Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Cybercrime Convention Negotiations

Microsoft's submission to the Fifth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Microsoft greatly appreciates the opportunity provided to the representatives of the multistakeholder community to contribute to the Ad Hoc Committee (AHC) efforts to elaborate a cybercrime convention. In line with our previous submissions, Microsoft reiterates its position that these negotiations will only be successful, and any resulting convention only effective, if its scope is narrowly defined and agreed by consensus. The new convention should therefore only criminalize serious offences that are cyber-dependent (e.g., illegal access to the whole or any part of a computer system) and focus on empowering public authorities to prosecute cybercrime more effectively. It should refrain from introducing industry regulation, including in the realm of prevention and cybersecurity standards, to avoid conflation with existing laws.

Cybercriminals, more often than not, operate across borders and as a result international cooperation needs to be at the core of any investigation or prosecution. This kind of cooperation needs to be based on trust and it will only be possible if the offences set forth in the convention are commonly understood and recognized by all parties involved. Furthermore, government access to data needs to remain narrowly tailored to meet specific public safety and national security requirements. With that in mind, we urge states to take concrete steps to balance criminal justice needs with the rights of end users of digital products and services by incorporating robust human rights safeguards and ensuring independent oversight and effective redress mechanisms for victims.

In line with the above we provide detailed comments addressing individual articles contained in the Consolidated Negotiating Document (CND) on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions as contained in document. However, as a matter of priority, we believe the convention should:

- **Contribute to harmonizing laws in this space.** We submit concrete proposals to ensure the convention creates a common baseline for participating states. Too great a deference to domestic legislation would likely undermine the existing Internet architecture.
- **Streamline and expedite government requests for data for the purposes of countering cybercrime.** Digital evidence should be sought from the "data custodian" - the most proximate source of the data. In many cases this will not be the service provider.
- **Limit the scope and applicability of international cooperation measures to focus on fighting cybercrime.** Measures outlined in Chapter IV on international cooperation should be limited to a concrete set of cyber-dependent serious criminal offences, where dual criminality can be established.
- **Avoid introducing any provisions that could legitimize mass surveillance through digital means.** We propose, at minimum, adding concrete human rights safeguards throughout Chapter IV. and deleting articles 74 and Articles 78 (1) on "*real-time collection of content data*" and on "*special investigate techniques*", respectively.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

- **Avoid any legal commitments that could result in preventive content take downs.** We propose deleting provisions that could limit freedom of expression online, such as language contained in Article 78 (4) on data "*removal*" and "*replacement*".
- **Enshrine transparency as a rule when accessing data.** Except in narrow circumstances where giving notice to a user may endanger an investigation, the public has a right to know when, and why governments seek access to their data. This should be enshrined in Articles 45, 61, 64, 68, and 71.
- **Address the challenge of "safe havens" for cybercriminals.** The convention will not achieve its desired results if cybercriminals continue to use safe havens to evade prosecution and accountability. To address this challenge, we propose strengthening measures on extradition in Article 58 (2) and amending grounds of refusal for mutual legal assistance contained in Articles 61 and 68.
- **Avoid provisions that circumvent state-on-state law enforcement cooperation.** As currently drafted, the convention allows for certain situations in which a state could request information directly from data custodians. The state which has jurisdiction over said data would have no knowledge of it being requested, by whom, and for what purpose. We propose to close this loophole by deleting Article 72(b).
- **Avoid mandatory forms of cooperation or forced technology transfers.** The technical assistance chapter of this convention should encourage voluntary cooperation among stakeholders, in line with existing capacity building principles, including those endorsed by consensus through the UN General Assembly. To this end we propose changes to Articles 86 and 89.
- **Avoid expanding the convention's focus on regulating industry, cybersecurity, or resilience.** Other instruments and international standards exist in this space, and these measures, which fall outside of the scope of criminal justice, should not be conflated with the new cybercrime convention. To that end, we propose deleting Articles 90 and 93 in chapter on preventive measures. To be effective, the convention should also avoid regulating specific technologies or imposing direct industry regulation or obligations on non-state parties. We therefore propose deleting Articles 71(4), 72(b), redrafting Article 76 and amending Articles 71(1), 75(1).
- **Establish effective, time-tested, and inclusive mechanisms of implementation.** We support "Option 1" outlined in the chapter on mechanisms of implementation. Establishing a Conference of State Parties with inclusive participation of the broader multistakeholder community would enhance the treaty's effectiveness, whilst avoiding conflation with other treaty commitments and responsibilities of other international bodies (such as the International Telecommunication Union).

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Detailed comments on the Consolidated Negotiating Document (CND) on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions

Our understanding is that the fifth substantive session of the Ad Hoc Committee, in April 2023, will focus on the Consolidated Negotiating Document (CND), specifically on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions. This submission therefore builds on Microsoft's submission to the third substantive session, which looked at some of the same issues.

Preamble & terminology

We understand that many states wish to discuss the preamble once key substantive provisions on, *inter alia*, the scope, criminalization, procedural measures, and international cooperation have been agreed. Microsoft concurs with this approach, but would nevertheless, urge states to consider the following:

- **The need to use commonly understood terms, such as "cybercrime" and "cyberspace"** as opposed to more expansive terms such as "*the use of information and communications technologies for criminal purposes*" throughout the convention. Microsoft continues to believe that effective global cooperation in this space will only be possible if offences are understood in the same way across jurisdictions. These definitions should include serious offences against the integrity, availability, and confidentiality of data (i.e., cybercrime offences). In line with this recommendation, we would encourage states to:
    - Consistently use well-established terms such as "*cybercrime*" and "*cyberspace*" throughout the convention.
    - Align the use of terms throughout the text. For example, the preamble uses the terms "*cyberspace*" (PP.10) and "*digital world*" (PP.3) interchangeably.
- **The need to balance criminal justice needs with legitimate commercial and non-commercial interests and the rights of end users of ICT products and services**. We urge the states to ensure that the convention does not undermine human rights and fundamental freedoms or produce unintended consequences for legitimate online activities. We emphasize that deferring excessively to domestic laws may lead to fragmentation of the existing Internet governance framework. In line with the above we propose states:
    - Retain the existing references to the protection of "*fundamental freedoms and human rights*" (PP.10) and "*personal data*" (PP.16).
    - Preambular Paragraph 10: Introduce terms "*free*" and "*interoperable*" in the description of cyberspace to read: "*promoting a free, open, secure, stable, accessible, interoperable, and peaceful cyberspace for all*".
    - Preambular Paragraph 13: Add the term "*end users*" to specify that the convention aims to protect the legitimate interests of all end users of ICTs, be it governments, private sector entities, civil society organizations, and individuals. The relevant section would read: "*the*

need to protect legitimate interests of end users in the use and development of information and communication technologies".

- Preambular Paragraph 16: Delete subjective words, such as "proper", from the preambular part of the convention.
- Ensure consistent use of terminology when referring to subjects of an investigation. Currently, the draft text refers to "accused person(s)", "suspects", and "persons of interests" inconsistently and interchangeably. We recommend that states address this in the zero-draft by using one well-defined term throughout the convention.
- Data custodian: Replace the term "service provider" with the term "data custodian" throughout the convention. With more and more organizations moving their digital information to the cloud or using cloud-based infrastructure to deliver applications and services to customers, law enforcement agencies often have multiple data sources at their disposal. Whenever possible, digital evidence should be obtained from the "data custodian" - the most proximate source of the data. In many cases this will not be the cloud or service provider. Going directly to the data custodian (usually the customer or consumer) can often be done without jeopardizing an investigation, just as it was the case before organizations moved their data to the cloud.

Chapter IV. – International Cooperation

The primary purpose of the convention should be to encourage effective international cooperation between and among national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime. It should complement the work of existing networks and mechanisms and draw on existing treaties and measures that have already proven to be effective and respect the generally applicable due process principles. Moreover, it should minimize and avoid conflicts with existing laws and create mechanisms to prevent conflicts and to resolve any disputes that arise.

With that in mind, Microsoft has consistently called on states to ensure that all provisions of this convention (a) apply to a precise and narrowly defined set of crimes, which can be commonly understood across jurisdictions to satisfy the criteria of dual criminality, and (b) incorporate activities with clear criminal intent, punishable, at minimum, by three years of imprisonment. Without clear limiting provisions, the convention could unintentionally undermine existing international cooperation. Too broad provisions could:

- overwhelm law enforcement agencies, private sector entities and data custodians more broadly with information requests pertaining to minor offences that may not be commonly understood as "crimes" across jurisdictions;
- gravely impact basic human rights, such as the right to privacy and the freedom of expression;
- undermine the work of cybersecurity experts and researchers.

To avoid such undesired outcomes, the provisions on international cooperation, should, at minimum, be applied to a precisely defined set of offences. They should also include clear provisions for transparency and refusal on the grounds of dual criminality, in respect of political offences, and in instances of persecuting individuals on grounds of their race, religion, gender, or other internationally protected characteristics. The provisions in this chapter should also ensure that human rights protections and due process safeguards are clearly and explicitly factored in at every step of the process. In particular, the rights to free expression,

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

access to information and privacy – as enshrined in existing international instruments – need to be preserved in line with the required minimum standards of legality, proportionality, and necessity.

In line with the above, we recommend states:

- **Limit the applicability of international cooperation provisions to a precisely defined and commonly understood set of serious crimes**.
    - Article 56 (1) and Article 61 (1): The two articles should incorporate the currently bracketed language "*offences set forth in this Convention*" into the final text. Moreover, the inclusion of the currently bracketed text "*any criminal offence*" would greatly increase uncertainty in this space and should therefore be deleted.
    - Article 56 (3): We recommend adding the term "*serious*" to streamline and prioritize international cooperation in this space. The relevant section would read: "*if the if the conduct underlying the offence for which assistance is sought is a serious criminal offence under the laws of both States Parties*".
    - **Specify the term "*serious criminal offence*" in the terminology section** as "*an offence that is punishable under the domestic law of both the requesting State Party and the requested State Party by a minimum deprivation of liberty of at least three years*." This addition would also align the proposed provisions, including those on dual criminality, with the envisioned extradition requirements in Article 58 (1).
    - Article 58 (1): This article likely refers to "*minimum*" deprivation of liberty of at least one year as opposed to "*maximum*". We presume this may be an error.
    - Article 75 (1): Section (a) of this Article could currently be interpreted as extending the scope of application of procedural and international cooperation measures to all crimes that states "*deem appropriate*". Such interpretations can vary widely across jurisdictions and will likely increase uncertainty in this space. We therefore propose to delete the following sentence: "*including, if the States Parties concerned deem it appropriate, links with other criminal activities.*"
- **Establish dual criminality as a key prerequisite for international cooperation**. Microsoft has previously emphasized that data custodians, technology industry included, will need to have a clear and common understanding of what constitutes a cybercrime across jurisdictions to be able to respond appropriately to government requests for information. Without such harmonization, conflicts of law may arise, making effective cooperation and timely information-sharing impossible.
    - Article 56 (3): The current text does not establish clear and predictable dual criminality requirements. At a minimum, offences triggering international cooperation provisions of the convention should (a) exist within the same or similar category of a crime, (b) be punishable by a deprivation of liberty of at least one year as is currently the case in draft Article 58 and (c) relate to the crimes established in the criminalization Chapter of the convention rather than defer to domestic definitions. We therefore propose redrafting Article 56 (3) as follows:
        - "*In matters of international cooperation, ~~whenever~~ dual criminality ~~is~~ shall be considered a necessary requirement, and ~~it~~ shall be deemed fulfilled ~~irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as that of the requesting State Party, or~~ if the ~~conduct of the underlying~~ offence for which assistance is sought is a serious criminal offence set forth in this Convention.*"

These changes will also be important in the context of additional articles, such as Article 61 and 68 (3). Article 61 currently provides states with the opportunity to refuse cooperation on the grounds of the absence of dual criminality. While we strongly welcome this article, its inclusion also implies that the convention should provide clear guidance on establishing dual criminality criteria for a specific set of offences set forth in this convention. This will be essential to avoid any potential abuse of Article 61 (6) as a general opt-out.

- **Ensure that international cooperation provisions do not defer extensively to domestic laws**, as seems to be currently the case across the CND. In our experience, conflicting rules raise barriers to international cooperation. Microsoft frequently deals with situations where one country's laws conflict with lawful demands from another country, which is often a lengthy, costly and difficult process. Global efforts to fight cybercrime will be significantly enhanced if the convention harmonizes rules across jurisdictions and ensures synergies with existing international obligations and instruments. Importantly, when discussing personal data protection, the convention should ensure states transmitting personal data do so in accordance with established international principles and agreements in this area.
    - Add references to "*existing international obligations*" ahead of sections of the CND text that defer to domestic laws, including in, but not limited to, draft Article 58 (9), (10), and (13), Article 61 (4)(m)(f) and (19)(c), Article 64 (1), Article 67 (6), Article 68 (3), Article 75 (1), Article 78 (2), Article 82 (4), Article 89 (7) and (10), Article 94 (1) and Article 97 (1).
    - Add references to existing "*international human rights obligations*" or "*applicable human rights instruments*", as appropriate, in relevant sections of the draft that currently defer exclusively to domestic laws, including in draft Article 58 (14), Article 61 (3) and (4)(f), Article 74, Article 78 (1) and (2), Article 89 (10), Article 94 (1) and (2).
    - Strengthen Article 57 on personal data protection. We propose deleting the outdated reference to "*return*" of personal data in section 2, which seems both insufficient and inappropriate in the digital context (i.e., deletion and destruction is sufficient). Furthermore, we propose including additional language in section 3 to safeguard end users against potential misuse or public dissemination of their data for any other purposes than those authorized under this convention, which would read as follows:
        - *"The States Parties shall take appropriate measures to ensure that the data transferred to them are protected from accidental or unauthorized destruction, accidental loss or unauthorized access, modification, or dissemination <u>for any other purpose than those specified in paragraph 1 of this article</u>."*
    - Delete the word "enhance" in Article 61 (29) to encourage harmonization of national laws and practices in line with provisions contained in this convention as opposed to their potential fragmentation via alternative bilateral arrangements.

<u>Human rights safeguards</u>

Microsoft believes there is a need to incorporate robust human rights safeguards throughout convention to protect end-users from potential abuse of executive authority. The chapter on international cooperation, should, at a minimum, include clear provisions for refusal of cooperation with respect to political offences, in instances where individuals may be persecuted on grounds of their race, religion, gender, or other internationally protected characteristics. Additionally, the rights to free expression, access to information and privacy – as enshrined in existing international instruments – need to be preserved. We propose states:

- **Delete Article 74 and section 1 of Article 78.** We are very concerned that these Articles on "*real-time collection of content data*" and on *"special investigative techniques"* may be misused to legitimize mass surveillance through digital means. As currently drafted, Article 74 neither specifies the information, which should be provided in the request for mutual legal assistance (such as details included in Article 73(3)), nor does it include potential grounds for refusal on the basis of a potential breach of fundamental rights of individuals. Article 78(1) gives rise to similar concerns by permitting any "*measures as may be necessary, including electronic and other forms of surveillance*" in deference to domestic laws and with no regard for existing international human rights obligations, particularly the right to privacy, as well as principles of legality, proportionality, and necessity.
- **Delete section 4 of Article 78 to avoid any legal commitments that could result in preventive content take downs**. The language around data "removal" and "replacement" is particularly concerning and could be used to limit freedom of expression online.
- **Underline the principles of legality, necessity, and proportionality** in relevant provisions throughout this chapter. We would, at minimum, recommend the principles of legality, necessity, and proportionality to be explicitly included in Article 61 (4)(f), Article 61 (28)(b) and Article 74. By a way of example, we would also recommend modifying Article 75 (1) (b) as follows to align its provisions with the aforementioned criteria:
    - *"The identity, whereabouts and relevant activities of persons suspected of involvement in such offences ~~or the location of other persons concerned~~".*
- **Delete the phrase "other persons concerned" in Article 75 (1)(b-I)** as it is currently unclear why states should be obliged to disclose information on location and activities of persons not suspected of being involved in offences covered under this convention (or any other criminal offence).
- **Exempt political offences** from the scope of provisions of the international cooperation section explicitly. The current exemption in Article 58 (4) is insufficient. We would recommend establishing clearer grounds for refusal by including a stand-alone section in this Article stating that "*this Convention shall not be used to extradite any individual suspected of having committed a political offence*".
- **Subject extradition to a clear set of conditions and safeguards**. Article 58 does not currently establish sufficient safeguards in this regard. At a minimum, Article 59 (9) should enumerate sufficient evidentiary basis required for extradition, rather than call for *"simplifying evidentiary requirements",* as is currently the case. Furthermore, to strengthen extradition safeguards we propose to explicitly tie the conditions for extradition referenced in Article 58 (8) to safeguards enumerated in Article 58 (15):
    - *"Extradition shall be subject to the conditions and safeguards provided for in Article 58 (15) of this Convention as well as by the domestic law of the requested State Party ~~or~~ and by applicable extradition treaties, including, inter alia, the grounds upon which the requested State Party may refuse extradition."*
- **Fully align international cooperation provisions with existing international human rights instruments**. As a general principle, we would encourage states to ensure that this convention does not quote selectively from existing instruments or alter the quotes. By way of example, the extradition exemption included in Article 58 (15) mirrors existing international instruments, including the International Refugee Convention, albeit only partially and selectively. We would therefore urge states to reinsert the phrase "*membership of a particular social group"* to fully align the Article 58(15) with

Article 33 of the Refugee Convention.[1] Additionally, we would also recommend adding the phrase "*politically motivated persecution, or inhuman and degrading treatment or punishment*" next to the existing reference on torture in that same Article to spell out in full the relevant provisions of the Convention against Torture.

Mutual legal assistance

Microsoft recognizes the central importance of provisions for mutual legal assistance (MLAT) to enable information-sharing and exchange of electronic evidence. However, any access to digital information can only be enabled pursuant to lawful process with appropriate safeguards. Any framework regulating a government's ability to access digital information stored with data custodians, technology industry included, must begin by recognizing the general principle that all access should be pursuant to the rule of law and compliant with existing data protection regulations. Principles surrounding lawful access to digital information are well established under existing legal instruments.

At a minimum, lawful access pursuant to mutual legal assistance provisions should be predicated on independent judicial authorization, notice to the user, orders which are strictly necessary and proportionate to stated aims and an independent redress, appeal, or review mechanism. In addition, the framework should recognize the potential conflicts of law inherent when a government requests data stored on a global cloud and should include mechanisms to raise such conflicts, so a recipient of a government request is not forced to violate one country's laws to comply with another's.

On the subject of mutual legal assistance, we commend that the CND includes an initial set of principles and provisions to ensure clarity and predictability in government access to digital information. We wish to reiterate some of our previous proposals on this subject:

- **Transparency as a rule:** Microsoft believes that except in narrow circumstances, the public has a right to know how, when, and why governments seek access to their data. Such transparency is necessary to safeguard end users from potential abuse of executive authority. We previously put forward proposals to Article 45 (1) to ensure accountability in the conduct of law enforcement authorities by providing notice to impacted individuals, provided that such notices do not compromise an investigation. [2] Secrecy should be the exception rather than the rule because otherwise users are unable to assert their rights and privileges, and trust in both the online ecosystem as well as in the rule of law is undermined. With that in mind we recommend:
    - Add a section (b) in Article 61 (17) stating the following: "*The requested State Party shall, unless secrecy is required as outlined in Article 45 (1)(c) of this Convention, notify the data custodian".*
    - When secrecy is required, we propose adding the following language to Article 61 (18) to specify that any request for information under secrecy rule "*should be made in writing and include detailed explanations as to why confidentiality is necessary not to endanger an ongoing investigation, prosecution or other proceeding."*

[1] "No Contracting State shall expel or return ("refouler") a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion." (Refugee Convention, Art. 33)

[2] Proposed Article 45 (1)(c): *"The Convention recognizes that absent narrow circumstances, users have a right to know when the government requires a data custodian to submit information and, unless secrecy is required, the data custodian shall have a right to notify the user."*

- Amend Article 64 (2) on provision of spontaneous information to specify that the information in question will be kept confidential "*for the purposes of not endangering an ongoing investigation, prosecution or proceeding ~~or~~ and only be used by the receiving State subject to specified conditions. If the receiving State Party cannot comply with such request, it shall notify the providing State Party~~, which shall then determine whether the information should nevertheless be provided~~.*"
- Revise section (g) in Article 68 (2) to read as follows: *"If there is a need to keep the request for preservation confidential and to not notify the user, the requesting State Party shall describe the rationale for confidentiality in writing and shall make such requests congruent with Article 45 (d) of this Convention."*
- Add a new section (f)bis to Article 71 (5) on emergency assistance to ensure that states communicate the need for secrecy in those situations as well. The section could read as follows: *"Any other information required under this Convention, including information to satisfy requirements contained in Article 61 of this Convention;"*

- **Human rights concerns as a ground for refusal**: Microsoft commends the inclusion of specific grounds under which MLAT can be refused, such as in Article 61 and Article 68. However, we note with concern that some relevant Articles do not include such grounds for refusal in a specific way and that human rights concerns are currently not included among relevant grounds for refusal. We would therefore propose:
  - Add a new section in Article 61 (18), Article 68 (5), and potentially Article 69 (2), which would read as follows: *"Mutual legal assistance may be refused if the requested State Party concludes that execution of the request is likely to materially violate the fundamental human rights of the subject of the legal assistance request or other persons that may be implicated"*.
  - Limit requests for information to ensure that only information relevant to the proceeding in question is being covered by MLAT provisions. This could be achieved by specifying, in Article 61, 28 (b) that requests for information can only apply to *"records or documents that are relevant to the investigation, prosecution or proceeding in question and meet the criteria of proportionality, necessity, and legality."*
  - Extend the grounds for refusal contained in Articles 61 and 68 to Article 70. Including specific grounds for refusal when it comes down to access, seizure, and disclosure of stored data is of paramount importance in protecting end users from potential abuse of executive authority and will increase predictability. However, no grounds for refusal are currently included in this Article, which stands in contrast to Article 61 (on general principles of MLAT) and Article 68 (preservation of stored data). We therefore propose that Article 70 should either duplicate or point to specific grounds for refusal that are relevant in this context (such as Articles 61 and 68).

- **Right of data custodians to review requests in a written form:** This provision is key to ensuring data custodians can respond appropriately to government requests for information. It increases transparency and ensures that requests can be processed without errors and in an expedited fashion. It also ensures effective judicial review and redress should rights of individuals be violated in the discharge of executive powers under this convention.
  - Revise Article 71 (6) to ensure that orally transmitted requests cannot be processed officially without being accompanied by a written request. Specifically, the following sentence should be deleted in its entirety: "*A State Party may also accept a request transmitted orally and may require confirmation in electronic form.*"

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Safe havens

In Microsoft's experience, strengthening international cooperation to address "safe havens" for cybercriminals is of cardinal importance. Even the most streamlined procedures for exchanging electronic evidence and obtaining data access will not achieve their desired results if cybercriminals continue to leverage safe havens to evade prosecution and accountability. Where there is an indictment supported by evidence acquired through legal process, subject to the protections outlined above, individuals engaged in cybercrime should be subject to formal international extradition proceedings. In this context, we commend Draft Article 89 (6), which proposes to address this issue through technical assistance. However, to address the challenge of safe havens more comprehensively, we would also recommend the following:

- **Strengthen Article 58 (20) on extradition** to read as follows: *"States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or enhance the effectiveness of extradition and to take other appropriate measures against States who harbour cybercriminals within their jurisdictions."*
- **Revise Article 61 (19)(b) and Article 68 (5)(b),** by removing "*other essential interests*" from the list of reasons for legitimate refusal for mutual legal assistance. As currently drafted, we fear this provision is too broad and could potentially be used by states as an excuse not to extradite cybercriminals hiding within their jurisdictions due to lack of capacity or other politically motivated reasons.

Technology-neutral criminal justice instrument

This convention should focus on empowering public authorities to prosecute cybercrime more effectively. We therefore recommend carefully evaluating each article to assess whether it, in fact, primarily targets public authorities or other, non-governmental entities. Moreover, as highlighted elsewhere in this submission, governments should address legal demands 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 trust in global data flows.

We commend that the draft introduces the term "custodian of the stored data" in Article 68. However, we note that the draft currently uses the term "custodian of the stored data" and the term "service provider" interchangeably and inconsistently. A service provider may not always be the most proximate source or rights holder of the data in question. We would therefore propose to replace the term "service provider" with the term "the custodian of the stored data" throughout the convention.

We have also previously called for this treaty to remain a technology-neutral criminal justice instrument. To do so, the treaty should regulate interactions among law enforcement agencies of state parties and avoid regulating specific technologies or imposing direct industry regulation or obligations on non-state parties. As it stands, there are several articles that seem to regulate specific technologies or interactions with non-public entities, industry included. With that in mind, we would propose states:

- **Amend Article 71 (1)** dealing with emergency assistance and establishing a 24/7 points of contact network by deleting the entirety of the text following the phrase "*immediate assistance*". This text establishes direct obligations for industry which we believe is inappropriate in a section dedicated to an intergovernmental points of contact network.

- **Delete Article 71 (4)**, which currently encourages states to develop new legislation to regulate the industry. We would propose to replace the existing text in sections (a – c) with a more general text that would read as follows "*each state party shall adopt such legislative measures as may be necessary to enable the implementation of provisions contained in this Article*".
- **Revise section (b) of Article 75 (1):** This section currently enumerates specific types of technologies, such as "*illicit encrypted platforms*" and "*operational indicators of compromise and other indicators of concern*" that should be subject to information exchange among states. We recommend deleting those references as a means of future-proofing the convention.

Relatedly, we would recommend that the convention leaves any potential interaction between public authorities and industry to be addressed at the level of domestic laws. With that in mind, we urge states to:

- **Delete, at minimum, reference to non-legislative "other measures"** in Article 71 (4).
- **Delete Article 72 (b)**, which could be misused by states to circumvent the requirement to cooperate with law enforcement agencies of other states. Specifically, the provisions of this Article could incentivize states to request data directly from the data custodians by securing consent of user (including under duress). This would result in situations where the state in which such data is located has no knowledge of it being requested, by whom, and for what purpose. We believe this provision could significantly undermine trust and reduce transparency in this space.
- **Delete Article 76** on public private partnerships and replace it with a general Article encouraging States parties to pursue public private partnerships on a voluntary basis without prescribing what form such partnership should take.

<u>Collection, Preservation, Retention and Access to Computer Data</u>

The convention should require strict and transparent data minimization, as well as retention and dissemination limits, taking into account that real-time collection or immediate preservation may not always be technically possible. Where applicable, the convention should also provide for specific preservation and retention limits rather than defer to domestic laws to streamline existing processes and clarify expectations for data custodians, technology industry included. In line with these comments, we recommend states:

- **Delete section (e) of Article 61 (4) on collection of real-time traffic data in its entirety.** Traffic data denotes record of communication consisting of indicators such as start and stop time, origination point (calling number, FROM address), and destination point (called number, TO address). As such, it is an after-the-fact record of communication or activity that cannot be collected in "real-time". For these reasons, we recommend that states address the issue of traffic data via a "retention" approach rather than via provisions on "real-time collection", which is conceptually flawed and technically not possible.
- **Delete Article 73 on mutual legal assistance in the real-time collection of traffic data in its entirety.** As noted above, the provisions of this article are not in line with the reality of traffic data and with what is technically feasible.
- **Revise section (f) of Article 61 (4) on collection and recording of content data.** As currently drafted, this provision could be interpreted as relating to law enforcement access of both stored "collected" and real-time "recording" of content data. We note that different international laws apply to these categories. We therefore urge states not to introduce new international provisions that would conflate and confuse the application of the existing rules. We propose revising section (f) as follows:

- ~~*Collecting or recording*~~ *Stored content [data]* ~~*[information]*~~ *of specified communications transmitted by means of a computer system, in line with existing international human rights obligations and in particular the principles of proportionality, legality and necessity, and to the extent permitted or required under the States Parties' applicable treaties and domestic laws;*

- **Amend Article 68 (7) to align its provisions with existing international rules on preservation of stored data**. We note that most existing rules require an initial preservation period of 60 days with a possibility for additional extension of 30 days before the requesting state proceeds with a production order. Following that, the data is traditionally preserved pending the fulfilment of the production order. However, the existing rules also specify that should the preserved data no longer be required, then the requesting state must inform the data custodian who can subsequently delete the preserved data. This is an important obligation, which should be reflected here. We would therefore propose adding the following section at the end of Article 68 (7):
    - *"If the requesting State Party does not submit a request for the disclosure of the data at the expiry of 60 days, then the requested State Party shall direct the data custodian to delete the data in question."*
- **Revise Article 69 on expedited disclosure of preserved traffic information**. As currently drafted, this Article runs the risk of conflating data disclosures with preservation requests. Furthermore, it seems to open a path for disclosing sensitive personally identifiable information of users. We therefore propose deleting the currently bracketed text "data" from the heading and the text of Article 69. Furthermore, we propose to clearly scope requests for traffic information by adding the following sentence to Article 69 (1):
    - *"…the requested State Party shall expeditiously disclose to the requesting State Party a sufficient amount of traffic* ~~*[data]*~~ *information to identify that service provider and the path through which the communication was transmitted, without disclosing personally identifiable information."*

Protecting victims of cybercrime

One of the key objectives of the convention should be protecting the targets and victims of cybercrime, including by offering them effective remedies, and setting out an adequate set of human rights safeguards. The new convention cannot become an avenue for states to remove or shirk their existing obligations under international law, especially international human rights law. Instead, this convention should add to or streamline existing international legal obligations with a focus on protecting victims.

In this context, we welcome the inclusion of cluster 7 provisions on the recovery and return of proceeds of cybercrime to victims. We particularly commend measures included in Article 80 that enable victims to initiate civil action in courts of other states to protect their property rights violated by cybercriminals. However, we note that any provisions regarding recovering criminally obtained property must be constrained by the parties' human rights obligations and contain appropriate grounds for refusal. With these considerations in mind, we recommend states:

- **Provide greater clarity on applicable jurisdiction.** This will be particularly relevant in the context of Article 82 (2), which compels states having jurisdiction over a particular offence to take measures to identify, trace and free or seize proceeds of cybercrime. While we applaud the inclusion of Article 82, we note with concern that the current text in the preceding chapters (in particular Article 40) does not offer any guidance on which jurisdiction applies for the purposes of the convention.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

- **Establish "Option 1" in Article 84 as the sole basis for further negotiations.** Microsoft supports this option to guarantee that any proceeds of cybercrime are returned to prior legitimate owners. We do not support Option 2, which defers exclusively to domestic laws and administrative procedures. The latter will likely give rise to jurisdictional disputes and undermine trust among states, victims and other relevant stakeholders, thereby frustrating international cooperation in countering cybercrime.

Chapter V. – Technical assistance and capacity building

Cybercrime knows no borders. Any effective response must enable the multistakeholder community to effectively work together. However, today, states are at vastly different levels of readiness when it comes to cybercrime investigation and prosecution. As cybercriminals have little respect for borders, work is needed, including through capacity building, to empower public authorities around the world to prevent and counter cybercrime.

Microsoft has called for the convention to explicitly address issues such as technical assistance and encryption to ensure they are framed in compliance with international human rights laws, in particular privacy rights and freedom of expression. Technical assistance provisions need to also remain technology-neutral, and only be provided on a voluntary basis, rather than mandating any forms of technology transfers. Intellectual property of products and services leveraged requires protections to facilitate public-private cooperation in combating cybercrime.

We therefore welcome provisions in this chapter creating a framework for training programs, as well as technical assistance to support the implementation of the convention. In this context, would like to recall existing cybersecurity capacity building principles, agreed through the adoption of the 2021 consensus report of the Open-ended working group on cybersecurity (A/75/816). In particular, we recall that states agreed that capacity building should respect human rights and fundamental freedoms, be gender sensitive, sustainable, results-focused, demand-driven, voluntary, and tailored to specific needs and contexts. Microsoft believes that these principles, endorsed by the General Assembly in consensus resolution, should be reflected in this chapter and guide its provisions.

- **Incorporate existing cybersecurity capacity building principles** via a direct reference to the OEWG 2021 consensus report and align individual provisions in this chapter with specific principles on (a) processes, (b) partnerships, and (c) people contained in paragraph 55. This is particularly relevant in the context of proposed principles contained in Article 89 (2), which seem disconnected from previously agreed UN language. By a way of example, of how to ensure alignment, we would propose to add a principle (c)bis in Article 89 (2), which would read as follows:
    - **(c)bis:** *"Ensuring respect for human rights and fundamental freedoms and gender sensitivity;"*
- **Delete Article 89 (d) to ensure that the convention is not used for mandatory or forced technology transfers.** As currently written, this section fails to incorporate the principle of voluntary cooperation in this space.
- **Reiterate the voluntary nature of capacity building cooperation.** To that end, we propose the following revisions:
    - Article 86 (a): "*Technical assistance and capacity-building shall be carried out in an inclusive and voluntary manner ~~and include all nations~~, with particular attention given to developing countries, and all relevant stakeholders;*"

- Article 87 (4): *"…developing, with the voluntary participation of the competent authorities and ~~main~~ stakeholders, including civil society and the private sector, strategies and action plans to prevent and combat those offences."*

- **Recognize the added value and expertise other stakeholders can bring into capacity building work**, including through their contributions to information sharing, training programs and technical assistance. We propose expanding existing provisions in this chapter as follows:
  - Article 87 (2): "*States Parties shall, to the extent necessary, initiate, develop, implement or improve, in voluntary collaboration with stakeholders whenever appropriate, specific training programs for their personnel responsible for the prevention, detection, investigation and prosecution of the offences covered by this Convention*."
  - Article 87 (3): *"States Parties shall assist one another, and in voluntary collaboration with stakeholders, in planning and implementing research and training programs…"*
  - Article 87 (9): *"States Parties shall entrust the United Nations Office on Drugs and Crime with the task of coordinating and providing specialized technical assistance to States Parties, upon request, in collaboration with other international, ~~and~~ regional, and non-governmental organizations, as appropriate, with a view to promoting the implementation of programs and projects to prevent and combat offences covered by this Convention, and to assist the States Parties to identify common gaps in capacity or needs for technical assistance that would facilitate effective implementation of the Convention."*
  - Article 88 (1): *"Each State Party shall consider analyzing, in consultation with relevant experts, including, on a voluntary basis, those from civil society and the private sector, trends in its territory with respect to offences established in accordance with this Convention, as well as the circumstances in which such offences are committed."*
  - Article 88 (2): *"The States Parties shall consider developing and sharing with each other, and with stakeholders, ~~and through~~ international and regional organizations statistics, analytical expertise and information concerning cybercrime…"*

- **Retaining sections (l) and (m) of Article 87 as proposed.** We welcome the focus of these sections on protection of victims/witnesses and human rights, respectively. These provisions are consistent with the cybersecurity capacity building principles endorsed by the General Assembly.

Chapter VI. – Preventive measures

Microsoft recognizes the importance of preventive measures in fighting cybercrime, in particular measures related to cybersecurity education, capacity building, awareness raising, and increased public-private cooperation. The implementation of technical measures, such as encryption or multifactor authentication is similarly pivotal. These types of investments ensure that the online environment is safer and more secure and drive up the barrier to entry for cybercriminals.

However, we believe the convention should primarily focus on dealing with cybercrime and investigating and prosecuting cybercriminals. Its scope should not be expanded to cybersecurity measures or increasing the overall societal resilience in cyberspace. Other instruments are available to address those areas. The convention should focus on public authorities and not introduce industry regulation.

States have typically focused on developing frameworks and legislative approaches that aim to increase the cybersecurity and cyber resilience of the online environment in non-criminal contexts and we recommend

that this separation persists. It is our view that the AHC process should not create additional rules in this space, particularly as this area covers a number of issues falling outside the scope of criminal justice and the existing remit of the Third Committee. In line with the above, we recommend states:

- **Delete Article 90 in its entirety.** As currently drafted, the Article touches upon multiple issues related to cybersecurity standards and regulation of safety of ICT products in way that expands the focus of the convention beyond the criminal justice domain. The Article also seeks to regulate industry in a specific way, including, but not limited to, in sections (d) through (g).
- **Delete section (d)(ii) of Article 92 (1).** This section, with its broad wording focused on "national security" and "morals", could be used to restrict what information is available about cybercrime.
- **Retain references to anonymous reporting of ICT incidents contained in Article 92 (2).** We have previously called for the convention to protect security researchers, ethical hackers, and penetration testers, who perform essential work in improving the security of the digital ecosystem. Persons engaged in lawful cybersecurity work should be exempt from the scope of any future cybercrime treaty. The existing reference for anonymous reporting of existing ICT vulnerabilities should be retained and the corresponding exemption included in the criminalization chapter.
- **Delete Article 93 on money laundering in its entirety.** Microsoft believes that the content of this Article is outside of the scope of this convention. Additionally, provisions addressing prevention and money laundering in cross-border crime are already included in existing international (UNCAC and UNTOC) and regional instruments. Adding such provisions here will likely generate significant conflict of laws and not contribute to a harmonization of rules in this space.

Chapter VII. – Mechanisms of implementation

Microsoft recognizes that for the convention to deliver impactful outcomes, its provisions must not remain empty words on paper. Therefore, it is essential to create and empower mechanisms of implementation. We call on states to draw on existing mechanisms that have proven effective. Moreover, we urge states to ensure the ICT industry has a meaningful role in any implementation mechanisms.

We believe a "treaty body" (e.g., a Conference of the Parties or Meeting of the Parties) should oversee the operation and effectiveness of the convention. Given the role the technology industry has in this space, it would be appropriate for the convention to explicitly affirm a meaningful role for ICT companies in those meetings. Previous experience from regional bodies, such as the Council of Europe's Cybercrime Committee, has shown the value of public private cooperation in this area.

Having said that, Microsoft does not support the creation of any new commission or similar body, or the expansion of the existing bodies' scope of work to this space (e.g., the International Telecommunication Union (ITU)). We believe that might lead to conflation of established mandates and other treaty commitments with those assumed under this convention. In line with the above, we recommend states:

- **Establish "Option 1" in Article 94 as the sole basis for further discussion on mechanisms of implementation.** As we have emphasized previously, any follow up convenings to improve capacity and collaboration to counter cybercrime within the framework of this convention should include technical experts from the ICT industry and the broader multistakeholder community in a meaningful way. This could be achieved by:
    - Adding the text of existing AHC modality on stakeholder participation in Article 94. This stakeholder modality, approved by consensus in relevant UN General Assembly resolution

(A/RES/75/282), gives non-ECOSOC organizations, including industry, the opportunity to meaningfully participate in UN cybercrime treaty negotiations, whilst protecting the decision-making prerogatives of states. Embedding this modality firmly in a future mechanism of implementation would ensure that states can continue to benefit from expertise of the multistakeholder community, including their cutting-edge insights into ever-evolving cybercrime threats, latest methods of detection, and evolving impacts on victims.

- Adding references to stakeholder contributions in sections (b) and (d) of Article 95 (4). The revised sections could read as follows:
  - Section (b): *"Facilitating the exchange of information among States Parties and non-governmental organizations, including civil society, academia and industry, on patterns and trends in cybercrime and on successful practices for preventing and combating such crime…"*
  - Section (d): *"Making appropriate use of relevant information produced by international and regional mechanisms for preventing and combating cybercrime, as well as relevant information produced by non-governmental organizations, in order to avoid unnecessary duplication of work."*
- Strengthening reference to stakeholder input in Article 95 (6) to read as follows: "*Inputs received from relevant non-governmental organizations ~~duly accredited in accordance with procedures to be decided upon by the Conference of the States Parties~~ ~~may~~ will also be considered*."

- **Create an expert forum** that would allow states, industry, and the broader technical community to exchange views on the latest cybercrime threats and potential mitigation measures. Given the dynamic nature of cybercrime, such a forum would greatly enhance public authorities' ability to respond effectively and timely to evolving threats.
- **Delete Article 95bis proposing the establishment of an International Technical Commission under the ITU.** We believe that expansion of the ITU competencies into the field of cybercrime would run contrary to its mandate and would lead to conflation of provisions in this convention with existing treaty commitments.