GPD Response to Ad Hoc Committee Consolidated Negotiating Document

Global Partners Digital submission
December 2022

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

We welcome the opportunity to provide comments on the "Consolidated negotiating document on the general provisions and the provisions on criminalisation and on procedural measures and law enforcement".

While GPD is not convinced of the necessity of a global cybercrime convention, we advocate for a treaty that respects, protects and promotes human rights. We appreciate the work undertaken by the Committee Chair to prepare this negotiating document. However, we believe that the consolidated text poses clear risks to human rights, particularly freedom of expression and privacy.

Please see below for our comments and suggestions on the consolidated text.

Chapter I: General Provisions

We are concerned about the broad scope of application provided under Article 3(1), which has the potential to capture an overly broad range of criminal offences, and would extend procedural provisions to a wide range of criminal activity. This poses risks to human rights and may result in implementation that is otherwise inconsistent with states obligations under international human rights law. We therefore recommend that the scope of application be narrowed to solely cover "the prevention, detection, investigation and prosecution of core cybercrimes".

We are also concerned about the inclusion of Article 3(3), which provides that "For the purposes of this Convention, it shall not be necessary, except as otherwise stated

herein, for the offences set forth in it to result in damage or harm to persons, including legal persons, property and the State". This provision risks capturing activity that is beneficial to the public or done without malicious intent, including acts that are undertaken by security researchers. We recommend that it be deleted.

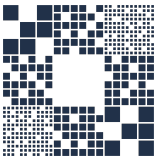
We are pleased with the inclusion of Article 5 on respect for human rights as it provides that "State Parties shall ensure that the implementation of their obligations under the Convention is in accordance with applicable international human rights law." But we believe that this Article 5(1) could still be strengthened by mentioning specific international legal instruments. For example, "State Parties shall ensure that the implementation of their obligations under the Convention is in accordance with applicable international human rights law as set forth in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and other international human rights instruments and standards".

We further recommend that Article 5 provide additional detail on the right to freedom of expression, explicitly providing that restrictions must be defined in law, satisfy a legitimate aim, and be necessary and proportionate. The same should be done for the right to privacy, which prohibits arbitrary or unlawful interference with a person's privacy, family, home or correspondence. The benefit in providing these references within the general provisions is that it reinforces their protective value and application as applying throughout the convention. But these references must be complemented by more specific protections for human rights, including safeguards and limitations, within all relevant chapters of the consolidated text.

Chapter II: Criminalisation

We are very concerned with the scope of criminal offences provided for in Chapter II of the consolidated text. Many are drafted with vague or overbroad language, and thus fail to comply with permissible restrictions under international human rights law. The scope of criminal offences should be narrow, precise and specific. It should be restricted to core cybercrimes–criminal offences in which information and communications technology (ICT) systems are the direct objects, as well as instruments, of the crimes; these crimes could not exist at all without the ICT systems. A useful reference for the types of crimes that are inherently ICT crimes can be found in Articles 2-6 of the Budapest Convention.

We therefore recommend including only those offences listed in Cluster 1 of the consolidated text. These offences (Articles 6-10) reflect core cybercrimes and would ensure a narrow approach to criminalisation, but they should still be subject to changes in order to mitigate risks to human rights. We are concerned that Articles 6 and 10 may capture the legitimate activities of journalists, whistleblowers and



security researchers. We recommend that these articles include a standard of malicious/fraudulent intent and harm, or provide a more clearly articulated and expansive public interest defence.

We are concerned with the wide range of offences included in Clusters 2-10, including offences where ICT systems are simply a tool that is sometimes used in the commission of an offence. Just because a crime might involve the use of technology does not mean that it needs to be included in the convention. We recommend that these offences, such as those relating to arms trafficking (Article 31) and money-laundering (Article 33) be removed from the consolidated text. Should non-core cybercrimes be included, we recommend that those "cyber-enabled" crimes reflect international consensus, and be narrowly defined and strictly consistent with international human rights standards.

We are also very particularly concerned with various content-related offences provided within the consolidated text, including those in Clusters 4, 7, 8 and 9. These offences are vaguely worded, overbroad and may be used to prohibit legitimate expression. We have seen national cybercrime laws with similar provisions used to silence human rights defenders, journalists and others that disseminate critical expression online. We recommend that these types of offences be removed because of the risks they pose to free expression, for example, extremism-related offences (Article 27) and terrorism-related offences (Article 28).

Chapter III: Procedural Measures and Law Enforcement

We are concerned with the scope of procedural measures as set out in Article 41, which provides that investigative powers may apply to "(a) criminal offences established in accordance with this Convention; (b) Other criminal offences committed by means of a [computer system][an information and communications technology system/device]". We recommend that these powers and procedures not apply to other criminal offences and instead apply only to core cybercrimes. This will help ensure that investigatory powers are only used with respect to crimes that are consistent with international human rights standards.

We are pleased that Article 42 provides that the establishment, implementation and application of investigative powers "are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights and fundamental freedoms arising from its obligations under applicable international human rights law, and which shall incorporate the principles of proportionality, necessity and legality and the protection of privacy and personal data". However, we recommend that this article provide additional detail on particular conditions and safeguards. For example:

- Article 42(2) should require prior independent (preferably judicial) authorization of surveillance measures and ex post independent monitoring;
- Article 42(2) should specify that requests for authorization must be made by an individual of a specified rank within a competent authority;
- Article 42 should provide an explicit guarantee of the right to an effective remedy, which provides individuals with the means and mechanisms to challenge measures that impact their privacy;
- Article 42 should provide a clear guarantee that investigative powers may not be used in ways that compromise the security of digital communications and services, as well as restricting government hacking of end devices.

We believe that the expedited preservation of stored computer data (Article 43) and expedited preservation and partial disclosure of traffic data (Article 44) would both benefit from an explicit requirement of reasonable belief or suspicion that a criminal offence has or is being committed and that the data sought to be preserved will yield evidence of that offence. We further recommend that interception of content data (Article 48) is only conducted when there is a reasonable belief that a criminal offence was committed or is being committed. These more detailed grounds for authorization will help to mitigate risks to individuals' right to privacy.

We are concerned with the language provided in Article 46(4) and the potential for obligations imposed on third parties. It is unclear whether it empowers authorities to demand that an individual would be able to order a person to disclose vulnerabilities or access to encrypted communications. Procedural and investigative tools included in the convention should not directly or indirectly undermine or weaken privacy-enhancing technologies, such as encryption (including end-to-end encryption) or anonymity, as these are considered essential for cybersecurity and the enjoyment of freedom of expression online, particularly for vulnerable and marginalised groups, journalists and human rights defenders. We therefore recommend that this provision either clearly provide protections against such interferences or be removed.

We are concerned that the current wording of Article 47 on the real-time collection of traffic data could facilitate indiscriminate data retention measures, which does not align with the principles of necessity and proportionality. We therefore recommend that Article 47 be modified to explicitly limit any blanket or indiscriminate data retention measures.

Summary of recommendations on CND

We recommend that:

Chapter I: General provisions:

- The scope of application under Article 3(1) be narrowed to solely cover "the prevention, detection, investigation and prosecution of core cybercrimes".
- Article 3(3) be deleted to avoid capturing activity that is beneficial to the public or done without malicious intent.
- Article 5(1) be strengthened by mentioning specific international legal instruments.
- Article 5 as well as all relevant chapters of the consolidated text integrate human rights safeguards, and specifically the requirement that restrictions to the right to freedom of expression and the right to privacy be defined in law, satisfy a legitimate aim, and be necessary and proportionate.

Chapter II: Criminalisation:

- The scope of criminal offences be restricted to core cybercrimes–criminal offences in which information and communications technology (ICT) systems are the direct objects, as well as instruments, of the crimes–including only those offences listed in Cluster 1 of the consolidated text.
- Articles 6 and 10 be amended to include a standard of malicious/ fraudulent intent and harm, or provide a more clearly articulated and expansive public interest defence.
- Should further offences be included beyond core cybercrimes, these must reflect international consensus and should be narrowly defined and strictly consistent with international human rights standards.
- Content-related offences, including those in Clusters 4, 7, 8 and 9, be removed.

Chapter III: Procedural Measures and Law Enforcement:

- The scope of procedures be changed to apply only to core cybercrimes.
- Article 42 be adapted to integrate particular conditions and human rights safeguards. For example, we recommend:
    - Requiring prior independent (preferably judicial) authorization of surveillance measures and ex post independent monitoring.
    - Specifying that requests for authorization be made by an individual of a specified rank within a competent authority.
    - Providing an explicit guarantee of the right to an effective remedy.
    - Including a clear guarantee that investigative powers may not be used in ways that compromise the security of digital communications and services, as well as restricting government hacking of end devices.

- Articles relating to the expedited preservation of stored computer data (Article 43) and expedited preservation and partial disclosure of traffic data (Article 44) be amended to contain an explicit requirement of reasonable belief or suspicion that a criminal offence has been or is being committed and that the data sought to be preserved will yield evidence of that offence.
- Article 48 is changed to require that the interception of content data is only conducted when there is a reasonable belief that a criminal offence was committed or is being committed.
- The language in Article 46(4) relating to the potential for obligations imposed on third parties either be amended to clearly provide protections against interferences with privacy-enhancing technologies, such as encryption or anonymity, or be removed.
- Article 47 be modified to explicitly limit any blanket or indiscriminate data retention measures.

Recommendations on modalities

We recommend that:

- The Chair and the Secretariat implement the modalities in such a manner to ensure an open, inclusive and transparent process, with meaningful opportunities for multi-stakeholder engagement. For example, we recommend that:
    - The modalities should not be interpreted in a manner to disallow stakeholders from adding their organisational affiliation to a joint submission where they have made or intend to make a submission on an organisational basis.
    - There is adequate and clear designation of time for accredited stakeholders to make oral interventions during the substantive sessions.
- The Chair modifies the process of co-facilitators and intersessional informal consultations in order that stakeholders are enabled to observe and make oral statements in intersessional informal consultations, as well as the open formal sessions. The principle of meaningful participation requires that stakeholders are permitted to participate in informal consultations, not least because the object of these consultations is to "explore possibilities to achieve consensus on specific challenging areas." The discussion of challenging and contentious in particular necessitates the observation of and input by multi-stakeholders.