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 international cooperation.

Agenda Item 4: Provisions on International Cooperation

Cybercrime is a transnational crime that takes place in the borderless realm of cyberspace. Very often, the perpetrators and victims of such crimes are located in different countries/regions/territories, making effective cross-border investigation and prosecution of cybercrime complex. To add to the complexity, the evidence associated with such offences may reside in a third independent jurisdiction. This adds to the legal complexity of investigations and prosecutions. In order to sufficiently prevent and combat cybercrime, the international community needs to devise adaptive and flexible legal frameworks with effective mechanisms for co-operation amongst participating member countries.

We submit that the convention should encourage both formal and informal means of international cooperation for (i) investigation and prosecution of offenses covered under this convention as well as (ii) collection of evidence in electronic form of a criminal offence. The convention should draw on common and well understood principles and standards in the areas of extradition, mutual legal assistance, transfer of criminal proceedings, and other effective measures, while being conversant with the divergent realities of participating member countries. The provision relating to extradition should only apply to criminal offenses established in accordance with this convention and in the case of “serious crimes” that include offenses punishable by maximum deprivation of liberty of at least four years or a more serious penalty as defined under United Nations Convention Against Transnational Organized Crime (UNTOC). This will help with proportionate outcomes wherein extradition is not used for less serious digital offences. We also propose that in furtherance to the principles of state

---

sovereignty, reciprocity, legality and the protection of individual rights, the provisions relating to extradition should be based on the principle of dual criminality. Further, the provision should also include grounds for refusal to extradite in relation to requests made for the purpose of punishing or persecuting the individual on grounds of their race, religion, gender, and other characteristics.

On the provisions relating to Mutual Legal Assistance, we propose that the convention should adopt provisions that enable member countries to conduct cybercrime investigations and prosecution in a timely and effective manner. The Convention should enable the law enforcement authorities’ access to digital information and incorporate provisions that allow for sharing of digital evidence between legal enforcement agencies and private organisations subject to the inclusion of strong human rights safeguards through institutional and procedural safeguards. Further, the provision on mutual legal assistance should also aim to expedite preservation and disclosure of data in emergency cases, for example, in situations where there is a significant and imminent risk to the life or safety of an individual. The convention would benefit if it explores avenues beyond the existing MLAT frameworks that are fraught with delays and challenges in facilitating access to information critical to protecting against imminent risks to life or safety. Alternatively, the Convention should consider setting up a 24*7 network consisting of single point of contacts (PoCs) designated by the member countries to ensure the availability of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Finally, and most importantly, we wish to highlight that such provisions must be coupled with necessary safeguards protecting human rights and any action thereto must be in line with the principles of legality, proportionality and necessity.

---
