Considerations on the Draft Text of a Convention on Cybercrime

Contents

Introduction 1

1. Preamble 2
2. General Provisions (Art. 1-5) 2
3. Criminalization (Art. 6-21) 3
4. Jurisdiction (Art. 22) 5
5. Procedural measures and law enforcement (Art. 23-34) 5
6. International cooperation (Art. 35-52) 6
7. Preventive measures (Art. 53) 8
8. Technical assistance and information exchange (Art. 54-56) 9
9. Mechanisms of implementation (Art. 57-58) 9

Introduction

Acts of cybercrime cross borders more often than not. Therefore, international cooperation is at the core of effective prosecution. This kind of cooperation requires that the offences are commonly understood and clearly recognised by all parties involved. Building a comprehensive and robust international framework that will define the scope, set the objectives, and describe the mechanisms of this cooperation is essential. An international framework 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.

Having contributed to the work of the Ad-Hoc Committee since its inception, ICC appreciates the opportunity to offer the following comments on the updated Consolidated Negotiating Document (CND).

Overall, we believe that the updated CND is a comprehensive and balanced summary of the Committee's deliberations thus far. We are greatly encouraged to see that the CND focuses on areas of consensus and broad support and that the language conveys the importance of further strengthening cooperation among States and between States and non-governmental

stakeholders. We are also encouraged to see that the draft reflects much of the input provided by non-governmental stakeholders, as expressed during both plenary and intersessional multistakeholder meetings. The structure of the CND is clear and easy to follow, our comments in this document follow that structure.

1. Preamble

We believe that this section of the CND properly contextualizes the transnational threat of cybercrime and therefore the pressing need for effective international cooperation.

We particularly welcome the recognition in the Preamble of the fundamental role of the private sector and other non-governmental stakeholders to support such collaboration. *(Preambular paragraph 9)*.

We further commend the Ad Hoc Committee on the consideration of gender perspectives in its discussions and wholeheartedly support the recognition in the Preamble of mainstreaming a gender perspective. *(Preambular Paragraph 10)*

The scope of the Convention should be narrowly defined and focus on cyber-dependent serious criminal offences, as discussed later in the criminalization chapter. We therefore recommend keeping the preamble also focused on such matters and deleting the second part of Preambular paragraph 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."*

2. General Provisions (Art. 1-5)

Scope

We support the statement of purpose as expressed in *Article 1*, and we see the scope of the Convention in particular to **increase effective international cooperation between national law enforcement and prosecutorial agencies to reduce the incidence of major cyber-dependent criminal activity** as the priority, as well as to **protect the victims of such crimes**.

For that reason, we recommend clearly and narrowly defining the scope of the Convention, making clear in *Article 1* that it is serious crimes that are its main focus.

Use of terms

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, that we discuss in the next section.

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** such as "wrongful" and "lawful." This would also include criminalising serious cybercrime offences where "**clear criminal intent**" can be established, rather than relying on terms such as "dishonesty" and "illegitimacy," which can carry various meanings across different jurisdictions and are used to refer to activity that is illegal, but not necessarily criminal.

Similarly, we would recommend for the Convention to **use precise terms** such as "unauthorised access," "computer data" rather than broad terms such as "avoiding security measures" and "access to information."

Human rights

The Convention should **include appropriate safeguards** to ensure robust independent oversight and effective redress mechanisms, minimize and avoid conflicts with existing laws, create mechanisms to prevent conflicts, and resolve disputes that 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.

3. Criminalization (Art. 6-21)

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. To achieve this objective, the **scope of the Convention must be clearly and narrowly defined and include appropriate safeguards** to ensure robust independent oversight and redress mechanisms, minimize and avoid conflicts with existing laws, create mechanisms to prevent conflicts, and resolve disputes that might arise.

In this spirit, we would like to offer the following suggestions, with regards to criminalization:

- We caution against unnecessarily expanding the scope of the Convention, which is being set forth as a criminal law instrument. Measures outlined in this chapter should be focused on **cyber-dependent serious criminal offences**, and language in subsequent chapters to refer to *"offences set forth in this Convention."*
- We highlight in particular the importance 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*.
- The Convention **should not treat traditional crimes as cybercrime** merely because a computer was involved in the planning or execution of the crime, and it should not attempt to regulate content. We appreciate the efforts made to tighten the text in this respect. 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.
- The Convention should **include illegal activity that is cyber dependent, only if the offenses are of the scale, scope, or speed that they would not be feasible without ICTs**.
- The Convention should **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*.
- Across all these dimensions, **dual criminality must be the starting place for international cooperation on cybercrime**. Experience shows that transboundary crime cooperation is much more likely to be effective if all jurisdictions recognise the act as criminal. Focusing on elements that are defined and understood similarly not only facilitates consensus in our discussions, but also helps ensure the implementability of the Convention and incentivizes cooperation. Therefore, the text of the Convention should require dual criminality in all instances and ensure offences are seen as the same or similar category of a crime.
- 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.
- In particular, the Convention should **not seek to increase cyber resilience through the introduction of industry regulation.** Other means of regulating industry exist, and these should not be conflated with cybercrime policy through being included in this Convention.

4. Jurisdiction (Art. 22)

The Convention should **not contain any provisions that could potentially give rise to jurisdictional disputes** but should instead focus on facilitating cooperation.

Therefore, we recommend deleting *Article 22, paragraph 2 except for subparagraph (b)* which we recommend moving to *Article 22 paragraph 1* and renaming it as *Article 22 (1) (c)*.

In the same vein, we recommend, in Article 22, paragraph 5 to refer to *"determining the most appropriate jurisdiction for prosecution"* rather than *"coordinating their actions"*, on the model of the Budapest Convention

We furthermore advise that the Convention **does 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 deleting *Article 27, paragraph 1 (b),* that refers to production orders in Chapter IV on Procedural measures and law enforcement.

5. Procedural measures and law enforcement (Art. 23-34)

Existing international conventions on cybercrime can provide valuable inspiration for a relevant framework on procedural measures.

Scope

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**.

In the same vein, and to safeguard end-users against potential abuse of executive authority, 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 *"offences set forth in this Convention"* instead of *"any criminal offence."*

Conditions and safeguards

As mentioned above, 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**. 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* in this chapter.

Considerations on data

The issues around access to **data for crime prevention and law enforcement purposes** are extremely complex and as a result present considerable risks of unanticipated negative consequences. To protect rights of end-users, purpose and reach of government access to data needs to be narrowly tailored. Here, I would like to mention a couple of general considerations on *Articles 25 to 28:*

- The Convention should clearly identify the types and categories of data subject to government access.
- The Convention should require strict and transparent data minimization, retention, and dissemination limit of ninety days.
- The Convention should 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;
- 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 position expressed in previous meetings 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.

6. International cooperation (Art. 35-52)

As previously expressed, ICC sees the primary scope of this Convention to enable, increase and strengthen international cooperation to reduce the incidence of major cyber-dependent criminal activity in particular, and to protect the victims of such crimes. Therefore, we see this chapter as the core of the Convention.

Finding common ground on procedural issues to allow for expedited and efficient investigations should be the priority of this Convention. However, the rules on coordination and cooperation must be carefully crafted as parties will need to maintain sovereignty when, for example, they are asked to hand over data or extradite persons charged for cybercrimes conducted in another party's territory. To this end, we recommend:

- Provisions of the Convention on international cooperation, just as provisions in other chapters, should **apply to precisely and narrowly defined set of serious, cyber-dependent crimes**, as discussed in the criminalization section. Therefore, we recommend in *Article 35* referring to *"offences established in accordance with the Convention"* and deleting the reference to other crimes.

  In the same vein, we recommend keeping the scope of *Article 47* on law enforcement cooperation equally precisely and narrowly defined to pertain to offences established in accordance with the Convention 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 noted above, **dual criminality must be the starting place for international cooperation on cybercrime**. Therefore, we recommend tightening the language in *Article 35 paragraph 2* to *"In matters of international cooperation, dual criminality shall be considered a requirement"*, instead of *"whenever dual criminality is considered a requirement."*

  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**. Given the global nature of data flows, there is significant risk of conflicting national rules which represent substantial compliance costs. The Convention should strive towards maximum flexibility and creating the least risk of conflict.

- When it comes to **mutual legal assistance**, in particular on matters of data access and sharing, we recommend that the text of the Convention includes some principles and provisions to ensure clarity and predictability in government access to digital information. As noted above, the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities offers a useful baseline.
- We advise that the Convention embrace **transparency** as the general rule of thumb, taking into account that except in narrow circumstances, the public has a right to know how, when, and why governments seek access to their data.

- Furthermore, we wish to reiterate our earlier comments that real-time collection of traffic data and interception of content data is considered in some jurisdictions as significant invasion of privacy and recommend removing references to such practices in *Article 40 paragraph (3), subparagraphs (e) and (f)*.

We would particularly like to highlight the importance of a **strong and clear commitment in the Convention to human rights and safeguards.** The powers and procedures described in this chapter should particularly be subject to conditions 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**.

We would like to commend that the draft already **builds on existing international agreements** like UNCAC and UNTOC. We urge member states when considering these articles to continue to ensure compatibility with existing international obligations, to avoid unintended negative consequences from overlapping or conflicting provisions and build on the lessons learned from existing mechanisms, such as the Budapest Convention.

7. Preventive measures (Art. 53)

In the face of continuously growing cyber threats, enforcement itself is not a complete solution: prevention is also key. Prevention efforts can help equip populations with capabilities to defend against risks, they can reduce harm by neutralizing cybercrime attempts and dismantling vulnerabilities before perpetrators succeed in committing offences, and they can also help deter perpetrators from malicious conduct. Strong international government cooperation, public-private voluntary collaboration, and deterrence measures against cyber criminals are an imperative.

In this respect, we welcome the recognition in *Article 53, paragraph 3 (a)* of the role of **multistakeholder cooperation.** Partnerships are fundamental to successfully prevent cyber threats given the prominent role that the private sector, CERTs and non-governmental organizations play in the digital arena. Collaborating with the various actors in the global ecosystem of cybersecurity is of paramount importance to successfully prevent and disrupt cybercrime.

Governments can benefit from the expertise and resources of the private sector in the fight against cybercrime. Opportunities include working with industry to share information with enforcement officials about new and emerging threats that technology suppliers experience real-time and that their customers see as priorities.

Governments often lack sufficient resources to deal effectively with cybercrime. Working with the private sector can help them achieve greater success, which will help drive trust on both sides, as well as trust of citizens and users in digital technologies overall.

Collaboration with non-governmental stakeholders can raise public awareness about the threats of cybercrime; ensure the work of governments is undertaken in a transparent manner; and ensure high standards for safeguards such as privacy, civil liberties, and human rights.

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. 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.

8. Technical assistance and information exchange (Art. 54-56)

Countries are at vastly diverse levels of readiness when it comes to cybercrime prevention, detection, investigation, and prosecution. Success in these dimensions depends on a complex mix of technical, technological, judicial, and administrative capabilities and on the constant updating of these capabilities given the pace at which criminal tactics are evolving in the cyber domain.

Therefore, we see it particularly useful that the Convention includes provisions that support **training programs** as well as technical assistance. When finalizing these provisions, we recommend ensuring that:

1. Provisions on technical assistance are **not overly prescriptive**, they remain **technology neutral**, and are **offered on a voluntary basis** with any **transfer of technology carried out on mutually agreed terms**. In the same vein, provisions should allow for the necessary flexibility to adapt to the ever-changing landscape of cyber threats, as well as to allow for assistance to be tailored to the needs of the requesting country.
2. Provisions are framed in accordance with **international human rights laws**, in particular privacy rights, freedom of expression, as well as relevant data protection laws.

Last, but not least, the Convention should recognize and **promote the experience and insight of all stakeholders**. For example, businesses and technical community experts provide invaluable expertise based on which policy guidelines and instruments can be developed to ensure they are commercially and technically feasible. Multistakeholder forums can act as a resource for states, coordinating regional and global cyber capacity projects and initiatives, sharing knowledge and expertise by recommending tools and publications.

9. Mechanisms of implementation (Art. 57-58)

We welcome the creation of a standing body, such as a Conference of the Parties, to oversee the operation and effectiveness of the Convention. We also welcome the Secretariat of the Conference of the Parties to be set up under the UNODC.

We appreciate that this section, as well as previous ones, recognizes the need for cooperation with the private sector and other non-governmental stakeholders. We feel that this could be further strengthened.

Given the role the technology industry has in this space, the Convention should **ensure the meaningful participation of the private sector in meetings of the Conference of the Parties**. Previous experience from similar bodies has shown the value of public-private cooperation in this area. Such cooperation would be especially valuable to parties who have less experience with transboundary cybercrime cooperation and would help all parties to work with concerned third

parties on the complexities of data access and other requests, as well as the conflict of laws situations that will inevitably arise.

The rules of procedure of this Ad-Hoc Committee in working with and creating meaningful opportunities for participation of stakeholders is truly exemplary and has quickly risen to be regarded as the gold standard for participation across current UN processes. This approach should be preserved for the implementing body, and we recommend **including in the text of the Convention a clear reference to enabling the meaningful participation of stakeholders**. We suggest in this respect using the same language as *operative paragraph 9 of General Assembly resolution 75/282*, that has enabled the effective work of this Committee.