DERECHOS DIGITALES'S ORAL INTERVENTION ON CRIMINALIZATION PROVISIONS
CLUSTER 1 and 2 - DELIVERED BY MARIA PAZ CANALES
Fourth Session - 9 January to 20 January 2023

Dear Madame Chair,

Today, we support the comments referred by the two previous speaker on Cluster 1 and 2. Madame chair, let me suggest a few concrete edits on Cluster 1 and 2:

Define clearly the word "unlawful," or "without right," or "without authorization" as bypassing technical security. Such terms should be defined more clearly to require the circumvention of a technical barrier. This definition is essential to ensure that these terms do not criminalize conduct only on the basis of a violation of a company's contractual terms, terms of services or internal security policies. If not, the provision will give authority to the private sector to determine the actual scope of the criminal conduct through their terms of services or contractual terms.

Articles 6-10 are **framed too broadly and will criminalize legitimate cyber defence activities**. The word "when committed intentionally" should be replaced with "when committed with fraudulent/malicious/dishonest intent," also known as ***mens rea.*** Make sure that bypassing security protocols with such intent is the primary component of this criminal offence.

Please consider adding a sentence that recognizes the protection of the public interest. While the specifics of what should be considered public interest should be defined at the domestic level, these provisions of the Convention should not criminalize a range of public interest activities.

We suggest **striking out aggravating penalties on articles 6.3, 8.3, and 9.2.** In particular, Article 6(3)(b) "Results in the obtaining of confidential government information". If States decide to keep such an aggravating factor, Article 6(3)(b) should be amended to only cover specific types of confidential information, likely highly classified information.

Article 10(1)(a)(ii) **over-criminalizes password sharing**. While passwords are sold criminally for profit, many more are shared by friends and family (without profit), which is more appropriately a civil issue if such action violates a company's Terms of Services. As written, this Article could turn these millions of ordinary people into "cybercriminals" overnight. Thus such conduct should be excluded.

Security tools are frequently dual use in nature. Even predominantly malicious tools are frequently used by security defence teams to probe internal networks and by security researchers more generally. Article 10(1) **would criminalize the possession, creation and dissemination of certain programs that could include key tools for cybersecurity testing**. We would therefore ask that Article 10(1) apply primarily to the criminal and malicious use of tools, not to their possession or dissemination.

Finally, we want to add our **general comments regarding offenses in the CND that should be excluded on the basis that they interfere with the right to freedom of expression** or because they receive more nuanced treatment in other contexts and particularly in contexts that are more focused on civil, administrative and regulatory solutions. For example, on **Cluster 5**, as pointed out in Article 19's written submission to this Committee, 179 Member States are already parties

to the Protocol to the Convention of the Rights of the Child, where mutual assistance already exists. Therefore, we question the need for the inclusion of Cluster 5. Particularly, as pointed out by UNICEF contribution during the third intersessional consultation, adolescents who are close in age, maturity and development should not be criminalized for consensual and non-exploitative sexual activity, provided that there is no element of coercion, abuse of trust or dependency between the adolescents. A child should not be held criminally liable for the generation, possession, or voluntary and consensual sharing of sexual content of him/herself, solely for own private use. This will require improvement in the current drafting of aricle.18.4.