidence is gathered through public authorities gaining access to data necessary to combat cybercrime.

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 relevant comments to the third session, available here.

The following additional points are also relevant:

1. **The convention should embed principles of proportionality and necessity regarding**

[2] A few examples are: Article 28, where the 1948 Convention on the Prevention and Punismhent of the Crime of Genocide already criminalises "public incitement to commit genocide" (Art 3) in a technology-neutral formulation. Article 29 could conflict with the 1999 International Convention for the Suppression of the Financing of Terrorism which already criminalises financing of terrorism, also in a technology-neutral formulation.

[3] In that light, on 14th December 2022. The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities was adopted. Amongst other things it clarifies law enforcement agencies can access personal data under existing legal frameworks, as well as addressing how legal frameworks regulate government access; the legal standards applied when access is sought; how access is approved, and how the resulting data is handled.

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

data collection and retention provisions to ensure they do 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 – particularly 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.

2. **The Convention should provide for custodial requirements on State Parties transmitting, or holding, personal data in compliance with domestic and international legal obligations** particularly where it relates to natural persons who are neither nationals nor legally resident in the territory of the State Party that holds their information. 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.

3. **The convention should 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 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 and recognising that third parties cannot be required to break the law in one jurisdiction in order to fulfil lawful requests in another.

4. Given the absence of robust safeguard provisions in the present draft - about which we speak in more depth elsewhere in this statement - **we cannot support inclusion of provisions on real-time access to content and traffic data at the present time.** We understand the importance of these activities in cybercrime enforcement and we hope that negotiators are able to include sufficient safeguards, and agree during the fifth substantive session on the necessity of dual criminality for operation of the convention, such that more carefully drafted provisions on these matters can be negotiated. **Therefore, we suggest that Articles 47, 48, and the relevant references to those articles are all deleted pending a resolution of the referenced issues.**

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

Comments on Specific Articles

General Provisions

The proper object of the treaty is "cybercrime" and not "Information and communications technologies for criminal purposes." The former term is more focused and well understood in international criminal law; the latter could allow the scope of the convention to apply to any object that has integrated circuits, such as a modern calculator, and we submit that such a scope would undermine the Convention's effectiveness considerably and open the door for very large numbers of requests for cooperation on minor offences, undermining cooperation on major offences. All articles should be modified accordingly, in this section Articles 1 and 3.

Article 2, Use of Terms: While we agree that definitions cannot be finalised until the text is more advanced, we think having working definitions to use as the rest of the text is negotiated will help all parties, **so we recommend that the negotiators agree that the starting place for negotiation of definitions should be those in the Budapest Convention.**

Article 3 (scope of application): As we have stated before we believe the focus of the convention should be on serious crimes and recommend making this clear by removing the brackets in Article 3(2) around 'serious crimes' and deleting the other options. Finally, we find the proposal in article 3(3), a modification of Article 3.2 of UNCAC, to be problematic as it would broaden the scope of the Convention to all acts, even those which did not do harm. We recommend restoring the original text from the source or deleting this provision. Further, a new provision should be added to ensure that activities which are conducted in good faith for legitimate purposes - such as penetration testing - do not fall within the scope of the Convention. The convention should not just avoid criminalising these activities, it should promote their work by ensuring their activities are protected.

Article 5 (respect for human rights) should become Article 4, to give human rights greater importance and it should contain references to specific human rights instruments, including ICCPR and UDHR amongst others. The qualifier "applicable" should be deleted: the protection of human rights must be an integral obligation of the Convention.

Article 4 is not needed. Sovereignty should not be a central feature of this Convention. Sovereignty and related issues are already core elements of international law, and the rights of sovereigns is not the objective of this convention; crime prevention and prosecution are. Extending the rights of sovereigns would actually be counterproductive in a Convention which seeks to promote collaboration on legal matters *between* sovereigns.

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

Criminalisation

References to critical infrastructure should be bracketed pending more clarity on what is meant by the term in the context of this Convention. We understand the motivation behind these elements however there is no international agreement on the definitions of the recognised types of critical infrastructure, and each member-state designates what it determines to be critical infrastructure; cooperation requests related to such offences are therefore quite likely to result in a failure of dual criminality which will frustrate cooperation that might otherwise have been successful, unless the provisions addressing this issue are very carefully crafted and more specific.[4]

All articles retained should be amended as follows:

1) Require criminal or malicious intent for the above referenced reasons; some articles make this optional, and some do not; such references could then be deleted;
2) Insertion of a new provision in each that a State Party may require that the conduct described in the article result in serious harm.

Articles 11-15 and 26-34 should be deleted for the reasons previously stated.

The Convention should not establish liability for third parties through a stand-alone article and instead cover those relevant elements in the procedural chapter as necessary. This is even more true given the very expansive scope of criminal offences in the current text**.** Third party liability is very complex and in national legislation addresses issues far beyond criminal law, creating the real possibility for obligations in this Convention to create unanticipated issues outside of criminal law at the national level. Moreover, member-states approach liability of third parties in very different ways making conflict of laws problems in transborder application even more likely. **Accordingly, Article 35 should be deleted.**

Child Sexual Abuse Materials (CSAM) Articles: While we understand and agree with the desire of member-states to provide for CSAM provisions in the Convention we submit that the provisions should be very carefully drafted so that they are most effective in day-to-day enforcement operations, covering activities which are widely recognised and subject to common interpretation across member-states. For example offences related to 'stalking' may well be very difficult to define in a manner that is understood across all member-states such that it facilitates expeditious cooperation on specific incidents. The objective should be to ensure that the Convention's provisions, when adopted in statute, are very likely to ensure that dual criminality will be readily mutually recognised during enforcement operations to help speed responses to these offences and increase the likelihood of successful prosecutions.

[4] Industry is strongly in favour of greater protections for critical infrastructure and participates in the work of the UNGA First Committee in that vein, where we have repeatedly called for more action for protection of CI and CII.

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

Article 39 (prosecution, adjudication, and sanctions): for the reasons previously mentioned we recommend 39.1 be modified to require a threshold of serious crimes, which should be understood as those offences that attract a minimum term of incarceration of three years. We further recommend modification of 39.2 to set a threshold for access to confidential government information which is obtained for criminal or malicious intent - as otherwise, as we have previously referenced, inadvertent criminalisation of activities such as whistleblowing may result. Finally, we recommend adding a right of appeal to 39.5, after the right to a fair trial, for obvious human rights reasons.

Procedural Measures

Article 40 (Jurisdiction): Article 40(2)(e) is novel in international criminal law and is not sufficiently clear to avoid extra-territorial impact; we recommend it be deleted. 40.5 should be rephrased to the Budapest Convention language ("determining the most appropriate jurisdiction for prosecution" rather than on "coordinating their actions").

Article 41 (Scope of procedural measures): 41.2(b) and (c) should be limited to serious crimes only, and then kept only if the many issues we've highlighted with safeguards more generally are resolved. Accordingly, we support leaving both bracketed options as they are, or deleting 41.2(b) and amending 41.2(c) such that both bracketed options at the end of the sentence are deleted. 41.3(a) and (b) should delete relevant references to real-time collection for the reasons previously articulated.

Article 42 (Conditions and safeguards): We propose several amendments to this article congruent with earlier comments both in this statement and those made to the Second and Third Sessions of the AHC:

1. Article 42.2: Provisions should be added to:
    a. Facilitate third parties in challenging requests made by a State Party in relation to the powers and procedures of this Convention on the basis of legality, proportionality, or necessity, such challenges to be adjudicated by an organ of the State Party independent of the requesting agency;
    b. Allow third parties to initiate a review of decisions made in relation to the immediately-previous point independent of the organ of the State responsible for adjudicating the decision;
    c. Allow third parties who are custodians of communications to disclose to the legal or natural persons the data, including traffic data, directly related to them that has been disclosed to a State Party, provided that doing so does not prejudice an ongoing investigation;
    d. State parties shall address requests for data to the owner of the data who is the proximate source and rights holder. This is consistent with the Trusted Cloud Principles and represents international best practices that are critical to maintain

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

trust in global data flows. This is also essential for expeditious replies to requests, as addressing requests to another entity will not be successful due to conflict of laws issues.

e. Article 42.3: a provision should be added to the end of this element ensuring that liability does not arise for third parties that do not act as requested or required by a State Party in relation to the powers and procedures in the Convention where doing so would require it, or them, to act unlawfully in the jurisdiction of another State.

2. A new provision should be added such that each State Party shall ensure that the data, including traffic data, of persons who are subject to the jurisdiction of another State Party or territory, which is acquired by the State Party through the powers and procedures of this Convention, are protected from modification or disclosure to unauthorised persons, and that any such data should be expeditiously deleted when it is no longer required for an ongoing investigation or prosecution. The data should also not be used for any purpose other than that for which it was originally requested.

Article 43 (expedited preservation of data): We recommend the following amendments:

1. 43.1 - the phrase "or similarly obtain" should be deleted as this article relates to preservation of data not to disclosure of that data. The final phrase ("including due to expiry of the retention period…" should be deleted; doing so would bring the article into congruence with the Budapest Convention (and the issues around retention are better dealt with in 43.2).
2. 43.2 - the article should be modified such that data may be held for up to 90 days, renewable for a total of one year.

Article 44 (Expedited preservation and partial disclosure of traffic data): The article should be amended to allow for preservation for 90 days, renewable for a total of one year.

Article 47 (Real-time collection of traffic data): As above referenced, we believe this entire article should be removed pending agreement on, *inter alia*, sufficiently robust safeguards and that dual criminality is necessary for the cooperation provisions to take effect. Only after that should this subject be considered and then the text would have to be significantly revised.

Article 48: (Interception of content data): As above referenced, we believe this entire article should be removed pending agreement on, *inter alia*, sufficiently robust safeguards and that dual criminality is necessary for the cooperation provisions to take effect, and then the text would need to be significantly revised. If those issues were resolved, some examples of modifications of this article that would be necessary are:

1. 48: change the object of this article from "interception" to "retrieval." The former term has many negative connotations that fall outside of criminal law and lawful access.
2. 48.1: deletion of the text following the phrase "... to empower its competent authorities

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

to:" to bring this article into congruence with the Budapest Convention; the added text is largely redundant given the conditions listed in the rest of 48.1;

3. 48.1(b)(ii): Modify this provision to make clear that content data is the subject of the provision and that it relates to specified communications in its territory.
4. 48.3: We believe this provision should be deleted or modified as service providers should be able to disclose these facts to those affected where it does not prejudice an ongoing investigation or prosecution as we have proposed in Article 41.

We thank the Committee for its consideration and look forward to further discussion of these issues during the Fourth Session.

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