Submission to the Second Session

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

ICC United Kingdom greatly appreciates the opportunity to participate in the deliberations of the Ad-Hoc Committee ("AHC") as a stakeholder. We see this as a profoundly important process that could considerably reduce the scope of cybercrime globally and thereby increase trust in the online environment for all, while reducing the very serious economic burden that growing transboundary cybercrime imposes on all stakeholders, including the private sector.

As the focus of the second session will be on the preamble, general provisions, and provisions on criminalization our submission focuses on these elements. Our comments supplement those of the International Chamber of Commerce of which we are a member, and we associate ourselves fully with its statements.

Foundational Concepts Applicable to the Entire Convention

Our submission is based on a foundational conception of the scope of the Convention which can be distilled as follows:

The Convention should focus on cyber-dependent crimes already reflected in the national legal traditions of a large majority of member-states, and cyber-enabled crimes should be covered only to the extent that those crimes are dramatically transformed by use of ICTs in scale, scope and speed, *and* where inclusion meets a series of tests we outline below. The reasons for these limitations are simple:

- The Convention will be most effective if it limits itself to essential provisions that can be complied with and implemented by as wide a number of member-states as possible without requiring new crimes to be inscribed in statute or significant changes to existing crimes, given that transboundary judicial cooperation is largely dependent on whether the act in question is compatibly defined in the jurisdictions where cooperation is necessary.
- Creating obligations to enforce crimes related to subjects which are not widely recognised across all member-states as *criminal* acts should be avoided - for the same reasons as listed above. We note that a number of states have proposed including acts in the Convention which are illegal acts subject to civil penalties and not criminal acts even in the proposing jurisdictions.

To this end, we recommend that the Secretariat of UNODC prepare an analysis of acts proposed by the various member-states for inclusion in the Convention which exist in

national law worldwide. This would be invaluable to determine how much convergence there is with respect to the proposed crimes - and in how many member-states there is no criminal law at present with respect to some acts proposed for inclusion in the Convention. It should also identify commonalities as well as differences between national approaches. We suggest the same analysis should be done with respect to the other operative elements of the Convention in due course. This will allow all stakeholders to identify what challenges will exist in implementing the Convention into at the national level. This will not only help focus the negotiations, it will also be critical to identify the capacity building and technical assistance essential to ensure the Convention's wide adoption. Finally, these analyses will be particularly valuable alongside the report the Secretariat has recently published, analysing the provisions of existing international instruments addressing cybercrime.

Preamble and General Provisions

We view the Chair's proposal regarding these elements as a good starting place, however we recommend several areas of further elaboration:

- Increased and more specific references to other international legal obligations - particularly with respect to human rights, the protection of which must be an integral obligation of the Convention, not a principle or recommendation limited to the Preamble. Where there is an obligation to comply with other principles of international law, we recommend the specific instruments are referenced, to avoid a situation where different member-states implement the obligations based on different sources of law which could create confusion or allow some states to exclude the source that is most appropriate[1].
- 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

[1] With respect to the centrality of human rights, we support the position of Article 19, in paragraph 2 of its submission.

matters *between* sovereigns. Finally, any references to sovereignty should be limited and take a human-centric approach to avoid negative impacts on fundamental freedoms through law-enforcement obligations that are state-centric.

- The Preamble should contain a strong statement that a key objective of the Convention is to foster healthy socioeconomic development through effective cybercrime prevention and prosecution and to assist developing countries, particularly least developed countries, landlocked developing countries, and small island developing states, as they seek to leverage this Convention to foster sustainable development.[2]
- The Preamble should highlight the benefits of technology generally and that information and communication technologies (ICT) and the Internet are global goods with profound socioeconomic benefits and are foundational to achieving the Sustainable Development Goals. The Convention could therefore be framed as protecting these many benefits for all citizens, while protecting potential victims of cybercrime[3].

We submit the following with respect to definitions and terms to be used in the Convention:

1. Definitions should be finalised after the operative parts of the agreement, to ensure they are tailored to their use, and should be adopted by consensus. This avoids spending time negotiating a definition which is not used or used very differently, forcing it to be revised.
2. Wherever possible, definitions should be taken from other instruments addressing cybercrime, particularly the Budapest Convention and its Protocols. This helps ensure that any provisions in the Convention that use these terms will not create confusion or other unanticipated negative consequences, especially where the operative provisions of this Convention cover similar ground as other agreements already in force.
3. Terms should be used consistently throughout the Convention and should be

[2] We would like to highlight, *inter alia*, Mexico's proposal in this regard on page 2 of their submission.
[3] The submission of GI-TOC on this point, and the contents of the Preamble more generally, is salutary.

specific - avoiding terms such as 'lawful' or 'licit/illicit' - where the meaning can be very different in different jurisdictions.

4. Definitions of data, data subjects, or other terms relevant to these should, wherever possible, be grounded in human-rights-centric[4] language.

The Convention should avoid provisions which override or supersede other instruments, due to the inherent risk of conflicts of laws and of degrading the operation of those instruments.

Provisions on Criminalisation

Taking into account our earlier overarching comments, we have the following additional points to make.

All crimes included should be the subject of consensus, not adopted by vote. This is important to ensure that the Convention is ratified, and implemented, by as many Member-States as possible; it also ensures that the definitions of included crimes will be implemented so that they lend themselves to international cooperation in enforcement. Acts which are not already subject to criminal penalties in, at a minimum, a substantial majority of member-states should not be included in the Convention.

Duplication of offences covered by other conventions simply because those offences leverage ICTs should be avoided, such as corruption, trafficking, terrorism, or drugs. Duplication raises the real risk of conflict of laws in implementation, confusion or contradiction and risks losing focus on a targeted, practical, effective instrument to tackle cybercrime effectively. Similarly, extending this Convention to include acts merely because they are criminalised in other conventions *or* are existing crimes simply because the crime leverages ICTs should also be avoided.

Measures related to online content should be excluded except where there is consensus amongst all negotiating states on the definition of the acts *and* a demonstrable need for

[4] With respect to this point the submission of AccessNow, and its concept of Protected Information, is salutary. Those of the Electronic Frontier Foundation and Privacy International, in their submissions' elements related to avoiding a hierarchical approach to different types of data containing personal information and their treatment, are also salutary.

them to be addressed by this Convention. Cooperation requires a compatible view of offending content as a crime across all jurisdictions where enforcement is needed and this is an area where there is very little convergence on what acts infringe the law, and even less on acts which constitute criminal acts. Acting absent convergence has considerable risks of unintended consequences to states' obligations in other areas of international law, particularly human rights.[5]

Intentionality should be a part of the definition of all acts the Convention addresses, and it should cover only those offences which cause serious harm and involve specific malicious or dishonest intent. This is important for many reasons, particularly the protection of human rights, but in addition at a practical level those engaged in security and vulnerability research should not inadvertently be accused of crimes when performing the valuable defensive services they undertake[6] and that devices (and computer systems) may be 'hijacked' for use in botnets, for example, without the knowledge of the owner of the device.

For cyber-enabled crimes, we can see value in considering inclusion of a limited number of such crimes, if they pass all the following three tests:

1. Each should be carefully and specifically defined. Provisions which simply obligate a Party to ensure that an act is included in their legal code without a meaningful definition of the act in question should be avoided. One of the most important reasons for this is to help ensure that acts to be covered by the Convention have compatible definitions across the parties to it;
2. They should be included only if coverage is necessary to ensure the necessary and proportionate level of cooperation required to address them;
3. Given that we propose that the procedural elements of the convention cover evidence-gathering and related activities for crimes not covered by the Convention directly, crimes should only be included if there is consensus that doing so is necessary to supplement existing legal norms in relation to them, or, where there is no international legal norm, that relying on the procedural elements of this

[5] In these regards, we support the approach of Article19 in its submission in the section "Speech-related offences."
[6] With respect to this point the submission of AccessNow is particularly salutary.

convention will be insufficient for some specific reason.

We further submit that even if a crime passes the above tests, there must also be a consensus for including them.

Procedural Provisions

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.

It is important to recognise that access to data by third parties for law enforcement purposes has significant risks to human rights, as well as data protection and fundamental privacy rights. When requests are made from one jurisdiction to another, those requests must not force any entity to violate the law in any jurisdiction in which they have legal nexus. While we will be providing a future submission to address in more detail the issues around access to data, for the purposes of the present session we recommend the following:

- Requests for data should be narrowly tailored to specific public safety needs and in all cases seek only the data that is necessary and proportionate. The Convention should make clear that requests for 'bulk' data sets are not appropriate; requests related to individuals in particular should specify distinct identifiers. Provisions addressing this should encourage requesting jurisdictions to rely on, whenever possible, existing bilateral or multilateral agreements such as MLATs.
- The Convention should clearly identify the types and categories of data subject to government access and the specific authorities required to fulfil data safety needs.
- The Convention should incorporate safeguards to ensure robust independent oversight and effective redress mechanisms
- It should contain provisions to address conflicts of law and mechanisms to resolve such conflicts that will inevitably arise.
- It should allow the custodian or owner of any data to challenge a request on behalf

of the data subjects to ensure the request is within the law and respects the rights of the custodian or owner *and* the data subjects themselves. Information and technology providers must not become extensions of public authorities through general mandates for cooperation with law enforcement that impact normal operations of and access to data held by them.

- The Convention should not create liability for providers due to requirements that they engage in activities that would negatively impact the data protection, privacy or other human rights of natural persons who are their customers.[7]
- Data acquired by authorities through operation of the Convention should be subject to strict data minimisation, retention, and dissemination limits and impose custodial obligations on the public entities that will hold any data provided.
- Legally binding remedies should be available to data subjects in the event of a breach by the government of the access, use and retention rules. Effective redress should be conducted by independent bodies such as courts or other impartial entities. These institutions may require correction or deletion of data, or award compensation for damages. If the information obtained through obliged access is later used in a criminal prosecution, those being prosecuted should have the right to obtain and challenge it. This notification right may be limited or deferred (for a limited period of time), "due to legitimate government need to protect the lives and integrity of national persons or national security or law enforcement information and investigations."
- The Convention should recognise that immediate/real-time access to data of any kind will not always be technically possible, and that data retention requirements of custodians or owners of data mean that they cannot practically retain many types of data for long periods - and they may be legally prevented from doing so even when it is technically possible. In addition depending on the circumstances retention can have broader human rights or conflict of laws issues - for example, where data relates to a postal code and of necessity therefore brings in data

[7] In this respect we agree with Article 19's submission, Procedural and Investigative Measures, paragraphs 8 and 9.

associated with far more persons than those an investigation is concerned with, retention rules would have to take account of the necessity of purging all the data that isn't actually required for the purpose at hand. For these and other reasons, we see significant issues with the proposals that have been submitted related to data requests and retention. Finally, we recommend a specific maximum limit, as the Budapest Convention so provides, for any data related to the operations of the Convention.

- The Convention should explicitly recognise that the public has a right to know how governments may access their information and under what circumstances third parties that hold their data may be obliged to provide it to public authorities. Therefore the Convention should obligate parties to publish the relevant statutes and related policies for public access - and it should also provide natural persons with a mechanism by which to know if their data has been disclosed - accepting that confidentiality must be maintained — for example, in instances where notifice would result in an interference to an ongoing investigation, a suspect's flight from prosecution, or witness tampering.. However, the reasons for delayed notice must be narrowly tailored to the facts at hand, and such delay cannot be indefinite in nature.
- With respect to all these measures, respect for human rights and fundamental freedoms must be integral and clearly delineated throughout as contextually relevant. This is especially important for personal information, extradition, and any seizure of property.

Leveraging procedural elements to facilitate crime prevention for crimes where ICTs are used in their commission

It is worth considering how procedural provisions could extend to facilitating transboundary cooperation for, *inter alia*, evidence-gathering associated with otherwise non cyber-dependent or cyber-enabled crimes, where for example ICTs have been used to communicate about the commission of otherwise entirely kinetic criminal acts.

It is also worth considering a straightforward link to the procedural provisions of UNTOC, allowing parties to this Convention to utilise UNTOC's provisions related to

investigative activities, evidence gathering and preservation of electronic evidence.

We submit that explicitly referencing crimes related to the online sexual exploitation of minors and trafficking in natural persons in connection with both the above two points would be a better approach to addressing these crimes than adding them to the list of crimes the Convention covers. To do otherwise risks overlapping obligations with existing agreements or creating provisions that could have unanticipated negative consequences for efforts to address these particularly loathsome crimes due to potential conflict of laws or confusion.

In addition to our earlier point on the same subject more generally the Convention should not establish liability for third parties. There are several reasons for this, the most significant being that the subject is very complex and in national legislation is far from limited to criminal law. It would be easy 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.

We recommend that the Convention explicitly protect whistleblowers, journalists, victims and witnesses in this section, reiterating and building upon the relevant provisions of UNTOC, particularly Articles 24 and 25.[8]

In closing we would like to once again thank the AHC Secretariat, the Chair and vice-chairs, and the Member-states for this opportunity to provide our comments to the AHC process. We are pleased to accept comments or queries at cyber@iccwbo.uk or by post to our UN Office.

[8] We note the congruent comments of GI-TOC in their submission, 3(4), in this regard.