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

Microsoft

Cybercrime Convention Negotiations

Microsoft's submission to the Third 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 participate in the discussions of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. We believe that this is an important process that can profoundly improve international cooperation on prosecuting cybercrime and are grateful for the opportunity to share our experiences and propose suggestions for a possible path forward.

Our understanding is that the focus of the third session of the Ad Hoc Committee in August/September, will be on international cooperation, technical assistance, preventive measures, and mechanisms of implementation. This submission therefore touches on those areas, supplementing our previous submissions that focused on (a) the process of negotiation, scope and potential objectives of the convention and (b) the preamble and general provisions of the convention and provisions on criminalization, respectively. The summary of our key recommendations is included below:

- **Enhance international cooperation by building on existing instruments.** The convention should encourage effective international cooperation between and among national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime. To do so, it should draw on existing treaties and measures that have already proven to be effective. It should replicate common, well established norms in previous UN Conventions. In particular, it should include options for refusal to extradite, for example on the grounds of dual criminality, when it comes to political offences, and in relation to any request made for the purpose of punishing or persecuting the individual on grounds of their race, religion, gender, or other protected characteristics. In addition, we urge states to ensure that human rights protections are clearly factored in at every step of the process, and that rights to free expression, access to information and privacy are preserved.
- **Focus on combating cybercrime.** The convention should focus on addressing cybercrime and prosecuting cybercriminals rather than on trying to increase resilience through industry regulation. Other instruments, such as development and implementation of appropriate international standards, could be leveraged to that end.
- **Create meaningful mechanisms of implementation by bringing in relevant stakeholders.** For the convention to deliver meaningful outcomes, its provisions must not remain just empty words on paper. As such, it is essential to create and empower mechanisms of implementation. We call on states to draw on existing mechanisms that have been proven to work. Moreover, we urge states to ensure the information and communication industry (ICT) industry has a meaningful role in any implementation mechanisms.
- **Provide a framework for technical assistance.** Countries 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 to empower authorities to prevent and counter cybercrime irrespective of where they are in the world. Moreover, prosecutors need to be flexible enough to adapt to the continuous evolution of criminal tactics. We therefore hope that the convention will provide a framework for training programs in this area, as well as technical assistance that could support its implementation. We would like to reiterate that such assistance should be tailored to the needs of the country in question and that it, likely, needs to be part of an ongoing/systematic process, rather than a one-off/ad-hoc initiative.

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

Microsoft

Provisions on international cooperation

The convention should encourage effective international cooperation between and among national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime. It should draw on existing treaties and measures that have already proven to be effective. Moreover, it should include options for refusal on the grounds of dual criminality, refusal in respect of political offences, and refusal of a request made for the purpose of punishing or persecuting the individual on grounds of their race, religion, gender, or other protected characteristics. Moreover, we urge states to ensure that human rights protections are clearly factored in at every step of the process, and that rights to free expression, access to information and privacy are preserved in line with certain minimum standards of proportionality and necessity. With this in mind, we recommend:

- **Allow access to digital information only pursuant to lawful process with appropriate safeguards.** Any framework regulating a government's ability to access digital information stored with technology providers must begin by recognizing the general principle that all access should be pursuant to the rule of law. Principles surrounding lawful access to digital information are well established under existing legal instruments. At a minimum, lawful access should be predicated on independent judicial authorization, notice to the user, orders which are strictly necessary and proportionate to stated aims and some 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.
- The convention's provisions should be **aligned with the Budapest Convention**[1] and the 2nd Additional Protocol, which are among the most widely referenced international legal instruments in this area. The latter notes that parties will cooperate "for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence." Such alignment will result in an approach that is well-established among many stakeholders.
- **Avoid establishing conflicting rules that raise barriers international criminal cooperation.** In a world where data flows are global, the risk of conflicting national rules is substantial. Because compliance costs from conflicting rules are enormous, governments should ensure that legislation provides maximum flexibility and creates the least risk of conflict. Examples of these types of policy issues include, data localization or access laws, data retention laws and data protection laws. Microsoft frequently has to deal with situations where one country's laws can create significant conflict when responding to lawful demands around the world.
- **Modernize rules governing appropriate targets of requests for cloud data.** With more and more public and private organizations moving their digital information to the cloud and many companies using cloud-based infrastructure to deliver applications and services to customers, governments often have multiple sources for the digital information they seek. Whenever possible, digital evidence should be obtained from the company most directly offering the service to customers. In many cases this will not be the cloud provider. Going directly to the company that is the data controller (usually the customer or consumer) can often be done without jeopardizing an investigation, just as it was done before the organization moved its data to the cloud.
- More generally, the convention's provisions on international cooperation **should not be overly state-centric**. For example, it would be inappropriate for the convention to (a) let states reject cooperation on the grounds of state security or sovereignty – while (b) forbidding rejection on the grounds of political retribution or human rights-abusing behavior. Furthermore, the convention should not

[1] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

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

Microsoft

introduce any provisions that undermine the **"principle of specialty",** specifying that one can only be charged for the crime(s) for which one was extradited.

- The convention should also **avoid noting specific channels** (e.g., specific law enforcement agencies) for parties to use when they make and respond to requests for international cooperation.
- In discussing the **expedited preservation of information**, the convention should draw from the good practices established by the Budapest Convention. For example, Article 29(2) of the Budapest Convention articulates the requirements for requesting expedited information. These requirements include that the request must specify "the offence that is the subject of a criminal investigation of proceedings." Additionally, the convention should not place sovereignty over human rights, including when creating bases for refusing requests for expedited reservation.
- The lack of modernized laws and international frameworks for accessing digital evidence and the increase in unilateral actions by law enforcement agencies to seize information stored outside their border threaten to erode consumer trust and are creating difficult legal situations for companies that provide cloud services. Therefore, when discussing **access to data**, the convention should draw from the Budapest Convention, which allows a party *without* the authorization of the other party to (in sum): (a) access publicly available computer data regardless of where it is located (including the territory of another state party); or (b) access or receive data on systems in its territory that was originally located in another party *if* the party has the consent of a person with lawful authority to disclose it.
- When discussing personal data protection, it would be important for the convention to include a reference to the state party transmitting personal data in compliance with **domestic and international legal obligations regarding the protection of personal data**.
- When addressing mutual assistance regarding the **real-time collection of information**, the convention should be careful not to create overly broad, unnecessarily mandatory, and intrusive provisions. The convention should invoke principles of proportionality and necessity to ensure it does not (a) ignore the particularly intrusive nature of real-time surveillance; and (b) represent a significant expansion of terms used in current mutual legal assistance treaties (MLATs). The convention should also create a right of refusal to cooperate, in particular when the protection of human rights might be at stake.
- Furthermore, on **mutual legal assistance**, the convention should draw from Article 25(4) of the Budapest Convention which, among other things, states that a party cannot refuse cooperation on the grounds "that the request concerns an offence which it considers a fiscal offence."
- **Authorize disclosure in emergencies.** Although governments should only be permitted to access digital information stored in the cloud through lawful process, narrow exceptions may be appropriate for emergency situations, such as when the provider has a reasonable, good faith basis to believe that access is needed to avoid death or serious physical injury. Such an exception can be especially crucial when law enforcement agencies face an ongoing emergency. Such a provision would reflect the current real world practice, which exists in major technology providers.
- Any provisions regarding the **investigation** of offenses should contain references to international human rights law. Similarly, any provisions regarding recovering criminally obtained **property** must be strongly constrained by the parties' human rights obligations, and should contain appropriate grounds for refusal, such as those articulated in Articles 25(4)-(5) and 27(4)-(5) of the Budapest Convention.
- Finally, we recommend considering a provision calling out **jurisdictions harboring cybercriminals**. Where there is an indictment supported by evidence acquired through legal process, subject to the protections outlined in this document, individuals engaged in cybercrime should be subject to formal international extradition proceedings.

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

Microsoft

Provisions on preventive measures

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

However, we believe what the convention should focus on dealing with cybercrime and cybercriminals. It should not focus on increasing the overall societal resilience in cyberspace. Other instruments, such as development and implementation of international standards, could be leveraged to that end. As such, we recommend the following:

- The convention should **not seek to introduce industry regulation**. It should instead focus on public authorities and empowering them to prosecute cybercrime.
- States have focused on developing frameworks and legislative approaches aimed at increasing the cybersecurity and cyber resilience of the online environment **in non-criminal contexts** and this separation should remain.
- Moreover, the convention should **not seek to develop or encourage the adoption** of any principles and standards, as those are typically voluntary, and dealt with in other mechanisms.
- Finally, and once again referencing our previous positions, we would like to note that a convention that focuses on cyber-dependent crimes that are serious, have criminal intent, and are defined similarly across jurisdictions has the most **potential of becoming ratified and used in practice**. This in itself can be an effective preventive tool.

Provisions on technical assistance

Cybercrime knows no borders. An effective response must enable the international community of states to effectively work together. Moreover, the convention should provide a framework for capacity building to enable effective investigation and prosecution of cybercrime globally. 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 to empower authorities to prevent and counter cybercrime irrespective of where they are in the world. We therefore hope that the convention will provide a framework for training programs in this area, as well as technical assistance that could support its implementation. We would like to reiterate that such assistance should be tailored to the needs of the country in question and that it needs to be part of an ongoing/systematic process. With this in mind, Microsoft recommends the following:

- The convention should 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, free expression, as well as relevant data protection laws. Similarly, any evaluations, studies and research called for by the convention should be expanded to include respect and protection of international human rights and data protection.
- The convention should focus on technical assistance that is **technology-neutral**, and affirm its provision on a voluntary basis only, rather than mandating any forms of technology transfers. Intellectual property rights of any products and services leveraged require appropriate protections to facilitate public-private cooperation in combatting ICT crimes.
- Microsoft could imagine a role for the United Nations Office on Drugs and Crime (UNODC), in facilitating specialized assistance to states parties promoting the implementation of programs related to the convention. As noted in Microsoft's Submission to the Second Session of the Ad Hoc Committee, however, it is important that such programs focus their attention on cyber-dependent crimes, rather than crimes where a computer merely was involved in the planning or execution of the crime.

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

- Data gathered and analyses conducted regarding **cybercrime trends should be made available as widely and transparently as possible**, including to industry, technical experts, civil society, and academia, as appropriate. Previous experience of cybercrime prosecutors and investigators has shown that when useful information is stored behind access approved databases that it becomes a barrier to widespread take up of such initiatives. Such types of multistakeholder inclusion – which the convention should explicitly call for – will help develop a robust, whole-of-society understanding of the threat landscape and of how to respond it. It will also help foster an understanding that can keep pace with the threat landscape's rapid and often unpredictable evolution.

Provisions on mechanisms of implementation

Microsoft recognizes that for the convention to deliver meaningful 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 been proven to work. Moreover, we urge states to ensure the ICT industry has a meaningful role in any implementation mechanisms. Specifically, Microsoft recommends:

- Microsoft believes there should be some **"treaty body"** (e.g., a Conference of the Parties or Meeting of the Parties) to oversee the operation and effectiveness of the convention. Given the role the technology industry has in this space, Microsoft believes it would be appropriate for the convention to explicitly affirm a meaningful role for ICT companies in meetings of the Conference of the Parties. 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.
- The convention should delimit **particular roles and responsibilities for any treaty body**. At the same time, it will be important not to constrain the body from performing future unforeseen functions necessary to ensure the convention's effective operation in line with its object and purpose. To do this, the convention could include at least some sort of open-ended authorization such as empowering it to "engage in any other appropriate actions for the achievement of the objective of the convention in the light of experience gained in its implementation."
- 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 other treaty commitments with those assumed under the present convention.
- Overall, deliberations, including any convenings to improve capacity and collaboration among states, should include technical experts from the ICT industry or the broader **multistakeholder community, as appropriate**. While we urge states to ensure that the convention is future-proofed and any definitions are technology neutral, we recognize that this is a fast-evolving environment. The creation of e.g., an expert forum that would allow states and participants from technical communities and industry to exchange views on the latest threats and potential mitigations would add to the security and stability of the online environment.