CCG-NLU Delhi contribution to the Third Session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes

2 September 2022

The Centre for Communication Governance at the National Law University, Delhi, India welcomes the opportunity to submit its comments for the third session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes. CCG-NLUD appreciates the Chair, the Secretariat, and staffers for their critical work and efforts in enabling broader stakeholder participation that allows a greater exchange of information and ideas between disparate actors operating in the global ICT ecosystem. In this document, we aim to offer our inputs on provisions concerning technical assistance.

Agenda Item 5: Provisions on Technical Assistance

In order to build effective response strategies and solutions to the threat of cybercrime, the convention should incorporate provisions which acknowledge the vast divergences in socio-economic conditions between developed vis-a-vis developing and least-developed countries. Many developing and least developed countries lack the requisite institutional mechanisms, technologies, skills, and financial resources and this has consequently 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. Such deficits can result in the rise of safe havens for malicious actors and cybercriminals and severely impair the ability of these countries to counter and combat cybercrime effectively.

The convention, therefore, should explicitly address these challenges by establishing strong and legally binding provisions that encourage building and strengthening the technical competence of these countries. The convention should promote the sharing of technology, know-how, modern law enforcement equipment and techniques, and development assistance for projects and activities that focus on awareness, education, and technical skills helpful in countering cybercrime. The scope of such provisions should be broad and should aim to promote training programmes which build the capability of law enforcement personnel, including prosecutors, Investigators, judicial officers, and other personnel charged with preventing, detecting and mitigating cybercrime. Moreover, it may be beneficial for the international community to deliberate on standards for government and/or court orders which request ICT infrastructure and digital service providers for electronic evidence of cyber offences. Such standards could consider incorporating indicators which help ensure that evidence requests embed requisite human rights and due process safeguards.

The convention should lay down specific provisions elaborating legal and technical standards in respect of the admissibility of digital evidence. Further, the convention should also facilitate the dissemination of digital forensics capabilities and best practices between public and private
institutions in the member countries. Recognising that the private sector, civil society and academia play a vital role in the digital ecosystem, the convention can also provide a basic framework encouraging the participation of non-state actors on a voluntary basis. We believe that the United Nations Office on Drugs and Crime (UNODC) can play a vital role in facilitating such specialised assistance to the developing and least developed countries and monitoring the implementation of capacity-building programmes instituted under the said convention.