Intervention on Criminalisation: Fourth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes

Chair, Excellencies, distinguished delegates, our thanks to the Chair and her team and the Secretariat for their support of our deliberations and we wish all a happy new year.

We support the statements made by ICC as a whole, and Microsoft and we highlight our written statement for the fourth session posted on this session's webpage; our written submission has detailed proposals regarding the text as well.

We agree with many delegations that the focus of this Convention should be addressing cyber dependent crime. We also urge that it should focus on serious crimes. This Convention will be seen as a failure if it does not have a meaningful impact on reducing the incidences of, and impact of, serious cybercrime. **Offences that should be included in the Convention are those in Articles 6-10 and the concepts in 16,** with amendments**.**

All offences should require criminal or malicious intent and not intent alone. We have heard the debate at this session on this threshold question, Madame Chair. The question before us is should the text require criminal, malicious, or dishonest intent, or simply require that offences are "without right" or "without authorisation" or at times based upon an evaluation of honesty?

There are many good reasons why criminal or malicious intent is not just the right approach, but of critical importance and not just to global businesses.

- This is a crime treaty, so it goes without saying that it should address criminal acts, and the clearer the focus is on criminal acts the more successful the convention will be. In that vein, using "dishonest" would be vague and harder to evaluate.
- Using criminal or malicious intent will make a finding of dual criminality simpler given that the fundamental requirement of such a finding is built into the definition of the offence.
- Such a threshold should make it more straightforward for the private sector to respond to requests it receives expeditiously.
- Last but not least it will make for greater legal certainty and reduced legal risk for all parties, as well as enhance public trust.

A few examples in the present text illustrate why this is so important:

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

Articles 6, 7, and 8 could create criminal liability for journalists and their sources. The sources *intended* to provide unauthorised material to others and the journalist to review that material but their intent was not *criminal.* It was both "without authorisation" and "without right". Madame Chair, this is just one of many examples and you've heard others from NGOs previously.

Most of the articles would criminalise the work of penetration testers and security researchers, as by definition their work involves intentional penetration of networks, accessing them, reviewing and retrieving information, and in some senses interfering with systems and devices - all frequently "without right" or "without authorisation."

On other issues Madame Chair, The convention should not include kinetic offences just because ICTs were used in their commission. Articles 11 - 14, 17, and 30 - 34 should be excluded.

Offences addressing online content should only be included where the offence is not already covered in other international agreements. Therefore articles 17, 23 - 25, and 26 - 29 should be excluded.

The Convention should not establish liability for third parties through a stand-alone article and instead cover those relevant elements in other chapters. Third party liability is very complex and goes beyond criminal law, creating the real possibility for obligations in this Convention to create unanticipated issues at the national level, especially given member-states approach this issue in very different ways making conflict of laws problems more likely. Commerce needs legal certainty and clarity, Madame Chair. Article 35 should be deleted.

The Convention should not criminalise offences related to data protection solely on that basis. Data protection legislation differs widely and is under revision in many jurisdictions. How infractions are dealt with is subtle, complex, and most infringements are not criminal acts. Finally, what constitutes 'personal information' widely varies, making a finding of dual criminality problematic. Article 15 should be removed.

Thank you, Madame Chair and delegates for your kind attention.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk