# Considerations on the Revised Draft of the Convention on Cybercrime

## Introduction

In our increasingly interconnected world, cybercrime stands as a pervasive and highly sophisticated threat that effortlessly 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, concerns within the global private sector have heightened that beyond operational deficits, the Convention's provisions may be misused to compromise cybersecurity, data privacy, and online rights and freedoms.

As the AHC prepares for its final meeting, there is a small, but crucial window to recalibrate and realign with the initial vision of crafting a targeted and effective cybercrime instrument.

Having contributed to the work of the Ad-Hoc Committee since its inception, the International Chamber of Commerce appreciates the opportunity to offer the following comments on the updated Consolidated Negotiating Document (CND). We reiterate our comments made in previous submissions in the hope of contributing to a Convention that cultivates a more predictable business environment, streamlining the complexities associated with cyber incidents that traverse national borders.

Our aspiration is for the Convention to strike a delicate balance: robust cybercrime prevention, detection, and prosecution coexisting harmoniously with the protection of data, privacy, and human rights.

## 1. Define the scope of the convention clearly and narrowly

The core objective of the Convention should be to **enable, increase and strengthen international cooperation to reduce the incidence of serious cyber-dependent criminal activity**. This objective can only be reached if the Convention's provisions focus on criminal acts that are similarly defined across jurisdictions, while avoiding overly prescriptive provisions that may lead to conflicting rules and barriers to cooperation. The scope of the Convention should be narrowly defined and **focus on cyber-dependent serious criminal offences**, as discussed in point 2. below on criminalization.

- We are generally supportive of the statement of purpose as expressed in *Article 1*, and recommend strengthening this text to clearly and narrowly define the scope of the Convention, making clear already in *Article 1* that it is serious crimes that are its main focus.
- We strongly recommend clarifying in *Article 3* that the scope of application of the treaty pertains to cyber-dependent serious crimes.
- Relatedly, we recommend keeping the preamble also narrowly focused and deleting the second part of *Preambular paragraph 3* that reads *"including offences related to terrorism, trafficking in persons, smuggling of migrants, illicit manufacturing of and trafficking in firearms, their parts, components and ammunition, drug trafficking and trafficking in cultural property."*

We strongly believe that the **scope of application of all procedural measures needs to be exclusively limited to crimes set forth in the Convention**. We would in particular recommend that the section on procedural measures refers to specific articles in the criminalization section and advise against including general references to *"ICT crimes"* or *"any other crimes."*

- We advise to delete *Article 23, paragraph 2 (b)* as this paragraph, as currently phrased, runs the risk of expanding the applicability of procedural measures to any and all offences conducted with the use of ICTs.
- Similarly, we propose in *Article 23 paragraph 2 (c)* referring to *"The collection of evidence in electronic form of criminal offences established in accordance with this Convention"* instead of "*any criminal offence*".

**Provisions on international cooperation, should also apply to precisely and narrowly defined set of serious, cyber-dependent crimes**.

- We recommend in *Article 35* referring to *"offences established in accordance with articles 6 to 10 of this Convention"* or *"cyber-dependent serious crimes"* and deleting the reference to other crimes, including references to *Article 17*.
- In the same vein, we recommend keeping the scope of *Article 47* on law enforcement cooperation equally precisely and narrowly defined and recommend deleting the last sentence of *Article 47 (1) (a)* that reads *"including, if the States Parties concerned deem it appropriate, links with other criminal activities."* Keeping the language in its current form risks expanding the scope of the provision to any criminal activity.

As acts of cybercrime, more often than not, cross national borders international cooperation is at the core of effective prosecution. Provisions on procedural measures should aim to enable such

cooperation. Therefore, **dual criminality must be the starting place for international cooperation on cybercrime**.

- We recommend tightening the language in Article 35 paragraph 2 to:
  *In matters of international cooperation, dual criminality shall be considered a necessary requirement, and shall be deemed fulfilled if the conduct for which assistance is sought is a serious criminal offence under the laws of the cooperating States Parties set forth within this Convention.*

In the same vein, the Convention should **build on commonalities across jurisdictions**. The scope of the agreement's measures should focus on widely understood criminal acts which have common, clear, and compatible definitions in many different legal jurisdictions. This is fundamental as many elements of cross-border crime cooperation are greatly limited or rendered ineffective if the acts are not similarly understood in all concerned jurisdictions. Focusing on elements that are defined and understood similarly not only facilitates consensus in discussions and incentivizes cooperation, but also helps ensure that the Convention is implementable. The Convention should **avoid overly prescriptive provisions and establishing conflicting rules that raise barriers to international criminal cooperation**. There is significant risk of conflicting national rules which not only represent substantial compliance costs, but risk rendering the implementation of the Convention ineffective. The Convention should strive towards maximum flexibility and creating the least risk of conflict. The Convention should **not contain any provisions that could potentially give rise to jurisdictional disputes** and should **not open the door to expansive claims of extraterritorial jurisdiction** by establishing jurisdiction over a crime committed in one country due to services being offered elsewhere. To that end, we recommend to:

- delete *Article 22, paragraph 2 except for subparagraph (b)* which should be moved to *Article 22 paragraph 1* and renamed as *Article 22 (1) (c);*
- delete *Article 27, paragraph 1 (b),* that refers to production orders in Chapter IV on Procedural measures and law enforcement; and
- in *Article 45, paragraph 1*, delete *"or where the data are in the possession or control of a service provider located or established in their territory"*.

## 2. Criminalize cyber-dependent serious offences only

As noted above, we see the objective of this Convention to enable, increase and strengthen international cooperation to reduce the incidence, especially, of serious cyber-dependent criminal activity and to protect the victims of such crimes. As discussed, to be effective in achieving this objective, the Convention, which is being set forth as a criminal law instrument, must focus narrowly on cyber-dependent serious criminal offences, and align all chapters of the Convention to apply to offences set forth in this Convention. Therefore, we recommend for the Convention to:

- **address the intentional development, spread, and use of malicious computer code** to attack government systems, critical infrastructures or ICT supply chains, **as well as the distribution, sale or offering for sale of hardware, software or other criminal tools used to commit cybercrime**, as expressed in *Article 10*.

- **do not treat traditional crimes as cybercrime** merely because a computer was involved in the planning or execution of the crime, and **do not attempt to regulate content**. This will help streamline the processes and procedures related to transboundary enforcement, as well as raise the prospect of reaching consensus between states which, consequently, could increase the number of signatories to the Convention.
- **do not contain provisions on offences covered by other conventions**, simply because those offences leverage ICT as this would create unnecessary duplication that can lead to conflict of laws in implementation, confusion, or contradiction and risks losing focus on a targeted, practical, effective instrument to tackle cybercrime effectively. Therefore, we recommend removing *Article 17*.
- **include illegal activity that is cyber enabled, only if the offenses are of the scale, scope, or speed that they would not be feasible without ICTs**.

We support the use of the term **"cybercrime"** over "use of information and communications technologies for criminal purposes" throughout the Convention. For the purposes of this Convention, the term "cybercrime" can be used in a self-defining way, under which we understand the crimes covered by the criminalization section, as discussed above.

In addition to the definition of cybercrime, **all terms and provisions used throughout the Convention should be aligned with established and agreed upon definitions**, particularly those included in the Budapest Convention, as one of the most widely referenced statutes in this area. Definitions must strive to be as precise as possible, they should remain **technology neutral** and **flexible** enough to ensure the Convention is future-proof and adaptable to the rapid development of technology.

The Convention should use precise terminology and clearly defined terms and **avoid the unqualified use of terms and overly broad and vague definitions**, such as *Article 12 (c)*.

## 3. Make human rights protection and safeguards a core commitment of the Convention

To ensure effective cooperation, a narrow scope must be paired with robust safeguards to protect freedom of expression, access to information, and privacy. Safeguards are also necessary to ensure independent oversight and redress mechanisms, minimize and avoid conflicts with existing laws, create mechanisms to prevent conflicts, and resolve disputes that might arise.

If national frameworks can develop in harmony to address cybercrimes in domestic context, then this will also help to create the foundation for effective international cooperation. Failing that, the Convention could run the risk of undermining and fracturing existing efforts to fight cybercrime and could also produce unintended negative consequences for legitimate commercial and non-commercial activity of all kinds and gravely impact human rights.

The intrinsic tension between effective investigation by law enforcement and the protection of fundamental human rights needs to be legally addressed and asserted through safeguards. Therefore, we would particularly like to highlight the importance of a **strong and clear commitment in the Convention to human rights and safeguards**.

The protection of human rights should be clearly factored in at every step of the process of cooperation on cybercrime, including the protection of freedom of expression, access to information and privacy in line with the principles of proportionality and necessity. This includes **compliance with both domestic and international legal obligations regarding the personal data protection when transmitting personal data**.

A **stand-alone article in the general provisions** section is necessary to provide an umbrella provision that establishes the core principles under which all procedural rules and powers are to be applied, such as *Article 5*.

Subsequent provisions of this Convention should not give ground to misinterpretation that might serve to limit fundamental human rights and freedoms, such as the right to freedom of speech, the right to privacy or gender equality.

**The protection of fundamental human rights needs to be equally considered when developing procedural measures**. Provisions on procedural measures must underline that fundamental human rights and freedoms should be equally ensured both offline and online and across national borders and legal systems. Human rights and rule of law benchmarks can limit the use (or abuse) of procedural powers and foster closer integration of telecommunication operations between countries with different types of governance structures – and as such, create predictable legal frameworks for private parties operating in different types of jurisdictions.

Therefore, we support the inclusion of *Article 24*.

## 4. Limit access to data to what is necessary and proportionate to law enforcement needs

Access to data for crime prevention and law enforcement purposes is extremely complex. Without appropriate consideration to these complexities, unchecked access presents considerable risks of misuse or unanticipated negative consequences. To protect rights of end-users, the purpose and reach of government access to data needs to be narrowly tailored. Therefore, related to *Articles 25 to 28* we recommend, that the Convention, at the minimum:

- clearly identifies the types and categories of data subject to government access;
- requires strict and transparent data minimization, retention, and dissemination limit of ninety days; and
- does not negatively impact data protection, privacy, freedom of expression or other human rights.

In this respect, we recommend referring to the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, adopted in December 2022, that seeks to clarify how national security and law enforcement agencies can access personal data under existing legal frameworks.

Relatedly, the Convention should:

- 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 – therefore we advise that the
- allow technology providers an opportunity to challenge government 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. The Convention should also include the right to redress for any individual whose rights were violated through the exercise of powers set forth in this Convention.

In addition, with regards to *Articles 29 and 30*, and references thereto in preceding and subsequent paragraphs, we would like to reiterate our previous position that **real-time collection of traffic data and interception of content data is considered in some jurisdictions as significant invasion of privacy, and in contradiction to the principles of necessity and proportionality of data collection.**

- We recommend removing *Articles 29 and 30* and related references, such as *Article 40 paragraph (3), subparagraphs (e) and (f)*.
- When it comes to mutual legal assistance, in particular on matters of data access and sharing as noted in *Article 45*, we recommend that the text of the Convention includes some principles and provisions to ensure clarity and predictability in government access to digital information.

Furthermore, as currently worded and without due process safeguards, *Article 28 paragraph (4)* runs the risk of enabling the prosecution or coercion of a company employee to provide assistance in subverting technical access controls without the knowledge of the service provider. This would not only expose the individual, but might undermine cybersecurity of ICT products and services more broadly.

- We recommend removing *Article 28 paragraph (4)*.

## 5. Do not create liability for third parties

We commend the commitment expressed throughout the CND for cooperation with all stakeholders, including the private sector, be that in preventing, detecting or combatting cybercrime.

This being said, the Convention **should not attempt to increase cyber resilience through industry regulation or by imposing standards or principles of behaviour** but should rather focus on enabling and empowering public authorities to prevent, investigate, and prosecute cybercrime. Other means of regulating industry exist, and these should not be conflated with cybercrime policy through being included in this Convention. States have focused on developing frameworks and legislative approaches aimed at increasing the cybersecurity and cyber resilience of the online environment in non-criminal contexts and this separation should remain.

As a default, the Convention should **not create liability for third parties**, but encourage and permit the production of timely mitigation measures in case of detection of vulnerabilities. Definitions of third party liability differ across jurisdictions and disturbing these arrangements through international obligations in one area is very likely to lead to unanticipated negative consequences in other areas.