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

Cybercrime Convention Negotiations

Microsoft's submission to the Second 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 and we are looking forward to more in-depth conversations at the upcoming intersessional. We believe that this is an important process that can profoundly improve international cooperation on prosecuting cybercrime and are grateful to be able to highlight our experiences and put forward suggestions for a possible path forward.

Our understanding is that the focus of the intersessional, as well as the second session of the Ad Hoc Committee in May, will be on the preamble and general provisions of the convention and provisions on criminalization. The current submission therefore focuses on those areas, supplementing our original submission that focused on the process of negotiation, scope and potential objectives of the convention.

At the outset, it is nevertheless worth repeating in this context, that Microsoft believes that these negotiations will only be successful, and any resulting convention only effective, if its scope is narrowly defined and agreed by consensus. Acts of cybercrime, more often than not, cross borders and therefore international cooperation is at the core of effective prosecution. However, this kind of cooperation requires that the offences are commonly understood and recognized by all parties involved. With that in mind, we encourage states to:

- Not expand the definition of cybercrime in a new treaty merely because a computer was involved in the planning or execution of the crime. The new convention should only include illegal activity that is cyber enabled and the offenses that are of such scale, scope, or speed that they would not be feasible without ICTs – and where the definitions are commonly understood, for example as it relates to online child sexual exploitation.
- 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 also contribute to streamlining the processes and procedures.
- Not duplicate offences that are covered by other legal instruments, such as corruption, trafficking or terrorism simply because these may be complemented using technology. Such an approach risks contradiction and confusion and will not deliver a targeted, practical instrument that can improve our collective ability to tackle cybercrime.
- While Microsoft appreciates the need to address novel and emerging forms of cybercrime, we call on states to ensure that the text is technology neutral.
- Moreover, we urge caution where the definition of cybercrime is expanded to include computer-enabled dissemination of information or those that are focused on online content, given some of the particular human rights challenges that content-related crimes can and have raised in other contexts. States should specifically avoid any commitments that would result in preventive content take downs.

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

The preamble and general provisions of the convention

Microsoft recommends leveraging the Chair's proposal on the scope and objectives of the convention, which was discussed as part of the First Session and received relatively broad support from the various states, to draft an initial preamble and general provision sections of the convention. Having said that, we would nevertheless, like to see these sections include the following:

- Much more robust references to **human rights, data protection laws, and the right to privacy**, in line with the references in in the Council of Europe Convention on Cybercrime[1] (the Budapest Convention). This means recognizing protection of human rights as a rule rather than principle, and ideally referencing other relevant international mechanisms, such as the International Covenant on Civil and Political Rights (ICCPR)[2].
- Relatedly, given the divergent interpretations of some of the issues at stake in the convention, we recommend the text be as precise as possible. For example, if the convention were to demand compliance with the principles of international law, we would recommend that it lists the **particular international legal instruments it seeks to invoke**. This would ensure that the convention would not inadvertently give certain states an opportunity to pick-and choose, or potentially even exclude a specific rule of international law they do not accept.
- Furthermore, we believe **that protection of sovereignty** should not be one of the main objectives of the convention as currently envisioned. Instead, the focus of the convention should be on enabling international collaboration between states in prosecuting what is by its very nature a transnational challenge. Extending sovereignty protection would in fact be counterproductive, as well as potentially inconsistent with existing international law frameworks on prescriptive jurisdiction, which allow states to exercise jurisdiction over their nationals abroad or activities of foreign nationals in foreign states that have "effects" within the state exercising jurisdiction. Moreover, in case the convention does end up containing specific references to the principle of sovereignty, we call on states to ensure that corresponding references are included to extend the relevant legal obligations of states.
- Finally, and more fundamentally, in discussing sovereignty, the convention should adopt a human-centric approach. The concept should not be used to expand law enforcement authority in ways that could negatively impact democratic freedoms.

As highlighted in the introductory section, Microsoft believes that the scope of the convention should be narrow/focused, as cooperation between states will only be effective where the offences included in the convention are commonly understood by all. With that in mind, we encourage states to be precise when drafting the general provisions and specific definitions and rely on established frameworks for consistency:

- Microsoft recommends that the terms and provisions used throughout the convention **be aligned with established and agreed upon definitions**, particularly those included in the Budapest Convention, as one of the most widely referenced statutes in this area. Moreover, we recommend that states only begin discussing the definition of terms once it has been agreed that the terms will in fact be used in the text of the actual convention, rather than up front.
- Furthermore, the convention should use terms in a **consistent** manner, and different parts of the text should not contradict each other. Relatedly, to avoid confusion, different terms should not be used

[1] Budapest Convention

[2] OHCHR | International Covenant on Civil and Political Rights

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

Microsoft

interchangeably, unless the convention explicitly notes their interchangeability. And we recommend **clearly defined terms** (e.g., avoid the unqualified use of terms such as "wrongful" and "lawful").

- When discussing activities excepted from the convention's scope (i.e., activities lawful under the treaty/convention), these **should be worded carefully and with precision**. For example, an exception described merely as the "lawful" version of an activity (e.g., "lawful [activity's name]") could be overly broad, because it would be unclear whose law is being invoked. Conversely, an exception that merely lists examples of permissible activities could be overly narrow; it should instead explain what the examples represent – much as the Budapest Convention does in Article 6, regarding the misuse of devices.
- Further, the convention should **not contain language that may force all relevant transnational law enforcement on cybercrime to use the treaty's/convention's mechanisms exclusively**. That could undermine existing mechanisms that currently function well and pose practical problems in urgent cases.

Provisions on criminalization

Similarly, when it comes to provisions on criminalization, we believe the convention will be most effective, if the scope is limited and definitions precise. For example, we recommend that:

- In line with what we have previously argued, the convention should criminalize only substantive offences that are **cyber-dependent**. We would recommend that the provisions on criminalization be aligned with those in the Budapest Convention and include offenses against the confidentiality, integrity, and availability of computer data and systems. Examples include access, interception, data and systems interference, and misuse of devices. A focus on serious crime only will also contribute to streamlining the processes and procedures.

  Moreover, and as highlighted above, we also believe that the definitions used need to be narrowly defined. For example, when discussing **interception**, the convention should retain the Budapest Convention limitation to "non-public transmissions" – this allows information not intended to be private to flow freely.
- When criminalizing various actions, the convention should explicitly mention **intentionality** for each action as appropriate. For example, we encourage states to ensure that security and vulnerability research and disclosure, when appropriately coordinated with affected vendors and relevant authorities, are not criminalized by the convention, since that would have the opposite effect and make the cyber ecosystem less secure, rather than more secure.
- The convention **should not treat traditional crimes as cybercrime** merely because a computer was involved in the planning or execution of the crime. These types of crimes are already adequately covered by existing instruments. The new convention should only include illegal activity that is cyber enabled and the offenses that are of the scale, scope, or speed that they would not be feasible without ICTs. It is important to remember that these types of activities can and are covered by other statutes. For example, terrorism-related offenses, arms trafficking, or counterfeit medical products should not be addressed by this new treaties as these activities are already **covered by other existing treaties**. Including these topics risks contradiction and confusion and will not deliver a targeted, practical instrument that can improve our collective ability to tackle cybercrime.
- The convention should not attempt to **regulate content**, given the different legal practices and cultural approaches to this area across the world. States should specifically avoid any commitments that would result in preventive content take downs, in particular if these could lead to hampering journalistic freedom or harming freedom of expression.

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

- Given the different levels of readiness of countries around the world, the convention should focus on public authorities and prosecution of cybercrime, and **not introduce industry regulation**. Other means of regulating industry exist, and these should not be conflated with the new cybercrime convention. Looking at the big picture, 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.

Provisions related to procedural measures and law enforcement

A new convention provides an opportunity for greater collaboration between governments and the private sector in matters related to lawful data access. This is especially the case for cloud service providers. Microsoft believes that states should use this opportunity to recognize the need to advance both public safety interests and fundamental privacy rights while resolving conflicts of laws, jurisdictional and sovereignty issues. Against that background, we recommend that:

- The purpose and reach of government access to data be **narrowly tailored** to meet specific public safety and national security needs.
- Any new convention clearly identifies the types and categories of data subject to government access and the specific authorities required to fulfil data safety and national security needs. The convention should incorporate appropriate safeguards to ensure robust **independent oversight** and **effective redress** mechanisms and should emphasize the importance of **minimizing conflicts of law** and creating mechanisms to resolve conflicts that do arise.
- The convention allows technology providers an opportunity to **challenge government demands** for data on behalf of their customers, including based on potential conflicts of law, to ensure that governments are acting within the law and are respecting the rights of the providers and their users.
- The convention requires strict and transparent data minimization and retention and dissemination limits. When addressing **preservation of information**, the convention should account for the fact that immediate preservation may not always be technically possible. Additionally, the convention should not be used to indefinitely extend retention periods by deferring to domestic laws. Instead, it should provide a specific limit, as the Budapest Convention does (ninety-day limit).
- The convention reflects that, absent narrow circumstances, the public has a right to know how, when, and why governments seek access to their data. There is a need to **ensure transparency** in the conduct of law enforcement authorities and to ensure notice to impacted individuals, provided that does not compromise an investigation. Overall, however, secrecy should be the exception rather than the rule because otherwise users are unable to assert their rights and privileges and trust in the online ecosystem as well as in the rule of law is undermined.
- 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.
- Recognize that international cooperation (addressed in the coming sessions) is critical to effective cybercrime prosecution. Therefore, the convention should not contain language that could potentially open the door to expansive claims of **extraterritorial jurisdiction** and subsequent demands for data that would be in tension with existing legal obligations (e.g., blocking statutes) or that would prevent/hinder effective international cooperation.

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

We hope these recommendations provide a helpful contribution to advance a shared objective: achieving a rules-based and rights-respecting online world for all. We strongly believe that this convention – as well as any convention related to threats emanating from cyberspace – should endeavour to protect people from such threats, rather than place undue restrictions on people, in particular with regard to their human rights. More than anything else, we believe accomplishing this requires trust and cooperation across stakeholder groups with responsibilities in this space.

We stand ready to provide any additional input or clarify any of the contributions provided here and we look forward to additional opportunities to collaborate in the future.