CCG-NLU Delhi Written Contribution to the Sixth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

---

Introduction/ Background

The **Centre for Communication Governance ("CCG")** is an academic research centre established at one of India's premier legal institutions, the National Law University, Delhi in 2013. CCG is India's only academic research centre dedicated to working on information technology, law and policy. The Centre undertakes academic research, provides policy input, and facilitates capacity building of relevant stakeholders in the ecosystem at the domestic and international level. The work at CCG is designed to build competence, facilitate public debate, enable research-based policymaking and raise the quality of discourse in information technology law and policy issues. CCG works in a vast array of disciplines including, but not limited to, cybersecurity, national security and technology, platform governance, governance of emerging technologies, privacy and data governance.

We welcome the opportunity to submit comments/ inputs on the **Draft Text of the Convention**[1] before the Sixth Session of the Ad-hoc Committee on Cybercrime (August 21-September 1, 2023).

[1] A/AC.291/22 dated 29 May 2023. Available here: <V2303951.pdf (un.org)>

Please see below for our comments/ inputs on the Negotiating Document:

A. Chapter IV: Procedural Measures and Law Enforcement (Article 23-34).

Article 23 of the Draft Text outlines the scope of the procedural measures relating to expedited preservation of computer data, search and seizure of stored computer data, preservation and partial disclosure of traffic data, and interception of content data, among others. These provisions are aimed towards assisting the legal enforcement agencies in investigation and prosecution of the cybercrimes in an expeditious manner. The provision expands the scope of such measures to include offences criminalised under the Draft Text, other criminal offences committed by means of ICT devices and for collection of electronic evidences in relation to any offences. While the designed scope may be essential for speedy investigation and prosecution of cybercrime, it is important that such provisions should not lead to disproportionate collection and retention of data. Such an unrestricted access to communication data can cause a detrimental impact on the right to privacy and other fundamental rights of an individual. Thus, such provisions should be scoped narrowly and must be accompanied with adequate safeguards to prevent any abuse or misuse. Therefore, we wish to submit that the scope of application of procedural measures should be confined to the set of "core cybercrime" criminalised under the Convention or may extend to include "serious offences"[2] as defined under the United Nations Convention Against Transnational Organized Crime (UNTOC). The broad scope of the procedural measures would inadvertently open the scope of such provisions to all offences carried out with the help of ICTs and may have unintended consequences for human rights and other fundamental freedoms. Accordingly, we propose the deletion of Article 23, paragraph 2(b). In addition, we also propose the replacement of the term "collection of evidence in electronic form of any criminal offence" with "collection of evidences in relation to offences established under the Convention".

[2] Article 2 of the United Nations Convention Against Transnational Organized Crime defines the term serious crimes as: "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty". See here: <UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME AND THE PROTOCOLS THERETO (unodc.org)> last accessed on August 25, 2023.

Article 24 of the Draft Convention lays down an obligation on the State Parties to ensure that the powers and procedures laid down under the Chapter IV, are subject to the certain "conditions and safeguards" and is consistent with State Parties obligations under the international human rights law. We are broadly in support of Article 24. We consider that the provisions relating to procedural measures and legal enforcement must be compliant with international human rights standards. In order to strengthen the said provision, we propose that the present text of Article 24 should include a clear mention of the principle of legality, necessity and proportionality. The current text of the Article 24 could benefit incorporation of specific provisions from the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) to avoid any confusion or ambiguity. Further, Article 24 should also lay down an obligation on State Parties to mandatorily seek an independent judicial authorisation before exercising their powers under the Convention. Lastly, we propose in favour of specific provisions and effective mechanisms empowering the affected individuals to challenge and seek redressal against measures taken by the enforcement authorities.

The provision laid down under **Article 25-30** of the Draft Text enables expedited preservation, and access to different forms of data (stored computer data, traffic data and content data). These provisions pave the way for increasingly intrusive legal and technical arrangements and could enable unmediated access to sensitive personal data and negatively impact the right to privacy, and other fundamental human rights. Therefore, such provisions should not allow retention of data of all users and should only be directed against specific individuals and only after receiving authorisation by an independent judicial authority. The provisions should also ensure that such data is collected and stored for specified, explicit and legitimate purposes and should not be processed in a manner incompatible with the original purpose.

B. Chapter VI: Preventative Measures

Article 53 of the Draft Text of the Convention outlines a list of preventative measures that includes developing, maintaining and implementing effective and coordinated policies to prevent cybercrime. We are broadly in support of the provision and wish to extend our strong support

towards the formal incorporation of a "multistakeholder governance model". The provision encourages active participation and dialogue amongst individuals, groups, and stakeholders from non-governmental organisations, civil society, academia, private sectors and even individuals. The suggestive list under Article 53 paragraph 3 lists a wide range of preventative measures including building cooperation amongst stakeholders, creating awareness, increasing capacity of domestic criminal justice systems, incorporating policies and strategies to end online gender-based violence, amongst others. While we consider the multistakeholder approach as crucial in the prevention of cybercrime, we feel that Article 53 would benefit immensely from an explicit reference to "international human rights obligations". In our understanding, any activity or collaboration between the State Parties and Industry should be limited to supporting government bodies in detection, investigation and prosecution of cybercrime. Lastly and most importantly, these provisions should be subject to adequate safeguards for protection of human rights and other fundamental freedoms.

C. Chapter VII: Technical Assistance and Information Exchange.

Chapter VII of the Draft Text lays down provisions on technical assistance and information exchange. We are appreciative of the fact that the Draft Text of the Convention acknowledges the vast divergences in socio-economic conditions between developed vis-a-vis developing and least-developed countries. As we have outlined in our previous submissions, many developing and least-developed countries lack the requisite institutional mechanisms, technology, skills, and financial resources prerequisite to effectively counter and combat cybercrime and which has made these countries susceptible to new forms of challenges and vulnerabilities. Such countries often struggle with weak legal and policy frameworks, as well as limited institutional resources and capacities as it relates to law enforcement agencies.

We are broadly in agreement with provisions listed under Chapter VII of the Draft Text, for it includes a wide and inclusive understanding of the terms, "technical assistance", and "capacity building" to include, "*training and other forms of assistance, the mutual exchange of relevant experience and specialised knowledge and, where possible, the transfer of technology*". The list is

further elaborated under paragraph 3 of Article 54. We are also appreciative of the fact that the Draft Text has taken due consideration for the lack of financial wherewithal in developing and least-developed countries for sustaining projects and activities that focus on awareness, education, and technical skills helpful in countering cybercrime. This is evident from the fact that the Draft Text has instituted a separate provision encouraging optimal implementation of the Convention through financial and material assistance to support developing countries. We further propose that provisions under this chapter are reconsidered and reworded in establishing strong and legally binding provisions that encourage building and strengthening the technical competence of developing and least-developed countries. To this end, we propose striking off vague terms such as “to the extent necessary”/ “to the extent possible”.

We also wish to highlight that capacity building tools discussed under this provision can include transfer of tools and skills that are dual use and are prone to misuse, posing serious threats against human rights and other fundamental freedoms. Therefore, we propose that the provisions in this Chapter should be subjected to State Parties obligations under international human rights law to prevent any potential misuse or abuse.