Oral submission on the provisions on criminalisation

Global Partners Digital

Madame Chair, distinguished delegates, thank you for again providing the opportunity for us to share our views.

We would like to highlight our continuing concern that many of the offences listed in this chapter are vague, overbroad, and fail to comply with permissible restrictions under international human rights law.

Regarding **Articles 6-10**, these articles as they are drafted risk capturing the important and legitimate activities of journalists, whistleblowers and security researchers. These articles should include a standard of malicious or fraudulent intent or a clearly articulated and expansive public interest defence, as well as a requirement of serious harm. We note that at present dishonest intent is inconsistently applied in the draft text, and at times such intent is only included as an optional component of the offence. It is our view that this language is insufficient and risks allowing the criminalisation of acts which are carried out legitimately and in the public interest.

We echo others in recommending that these articles should include a requirement to ensure that these provisions cannot be interpreted as covering conduct in violation of terms of services or internal security policies.

Regarding the remaining articles, as we have previously highlighted, it is the view of Global Partners Digital alongside 78 other civil society organisations that this convention should be **restricted to core cybercrimes - criminal offences in which info and communications systems are the direct objects, as well as instruments, of the crimes.** Just because a crime might involve the use of technology does not mean it should be included. It is on this basis that we recommend that these offences be deleted.

If, however, these cyber-enabled crimes are included, we recommend that they reflect international consensus, be narrowly defined, precise and specific, and strictly consistent with international human rights law standards.

Of these cyber-enabled crimes, we are particularly concerned with the various **content-related offences**, including those which are still being discussed in the plenary in clusters 5 and 7. These articles are overly broad and risk criminalising legitimate expression. For example, we note that the language in Articles 20, 24 and 25 is vague and risks application in a subjective and discriminatory manner. Definitions of terms like "intimate", "explicit" and "grooming" are discretionary and have been used in certain states to criminalise same-sex relations. Like other civil society organisations, including ARTICLE 19, we question the appropriateness of the inclusion of these offences in an international criminal treaty. We therefore urge again that these offences be excluded. If included, they must be drafted as narrowly as possible and in compliance with international human rights law, including the requirements of legitimate aim, proportionality and necessity.

Thank you for your attention and consideration.