Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft's Presentation at the Panel Titled:
A Concerted Effort: The Role of the Private Sector in the context of the chapter on criminalization and procedural measures and law enforcement
Deliver by Nemanja Malisevic, Senior Director, Digital Diplomacy, Microsoft

Third intersessional consultation of the Ad Hoc Committee on Cybercrime
Friday, 4 November 2022

Madame Chair, Excellencies, Distinguished colleagues,

At the outset, allow me to reiterate Microsoft's appreciation that the multistakeholder community can meaningfully contribute to the discussions of the Ad Hoc Committee. Frankly, the AHC's inclusiveness should serve as an inspiration and precedent for other UN cyber-related discussions.

As it happens, later today, Microsoft will publish its annual Digital Defense Report. The conclusions of the report are sobering. The past year has seen a burgeoning cybercrime economy and a rapid rise of cybercrime services – many of which are targeting even the most essential of public services. We have seen the cyberattack landscape become increasingly sophisticated as cybercriminals continue, and even escalate, their activity in times of crisis.

Against this backdrop, finding a way to effectively prosecute and deter cybercriminals is paramount – and it is, of course, here that the work of the Ad-Hoc Committee comes in. And it is one of the reasons this work is so important and timely. With that in mind, allow me some high-level remarks on "*The Role of the Private Sector in the context of the chapter on criminalization and procedural measures and law enforcement*."

The ongoing negotiations within this Ad Hoc Committee provide a unique opportunity. But we should also remind ourselves that much is at stake. Should states fail to agree a UN cybercrime treaty by consensus to ensure the broadest possible buy-in, the outcome may well lead to a weakening of existing data protection and cybersecurity practices. It could undermine human rights, erode trust between states and among states and other stakeholders. In short, this would make the situation worse, not better.

To avoid such scenario, we continue to urge states to focus international efforts on addressing core cybercrime offences where international consensus can be reached.

As such, the future treaty should combat cybercrime by facilitating international cooperation while protecting, rather than undermining 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 include appropriate safeguards to ensure robust independent oversight and effective redress mechanisms. And it should minimize and avoid conflicts with existing laws, create mechanisms to prevent conflicts, and resolve disputes that arise.

To ensure a clear scope, all provisions of the treaty, including procedural and law enforcement measures should relate to a precisely defined set of crimes covered by the convention. Similarly, the treaty should

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

remain an instrument of public international law focusing on facilitating cooperation among public authorities to effectively prosecute and investigate cybercrime with cross-border components.

We would like to reiterate that for the convention to remain an effective criminal justice instrument, it should not seek to introduce industry regulation, data and consumer protection or liability measures. Such provisions would likely come into conflict with existing laws and would at any rate fall outside the scope of the criminal justice domain. Against this background, we recommend carefully evaluating each proposed provision to assess whether it, in fact, primarily targets public authorities or other, non-governmental entities.

Going forward, the technology industry, and service providers in particular, will have to have a clear understanding of what constitutes an act of cybercrime to respond appropriately to government requests for information. As we and other stakeholders have repeatedly stated, 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 the crime.

We would also encourage states to put emphasis on "criminal intent" as a prerequisite for establishing crimes under this convention. We have previously highlighted the importance of adequately protecting, *inter alia*, security researchers or penetration testers, who perform essential work to continuously test and improve cyber defences.

Establishing dual criminality for crimes under the future cybercrime convention will be equally important, both for states as well as service providers, who need to understand the instances in which states can be expected to legally request information. In this context, we would also like to caution against introducing via this convention new definitions of widely applied criminal justice concepts, such as, *inter alia*, obstruction of justice, liability, and negligence. These types of acts may not always imply criminal responsibility and are not limited to cybercrime or to the online environment as such.

Where it is necessary to establish dual criminality, the future convention should also leverage agreed language as much as possible. Existing instruments, such as the UN Convention on Transnational Organized Crime (UNTOC), UN Convention Against Corruption (UNCAC), and other widely accepted instruments such as the Budapest Convention can provide guidance and help in this regard. We would therefore recommend the exact text of these conventions to be used whenever possible since such provisions have already been transposed into national legislation 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.

Importantly, we would urge caution where the definition of cybercrime is expanded to include computer-enabled dissemination of information or provisions that are focused on online content. We believe that the convention should not attempt to regulate content, given the different legal practices and cultural approaches to this area across the world.

For the reasons just mentioned, we would also urge states to use precise terminology, throughout the convention. This would include criminalizing serious cybercrime offences where "*clear criminal intent*" can be established. To follow up on a point I previously made, using precise language like this would also prevent the inadvertent criminalization of, for example, penetration testing.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

We recognise that international cooperation is critical to effective cybercrime prosecution. However, to safeguard end-users against potential abuse of executive authority, the scope of application of all procedural measures set forth in a future treaty should be limited to crimes set forth in the convention. We would in particular recommend this section to refer to specific articles in the criminalization section.

We would also like to reiterate that the convention should not contain any provisions that could potentially open the door to expansive claims of extraterritorial jurisdiction, such as establishing jurisdiction over a service provider merely because of offered services. The same applies to potential demands for data that would conflict with existing legal obligations (e.g., blocking statutes) or that would prevent/hinder effective international cooperation. To protect rights of end-users, purpose and reach of government access to data needs to be narrowly tailored to meet specific public safety and national security needs.

Moreover, the convention should allow technology providers an opportunity to challenge government demands for data on behalf of their customers, including based on potential conflicts of law – for example, potential conflicts between provisions related to the real time collection of traffic or content data need to be evaluated against existing data protection obligations (including the GDPR).

To ensure respect for human rights, in particular the principles of necessity, legality, and proportionality, we also urge states to include a provision to condition any data intercepts upon a receipt of independent judicial authorization outlining reasoning for such requests. Furthermore, the convention should also include the right to redress for any individual whose rights were violated through the exercise of powers set forth in this convention. Except for very specific and narrow circumstances, the public has a right to know how, when, and why governments seek access to their data. Overall, secrecy should be the exception rather than the rule.

We suggest that greater transparency would be appropriate, by, for example, preserving the right for service providers to give users notice and preserving the rights of those users to object to certain uses or disclosures of their data especially where doing so does not interfere with or otherwise compromise an ongoing investigation or prosecution.

Importantly, 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.

Last but certainly not least, 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. For example, preservation for up to a maximum of ninety days, to enable the competent authorities to seek its disclosure seems appropriate as the baseline.

In the interest of time, I will leave it at this. And I would like to align our position with that of the International Chamber of Commerce UK. Looking ahead, we intend to submit a much more detailed position ahead of the next substantive session in January.

Thank you, Madame Chair.