Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Cybercrime Convention Negotiations

Microsoft's submission to the Seventh Reconvened 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 remains grateful for the opportunity to contribute to the Ad Hoc Committee (AHC) efforts to develop a Cybercrime Convention. Clearly, a more effective international cooperation framework against cybercriminal activity could be beneficial. Cybercrime remains a growing problem, set to cost the world trillions of dollars each year. Therefore, the intended purpose of a new UN Convention on Cybercrime should be to aid the international community to fight the scourge of cybercrime.

However, Microsoft continues to remain gravely concerned with the revised draft text. We are disappointed that many key concerns, that we and other industry and civil society entities shared with member states throughout the nearly three years of this process, have not been addressed. In fact, several of the already harmful provisions are now broader, limitations on the scope have been removed, and human rights articles weakened.

After nearly three years of negotiations and with only one session remaining, states have not yet reached consensus on some of the most fundamental issues, including the very purpose and scope of the Convention. Additional provisions are also included calling on immediate Protocol negotiations to, *inter alia*, further broaden the scope of the convention. To be clear, failure to agree that cybercrime – and not the misuse of technology in general – is the objective of this treaty would inevitably create legal uncertainty and encourage abuse of its provisions. Additionally, the broad scope would make this the broadest multilateral crime treaty ever adopted.

We urge states to use the "final final" session to clearly and narrowly define the scope of this treaty, and significantly improve safeguards throughout the Convention. In its current form, this treaty will erode data privacy, threaten digital sovereignty, and undermine online rights and freedoms globally.

There is still time for states to negotiate a favorable outcome – but a fundamental change of course is needed. We continue to strongly believe that *no* outcome is better than a *bad* outcome.

Below, we outline major concerns and provide suggestions for a course correction on this draft text. Importantly, the proposals below represent the *minimum necessary changes*.

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

1. **The draft Convention will undermine national security because the current draft text allows for unauthorized disclosure of sensitive data and classified information to third states.**

The treaty does not yet have a defined scope and allows for clandestine access to secured systems, secret real-time surveillance, in perpetual secrecy, coupled with inadequate safeguards. While surveillance and intelligence collecting are part of the national security activities of states, this should not be supported and, *de facto* blessed, by a UN treaty under the guise of combating cybercrime. Disclosure or real-time surveillance concerning traffic data of third-state nationals, such as an individual's location, could place government employees and national security at risk, especially at times when geopolitical tensions are high. While the latest draft makes these articles optional the door is still wide open for abuse and should be deleted.

Additionally, Article 28.4 permits an IT professional from one state or any other individual with *"knowledge about the functioning of the system in question"*, while traveling in another state, to be compelled to provide necessary information for conducting searches and seizures of computer systems. This provision can – and will – be abused to force individuals with knowledge to reveal proprietary or sensitive information. Handing over such information could expose the critical infrastructure of a state to cyberattacks or the theft of state secrets, which should give all negotiators in this treaty process pause.

States must reconsider secrecy and safeguards provisions. Transparency is required to protect both individuals and national security. Apart from safeguards proposed elsewhere in this document the objective of this treaty is to fight cybercrime. Therefore, states should be required to notify third states whenever e-evidence is requested on residents or data located therein. Furthermore, states should delete the most intrusive provisions, such as those on real-time surveillance and access to ICT systems, where even retroactive notification alone cannot mitigate national security risks.

In addition, global surveillance laws may lead to conflicts of law and challenges to digital sovereignty. None of this has been adequately addressed by the draft text, which is silent on any proposed resolution mechanisms for such conflicts.

Minimum Necessary Changes:

- Delete Articles 29 and 30 on real-time surveillance and all related references.
- Delete Article 28.4.
- Introduce an additional provision to require advance notification of a third-state party whenever data is requested on a person domiciled, or data located, in its territory.

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

2. The draft Convention will weaken human rights online and will put individuals at greater risk of being prosecuted for exercising their digital rights.

Microsoft continues to strongly oppose a Convention that would apply to an undefined and unlimited list of activities that leverage digital technology. As we have previously stated, a cybercrime convention should apply to crimes unique to cyberspace and not cover any crime simply because it has an ICT element. The scope of this treaty remains too broad. Applying this Convention to other offences *without defining those offences* would effectively override the applicability of existing international human rights online, paving the way for abuse by authoritarian regimes to increase online censorship, preventive content take-downs, and government surveillance with minimal guardrails.

We welcome that the Canadian and New Zealand safeguard proposals have been included in the new draft, which we strongly support. We again call on states to use this final session to negotiate a targeted instrument focused on cyber-dependent offences where international consensus already exists. We must protect individuals, including political dissidents, human rights defenders, journalists, regime critics, and minorities from extraterritorial surveillance in secret, where they could be extradited, and prosecuted.

The latest version of the text has made several human rights safeguards subject to domestic legislation which can vastly weaken their effectiveness, as national laws vary significantly and many of them simply will not provide adequate human rights protections. One example is how this treaty makes procedural conditions and safeguards optional under Article 24.1. This safeguards article, drawn from the Budapest Convention, has been significantly weakened by including the clause "under its domestic law," without providing clarity which specific obligations shall be included, as Budapest does, except for a vague reference to states' "obligations under international human rights law." Without at least some specific human rights references, it makes it easy for states to claim compliance without any verifiable means for other states to contest that position. If Article 60 remains as written and supplants Article 15 in the Budapest Convention, it might also weaken the existing safeguards in the Budapest Convention. The new Convention should not become a way for states to appear in line with international human rights law, when they have no obligations to do so.

Minimum Necessary Changes:

- Amend Article 3 in the "advanced draft" to ensure the Convention applies only to offences established in accordance with articles 7 to 17 of this Convention.
- Amend Article 23 to limit the scope of procedural measures only to offences in articles 7 to 17.

- Amend Article 24.1 to include specific references to which obligations under international human rights law shall apply and include the principles of legality, necessity, proportionality, and non-discrimination.
- Amend Article 35 to limit the scope of international cooperation measures to Article 7 to 17 only (including by deleting references to other serious crimes, e-evidence gathering for any crime).
- Remove qualifiers of "in line with domestic legislation," from Articles 24.1, 33, 54(3)(e), 54 (3) (h).
- Remove all references to "the use of information and communications technologies for criminal purposes" and un-bracket "cybercrime."

3. **The draft Convention will weaken global cybersecurity by compromising critical security measures and criminalizing practices that secure the digital ecosystem.**

Today, legitimate cybersecurity solutions include innovative and highly advanced practices that provide a crucial line of defense against the constantly evolving threats of cybercrime. The world greatly benefits from these practices – work conducted by security researchers, penetration testers and ethical hackers who have a crucial role in securing information technology systems. Recognizing their importance, some states have recently legalized ethical hacking through dedicated legislation. The current convention provides no meaningful protection for these individuals, and we strongly recommend including language that explicitly exempts individuals engaged in lawful cybersecurity practices from its scope.

The Convention criminalizes, without exception, any unauthorized access to a computer system. This will inevitably lead to prosecution of good faith cybersecurity researchers. This is not a hypothetical. We already see cybersecurity practitioners aggressively targeted, including for responsibly identifying security flaws. The vague provision, Article 53(3)(e) (on 'preventive measures'), would have no impact on the interpretation of the criminalization articles on cybersecurity researchers. These professionals are critical to helping secure systems used by billions of people every day. If this is not fixed, this Convention will undermine global efforts to secure systems from cyber criminals, systems that global users rely on daily.

Article 28(4), discussed above, is problematic from a cybersecurity perspective. It allows any state – including states who have conducted cyberattacks against critical infrastructure – to compel a company or government agency employee with special knowledge of a computer system to hand over e.g. access credentials and other sensitive information to third states, all in secret, forever.

A UN treaty that undermines cybersecurity for everyone, makes cybercriminals' jobs easier, and compromises online trust and safety should be unacceptable for the international community of states.

Minimum Necessary Changes:

- Delete Article 28.4.
- Add a 'criminal intent' (mens rea) requirement to all relevant articles in the criminalization Chapter, Articles 7-17.
- Change "may" to "shall" in Articles 7(2) and 8(2).
- Strengthen 53 (e) on cybersecurity researchers, removing "in line with domestic legislation as a qualifier."

4. **Additional Protocols open the door to further broadening of the scope and prove that positions among member states are still too far apart from reaching consensus on key issues.**

The Convention must be narrowly and clearly defined to achieve its intention – to increase international cooperation to combat cybercrime. There remains much work to be done to narrowly define the scope of this treaty. We are strongly opposed to Article 61 on additional protocols to this Convention and the language in the draft General Assembly resolution which calls for two sessions to negotiate a draft protocol.

Adding a provision on Protocols for additional cybercrimes to be covered, before the scope of the Convention is agreed upon is an inadequate compromise on the scope of the Convention itself and suggests that member states are too far apart to reasonably deliver a useful new cybercrime treaty today.

Including Protocol negotiations, for undebated and undefined additional crimes, immediately after the end of the AHC, as proposed in the draft UNGA resolution, broadens the already overly broad scope of the convention. Protocol negotiations should not be used to attempt to fix the scope of the convention itself.

If Protocols are to be added to this Convention, the scope of the Convention must be narrowly defined. This can only be achieved if they are debated by the full AHC, and the same rules of procedure continue to apply to Protocol negotiations. The last time a crime convention was negotiated - the UN Treaty against Transnational Organized Crime (UNTOC) - it did in fact include Protocols. However, there are significant differences between the UNTOC AHC and the current AHC on cybercrime which include, but are not limited to, the following: 1) the Protocols in the UNTOC had been standalone ideas promoted by member states and civil society for years before the UNTOC AHC began its work; 2) the General Assembly mandated protocols were elaborated as part of the UNTOC AHC's work; 3) the Protocols themselves were negotiated alongside the UNTOC and draft protocols tabled before the AHC opened its first negotiating session; 4) two of the three Protocols were adopted at the same time as the UNTOC, with one extra session for the firearms protocol to be negotiated. In the instance of the AHC on cybercrime, not one of these

four situations is present. Therefore, we strongly recommend the deletion of Article 61 and the corresponding provision 57(g).

Minimum Necessary Changes:

- Delete Article 61.
- Delete Provision 57 (g).

As member states enter the "final final" negotiating session of the Ad Hoc Committee on cybercrime, it is clear that they remain divided over fundamental components of this convention – including the very purpose and scope of the convention itself.

It is our hope that, ahead of this last session, member states recognize the severe flaws that still exist, raised by civil society and industry alike throughout the almost three years of negotiations. A treaty focused on core cybercrime offences with robust safeguards and clear intent requirements would be a useful outcome. The current draft of this convention is not that treaty. If adopted in its current form this treaty would make cyberspace less secure, erode data privacy, and severely threaten online rights and freedoms globally.

It is not too late for member states to make significant changes to the revised text. That said, in its current form, we cannot support member states signing or ratifying this convention. The Budapest Convention has 75 parties, with 18 invited to accede, a functioning cybercrime convention already exists. Encouraging more states to accede to the Budapest Convention would avoid duplication between the two conventions and prevent the harmful impacts of a flawed convention. If significant improvements cannot be made, it would be better to have no new convention than for the UN to adopt a harmful one.