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 Fourth 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 meaningfully participate in the discussions of the Ad Hoc Committee (AHC) to elaborate a cybercrime convention. We believe that the AHC's inclusiveness should serve as an inspiration and precedent for other cyber-related discussions at the United Nations (UN) and elsewhere.

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. 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. However, this kind of cooperation requires that the offences are commonly understood and recognized by all parties involved.

A summary of what we believe are key recommendations that we have put forward previously includes:

- **Criminalize substantive offences that are cyber-dependent**, e.g., illegal access to the whole or any part of a computer system. However, only do so when description and definitions are widely accepted. A focus on serious crime will contribute to streamlining of processes and procedures.
- **Do not expand the definition of cybercrime to include all crimes where a computer was involved** in the planning or execution of the crime. The new convention should only explore including illegal activity that is cyber-enabled when the offenses that are of such scale, scope, or speed that they would not be feasible without information and communication technologies (ICTs) – and where the definitions are commonly understood, for example as it relates to online child sexual exploitation.
- **Avoid duplication of offences covered by other legal instruments**, such as corruption, trafficking, or terrorism simply because these may be complemented using technology. Such an approach risks introducing contradiction and confusion and will not deliver a targeted, practical instrument that can improve our collective ability to tackle cybercrime.
- **Do not expand the definition of cybercrime to include online content**, given the potential impact on human rights. States should specifically avoid any commitments that would result in preventative content take downs.
- **Ensure the purpose and reach of government access to data remains narrowly tailored** to meet specific public safety and national security needs.
- **Incorporate robust human rights safeguards** to ensure independent oversight and effective redress mechanisms. The convention should emphasize the importance of minimizing conflicts of law, including with international human rights law, and create mechanisms to resolve conflicts that do arise.
- **Refrain from introducing industry regulation (including as an unintended consequence).** The new treaty should focus on empowering public authorities to prosecute cybercrime more effectively. Against this background, we recommend carefully evaluating each article to assess whether it, in fact, primarily targets public authorities or other, non-governmental entities.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

In addition to the above, we would like to draw attention to the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes, adopted by members of the Organization for Economic Development (OECD) on 14 December 2022. The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities seeks to improve trust in cross-border data flows – which are central to the digital transformation of the global economy – by clarifying how national security and law enforcement agencies can access personal data under existing legal frameworks. The principles set out how legal frameworks regulate government access; the legal standards applied when access is sought; how access is approved, and how the resulting data is handled; as well as efforts by countries to provide transparency to the public. They also tackle some of the thornier issues – such as oversight and redress – that have proven challenging to policy discussions for many years. We believe the Declaration could provide useful guidance in the ongoing treaty negotiations.

In the following sections, we provide our observations and recommendations on some of the provisions included in the Consolidated Negotiating Document. We remain available for any additional clarification.

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 general provisions and the provisions on criminalization and on procedural measures and law enforcement

Our understanding is that the fourth substantive session of the Ad Hoc Committee, in January 2023, will focus on the first reading of the Consolidated Negotiating Document (CND) on the general provisions and the provisions on criminalization and on procedural measures and law enforcement as contained in Chair document A/AC.291/16. This submission therefore focuses on said document, building upon our submission to the second substantive session, which looked at similar issues.

Definitions & Terminology

We understand that definitions and terms will be contained in a separate chapter of the convention, which would be drafted once substantive provisions of the convention have been agreed. Nevertheless, we would encourage states to use precise definitions and terminology throughout the drafting process, in particular as it relates to:

- **Criminalizing *"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. This would prevent the inadvertent criminalization of, for example, penetration testing, a common cybersecurity practice where simulated cyberattacks against computer system are used to check for and responsibly report exploitable vulnerabilities.
- **Using precise terms such as "*unauthorized access*", "*electronic data*", and "*ICT system or device*"** as opposed to broad terms such as "*infringing security measures*", "*access to information*", or a "*computer system*". In particular, the language regarding the *"access to information"* may come into conflict with a basic human right "*to seek, receive and impart information through any media and regardless of frontiers*" enshrined in Article 19 of International Covenant on Civil and Political Rights of 1966.
- **Giving preference to the term "*ICT system or device*" over the term "*computer system*"**, which was used in the Budapest Convention. In our view, the term "*computer system*" may not be as appropriate in the modern context as the term "*ICT system or device*", which would – as opposed to a computer system - also include telecommunications conducted over the internet. Considering the volume of Voice over Internet Protocol (VoIP) calls that are conducted over the internet and the receding of the Public Switch Telephone Network it is important that the provisions of the convention reflect that reality.
- **Using the commonly understood term "cybercrime"**, as opposed to more expansive and less defined 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 serious cybercrime offences are commonly understood and recognized across jurisdictions. We therefore urge states to focus international efforts on addressing core cybercrime offences where international consensus can be reached. Considering the AHC discussions to date, such core cybercrime offenses seem to include first and foremost **serious offences against the integrity, availability, and confidentiality of data**, which threaten us all.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Chapter I. – General Provisions

From Microsoft's perspective, the convention should combat cybercrime by facilitating international cooperation while protecting, rather than undermining the confidentiality, integrity, and availability of user data and essential digital services. To that end, the **scope of the future convention should be clearly and narrowly defined**. It should, further, include appropriate human rights safeguards and ensure robust independent oversight and effective redress mechanisms. Moreover, it should minimize and avoid conflicts with existing laws, create mechanisms to prevent conflicts, and resolve disputes that arise. Anything less would not only risk undermining and fracturing *existing* efforts to fight cybercrime, but could also produce *additional*, unintended negative consequences for legitimate commercial and non-commercial online activity and could negatively impact human rights.

In line with the above, we propose the following changes:

- **Articles 1 (a):** Introduce the term "serious" for the article to read: *"…promote and strengthen measures to prevent and combat cybercrime, while protecting users of information and communications technologies from such serious crime"*.
- **Article 1 (c):** Replace the term *"measures*" with the term "*support*". The use of the term "measures" could create unfounded expectations of technology transfers, in particular as we believe that the convention should focus on enhancing cooperation among states. It should not impose obligations on private entities. The revised Article could read: *"…provide practical ~~measures~~ support to enhance technical assistance among States parties…"*.
- **Article 3 (1):** Remove the term "*detection*" as that appears to be out of scope of this particular convention. On a related note, remove the term *"suppression*" from the draft. "*Deletion*" is a term that is widely accepted in this space.
- **Article 3 (3):** We recommend deletion of this article, as it expands the scope of the convention unnecessarily.
- **Article 4:** As for the protection of sovereignty, we want to stress that when conducting extraterritorial surveillance measures, governments must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use extraterritorial measures to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory.
- **Article 5 (1):** Delete the qualifier "*applicable*", as it opens the doors for potentially unhelpful interpretations as to which international human rights law is and is not applicable. In addition, we would propose adding a clear reference to applicable human rights instruments in this paragraph, including, at minimum the International Covenant on Civil and Political Rights. The Article 5 (1) would read:
    - *"States Parties shall ensure that the implementation of its obligations under this Convention is in accordance with ~~applicable~~ international human rights law, including, but not limited to, the International Covenant on Civil and Political Rights."*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Chapter II. – Criminalization

Microsoft reiterates that for the convention to facilitate effective international cooperation, the technology industry, and service providers in particular, will have to have a **clear understanding of what constitutes an act of cybercrime** in order to respond appropriately to government requests for information. This will require criminalizing substantive offences that are cyber-dependent only and not expanding the definition of cybercrime merely because a computer was involved in the planning or execution of a crime.

Should other non-cyber dependent crimes be included, we recommend these are narrowly defined and consistent with international human rights standards. The convention should not seek to cover ordinary crimes already clearly and adequately prohibited under existing domestic legislation and merely incidentally involve or benefit from ICT systems without targeting or harming those systems. For example, "drug trafficking," "arms trafficking," "distribution of counterfeit medicines," and "money laundering" are already crimes, and a computer may merely have been used to communicate about an offense.

Overall, we reiterate our call for states to keep the principle of **dual criminality** in mind for crimes included in the convention. We also urge states to recognize that their diverging political, cultural, and legal systems will likely make consensus agreement on a meaningful list of all offenses committed by using a computer system difficult, if not impossible to agree on, within the short timeframe of current AHC negotiations.

Furthermore, we encourage states to include **"*criminal intent*" as a prerequisite for establishing crimes under this convention**. Standards such as "without authorization" or "unlawfully" risk allowing the criminalisation of acts carried out with beneficial intent, such as security research, and increase the likelihood of prosecuting individuals for behaviour that did not, or could not have been expected to, cause harm.

Finally, we urge states **to leverage agreed language as much as possible**. Existing instruments, such as the UNTOC, UNCAC, and other widely accepted instruments such as the Budapest Convention can provide guidance in this regard. We recommend the *exact* language of these conventions to be used or referred to whenever possible since such provisions have already been transposed into national legislations across the world. Introducing differences in similar provisions across instruments could result in unintended negative consequences and create confusion which can produce delays, increase costs, or even in some cases frustrate cooperation entirely.

In line with the above, we propose the following changes:

- **Article 6**: We have previously highlighted the importance of adequately protecting security researchers or penetration testers, who perform essential work to improve cyber defences. As such, the convention should include legitimate exceptions for what would otherwise be considered unlawful behavior by including a paragraph in Article 6 on illegal access stating that:
    - *"Nothing in this convention shall be interpreted as criminalizing the conduct of persons engaged in lawful cybersecurity work."*
- **Article 12:** Avoid criminalizing broad categories of acts that may be *unlawful* but not necessarily *criminal* across jurisdictions, such as "*false representation*" or "*deception*" as is, for example, currently the case in Article 12. Such acts may be pursued by private parties in civil court. Including such acts in the scope of this convention risks overwhelming states and private sector providers with information requests while diverting attention from combating serious cybercrime offences where prompt action can contribute to disrupting organized cybercrime networks that operate across multiple jurisdictions.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

- **Avoid introducing new definitions for existing crimes**, such as "*obstruction of justice*", "*arms trafficking*", or "*money-laundering*". As highlighted above, this may prove detrimental to reaching consensus. In line with this, we recommend deleting Articles 30, 31, 32, 33 and 34.
- **Refrain from expanding the definition of cybercrime to include computer-enabled dissemination of information or provisions that are focused on online content**. The convention should not attempt to regulate content, given the different legal practices and cultural approaches to this area across the world. In particular, the convention should specifically avoid any commitments that would result in preventive content take downs of criminalizing freedom of expression, a basic human right. In line with this, we would recommend:
    - Deleting Article 23, or, alternatively, scoping its applicability to "*children*" only.
    - Deleting Articles 26 and 27 since no widely accepted or agreed definition of such crimes exists across jurisdictions.
    - Deleting Article 28, whose provisions can come into conflict with existing international instruments, particularly the 1948 Convention on the Prevention and Punishment of the Crime of Genocide, which already criminalizes "*public incitement to commit genocide*" (Article 3, paragraph (c) regardless of media or the type of technology used to commit such act.
    - Deleting Article 29, whose provisions can come into conflict with existing international instruments, including the 1999 International Convention for the Suppression of the Financing of Terrorism, which already criminalizes financing of terrorism regardless of the type of technology used.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Chapter III. – Procedural Measures and Law Enforcement

It is our opinion that the current draft would benefit from additional safeguards that would protect citizens from potential abuse of executive authority. In particular, we believe that the scope of application of all procedural measures needs to be exclusively limited to crimes set forth in the convention. Furthermore, clear scoping of the convention is necessary to ensure that technology industry have a clear understanding of what constitutes an act of cybercrime so that they can then respond appropriately to government requests for information. In view of the above, we propose the following changes:

- **Refer to specific articles in the criminalization chapter and avoid imprecise references to "ICT crimes" or "any other crimes"** to avoid inadvertently creating confusion for prosecutors operating across countries, in particular if the crime in question is only criminalized in one of the two jurisdictions in question. In particular:
    - Delete Article 41, paragraph 2 (b) as the phrasing contained therein would inadvertently expand the applicability of procedural measures to any and all offences conducted with the use of ICTs. Similarly, we propose the deletion of the brackets *"[any criminal offences]"* and *"[serious crimes"]*, in Article 41, paragraph 2 (c).
    - Add a new Article scoping the applicability of all procedural measures contained in this chapter to a precisely defined set of crimes: *"The scope of application of all procedural measures set forth in this convention will be exclusively limited to serious crimes set forth in Articles XX to YY in the present convention."*
- Delete, from Article 41, paragraph 3 (a) the phrase *"Each State Party shall consider restricting such a reservation to enable the broadest application of measures on real-time collection of traffic data."* We would like to reiterate that **real-time collection of traffic data** has been determined in some jurisdictions to be a significant invasion of privacy and we believe that the provision, as currently drafted, would be in contradiction to the principles of necessity and proportionality of data collection. For similar reasons, we recommend deleting from Article 41, paragraph 3 (b) the phrase *"Each State Party shall consider restricting such a reservation to enable the broadest application of measures on real-time collection of traffic data and on interception of content data."*
- **Ensure the convention does not contain any provisions that could potentially open the door to expansive claims of extraterritorial jurisdiction.** For instance, we do not believe that offering services in a given country provides sufficient ground for that state to establish jurisdiction over a crime committed elsewhere. To that end, we recommend deleting Article 45, paragraph 1 (b) and Article 40, paragraph 2 (e).
- **Provide clear guidance on which jurisdiction applies for the purposes of investigating and prosecuting crimes covered by the convention**. The convention should not give rise to jurisdictional disputes, but focus on facilitating cooperation. With that in mind we recommend aligning Article 40 with Article 22 of the Budapest Convention, in particular by:
    - Deleting Article 40, paragraph 2, except for subparagraph (b), which should be moved to paragraph 1 and renamed as Article 40 (1) (c).
    - Aligning Article 40, paragraph 5 with the text of Budapest Convention to place emphasis on "*determining the most appropriate jurisdiction for prosecution*" rather than on "*coordinating their actions*".
    - Streamlining the applicability of Article 40 (1), paragraphs (a), (b) and (c) by adding the following phrase at the end of Article 40 (1): "*…save and unless the State in which the offence was allegedly committed refuses to prosecute the national or legal person with reasonable/due expedition*."

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Data Access & Human Rights Safeguards

Microsoft urges states to include robust human rights safeguards throughout the convention to protect end-users from potential abuse of executive authority. We again reiterate that, except in narrow circumstances, the **public has a right to know how, when, and why governments seek access to their data**. There is, in our view, a need to ensure transparency and accountability in the conduct of law enforcement authorities and to ensure notice to impacted individuals, provided that this does not compromise an investigation. 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 ask to:

- **Introduce limitations to ensure the purpose and reach of government access to data remain narrowly tailored** to specific public safety and national security needs. Moreover, 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.
- **Clearly identify the types and categories of data subject to government access** and the specific authorities required to fulfil data safety and national security needs. As we have repeatedly stated, precision in language and framing will facilitate cooperation. Specifically, the convention should not allow for bulk collection of information. Demands should include specific account identifiers and should be limited to seeking data that is necessary and proportionate to the government interest and required for the investigation of each specific case. To this end we propose adding a new paragraph to both Articles 43 and 44 along the lines of: *"Requests under this Article shall be targeted at a specific account, identifier or device. In addition, requests shall only be approved when they are supported by specific evidence that demonstrates criminal conduct and that the data demanded is needed in connection with an investigation of a serious criminal offense covered by this convention. Higher levels of legal order, such as those which are judicially approved, should be required where the request seeks content data."*
- **Introduce a provision to allow technology providers an opportunity to challenge government demands for data on behalf of their customers**, including based on potential conflicts of law. States should be mindful that they do not create conflicts of law with this convention, such as for example, those arising from current provisions related to the real time collection of traffic or content data and existing data protection obligations.
- **Ensure that any data acquisition by governments is only possible upon a receipt of independent judicial authorization** outlining the reasoning fur such request. Law enforcement demands for content and other sensitive user data should be reviewed and approved by an independent judicial authority prior to enforcement of the order, and only after a meaningful minimum legal and factual showing. With that in mind we propose the deletion of phrase "*as appropriate in view of the nature of the procedure or power concerned*" in Article 42, paragraph 2. In addition, we propose strengthening the safeguards referenced in Article 42, paragraph 2, so that it would read reads as follows: "*Such conditions and safeguards shall, ~~as appropriate in view of the nature of the procedure or power concerned,~~ inter alia, include judicial or other independent supervision, grounds justifying application, a meaningful minimum legal and factual showing, and limitation of the scope and the duration of such power or procedure."*
- **Secure a right to redress for any individual and entities whose rights were violated** through the exercise of powers set forth in this convention. We propose inclusion of an additional paragraph under Article 42 along the lines of: *"Such conditions and safeguards shall further include a formal mechanism through which individuals, who believe that their rights may have been violated through the exercise of the powers set forth in this convention, can seek redress for any such violations.*

- **Preserve the right for service providers to give users notice**, especially where doing so does not interfere with or otherwise compromise an ongoing investigation or prosecution. To this end we propose adding subparagraphs (c) and (d) to Article 45, paragraph 1:
    - **Subparagraph (c)**: *"The convention recognises that absent narrow circumstances, users have a right to know when the government requires a service provider to submit information and, unless secrecy is required as outlined in Article 45 (d) below, the service provider shall have a right to notify users."*
    - **Subparagraph (d)**: *"When secrecy is required, the competent authorities shall be required to (1) make their case for secrecy to an independent authority, such as a judge; and (2) present case-specific facts to justify both why the government itself should not be obligated to notify the target and why the government must limit the service provider's right to notify its customers of the request. Any nondisclosure order imposed on a service provider must be narrowly limited in duration and scope and must not constrain the provider's right to speak any more than is necessary to serve law enforcement's demonstrated need for secrecy. Service providers must also be permitted to challenge these orders to ensure that government nondisclosure orders satisfy these requirements."*

Data Retention

The convention should require strict and transparent data minimization and retention and dissemination limits, taking into account that immediate preservation may not always be technically possible. In particular, the convention should **not be used to indefinitely extend retention periods by deferring to domestic laws**. Instead, it should provide a specific limit, as e.g. the Budapest Convention does. In our view, preservation for up to a maximum of ninety days, to enable the competent authorities to seek its disclosure seems appropriate.

With this in mind, we propose that Article 43 (2) is revised: "~~*A State Party may provide for such an order to be subsequently renewed.*~~ *A State Party could request such an order to be subsequently renewed for one further period of 90 days provided that it supplies sufficient reasons for such an extension."*