To,

The Secretariat

Ad Hoc Committee

United Nations Office on Drugs and Crime

Written Submission on behalf of Rashtriya Raksha University for the Fourth Session of the Ad Hoc Committee to elaborate a comprehensive International Convention on countering the use of Information and Communications Technologies (ICTs) for Criminal Purposes.

Introduction

Rashtriya Raksha University ('RRU') is an Institution of National Importance and has a vision to emerge as a premier center of knowledge and an academic-research-training ecosystem for national security and police. It aims at providing security and strategic education in the contemporary and futuristic security and strategic studies and interdisciplinary areas. Our University contributes to the vision of India of Peace, Prosperous, and Stable World in alliance with grand strategic cooperation between like-minded nations and promoting greater understanding between internal security officers, military and paramilitary forces, diplomats, civil servants, and civilians to promote the cause of the nation. It also adopts a two tier approach, at the national and international levels, its education, research and training, and extension in order to achieve capabilities to respond to the needs, expectations, and aspirations of the security and strategic institutions and forces as well as law-making, governance, judiciary, economy and the civil society organizations.

RRU welcomes and appreciates the initiative of the Ad Hoc Committee ('AHC') to elaborate a comprehensive International Convention on countering the use of Information and Communications Technologies (ICTs) for Criminal Purposes ('Convention'). RRU was actively involved and has submitted its observations and recommendations in the Third Session of AHC. Since the Fourth Session calls for discussion on facets like general provisions, provisions on criminalization, provisions on procedural measures, and law enforcement; RRU reiterates its complements towards the systematic and well channelized negotiation processes of the AHC. Such sessions give academic institutions like ours an opportunity to contribute to the cause.

In this regard, RRU submits its observation and recommendations on the relevant chapters as follows:

Chapter I
General Provisions

Article 1. Statement of purpose

1.1 RRU emphasizes on providing practical measures to enhance technical assistance among States Parties, build the capacity of national authorities to prevent and combat [the use of ICTs] [cybercrime], in particular for the benefit of developing countries, and strengthen and promote the exchange of information, specialized knowledge, experiences and good practice.

1.2 RRU is a firm believer of the postulate that we should initiate towards an inclusive, transparent, stable, accessible, free, and secure cyberspace that is fair in all terms.[1] There has to be enhancement in the capacity and capability of concerned entities and each state party.

Article 2. Use of terms

1.3 We emphasize on the terms of usage depicted by India in its submission at the Second Session of the Ad Hoc Committee (Para 13).[2] However, we also accept the fact that this provision can be addressed after the main substantive articles of the convention are defined.

Chapter II
Criminalization

2.1. It is of paramount importance to classify crimes that are committed using Information and Communications Technologies (ICTs). The development of international model provisions on

[1] Statement by Joint Secretary (Cyber Diplomacy), March 02, 2022, available at https://www.mea.gov.in/SpeechesStatements.htm?dtl/34917/Statement_by_Joint_Secretary_Cyber_Diplomacy_at_the_1st_Session_of_UN_Ad_Hoc_Committee_to_Elaborate_a_Comprehensive_International_Convention_on_Counte.
[2] Indian contribution for 2nd Session of AHC, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf.

criminalization of core cybercrime acts, with a view to supporting States in eliminating safe havens through the adoption of common offence elements is the need of the hour.

2.2. The provisions could maintain the approach of existing instruments regarding offences against the confidentiality, integrity and accessibility of computer systems and data and could also cover 'conventional' offences perpetrated or facilitated by use of ICTs.

2.3. In furtherance of the same, each State party shall adopt such legislative and other measures as are necessary, as provided in the following points, to establish as an offence or its equivalent clauses under its domestic law.

CLUSTER 1

Article 10. Misuse of devices and programs

Tampering with computer source documents: -

2.4. In addition to the elaborated Articles, there can be provision on tempering of computer source documents.

2.5. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, when any person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable.[3]

CLUSTER 3

Article 15. Violation of personal information

Disclosure of information in breach of lawful contract.

2.6. In addition to the provision on violation of personal information, provision on the disclosure of information in breach of lawful contract ought to be included.

[3] Indian contribution for 2nd Session of AHC, para 4 (c), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf.

2.7. Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person.

CLUSTER 4

Article 17. Infringement of copyright

2.8. It is a welcome step to include infringement of copyright and trademarks because of the fact that some countries do not have specific IPR law that prevents infringements. Using general criminal law for prosecution of such offences, would be inadequate for prosecuting high level crimes of commercial scale.

CLUSTER 7

Article 24 and 25

(Provisions on sexual extortion and non-consensual dissemination of intimate images)

2.9. In addition to the provisions on sexual extortion and non-consensual dissemination of intimate images, a distinct provision on privacy can be elaborated.

2.10. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person, intentionally or knowingly captures, publishes or transmits private images of any person without his or her consent, under circumstances violating the privacy of that person.[4]

CLUSTER 9

Article 29. Terrorism-related offences

2.11. RRU appreciates the elaboration made under this Article. In addition to this, few additions pertaining to *'cyber terrorism'* that can be taken into consideration is that each State party shall adopt such

[4] Indian contribution for 2nd Session of AHC, para 4 (h), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf.

legislative and other measures as are necessary to establish as an offence under its domestic law, if any person–

(A) with intent to threaten the unity, integrity, security or sovereignty of State or to strike terror in the people or any section of the people by–

(i) denying or cause the denial of access to any person authorised to access computer resource, or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure;

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of State , the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.[5]

[5] Indian contribution for 2nd Session of AHC, para 4 (i), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf.

Chapter III

Procedural Measures and Law Enforcement

3.1. It is expected that the States work towards strengthening their procedural and cooperative measures to prevent and counter more effectively the use of ICTs for criminal purposes by facilitating legal enforcement. Evidently, in addition to adequate criminalization, law enforcement by concerned agencies are vital too.

CLUSTER 1

Article 40. Jurisdiction

3.2. RRU appreciates and welcomes the exhaustive explanation to the clause of jurisdiction. It is in consonance with India's submission in the Session of the Ad Hoc Committee.

CLUSTER 2

Article 44. Expedited preservation and partial disclosure of traffic data

3.3. Each party shall create a nodal point for coordination by which such request for preservation can be carried out by the other state.

Article 47. Real-time collection of metadata

3.4. Each Party shall adopt such legislative and other measures as may be necessary to provide metadata expeditiously without the need of MLAT. The service provider who has such metadata shall provide such information on direct request of the Law Enforcement Agencies (LEAs) through the designated nodal agency of each State.

3.5. Each Party shall adopt such legislative and other measures as may be necessary to provide content data expeditiously. Mechanism for such expeditious data sharing will be developed under this convention.[6]

[6] ibid.

Article 49. Admission of electronic/digital evidence

3.6. RRU is of the opinion that a provision on electronic evidence is the need of the hour. It is true that due to the volatile nature of electronic evidence, many states face stiff challenges in prosecuting cybercrimes. Evidences are not available in time as there is lack of coordination among various LEAs due to issues of jurisdiction and non-agreement on sharing the non-content and content data.

CLUSTER 3

Article 50. Freezing, seizure and confiscation of the proceeds of crime

3.7. Each State Party, in order to provide mutual legal assistance in relation to property acquired through the commission of an offence established in accordance with this Convention, shall, in accordance with its domestic law:

(i) Take such measures as may be necessary to enable its competent authorities to give effect to an order of seizure, confiscation issued by a court of another State party;

(ii) Take such measures as may be necessary, within its jurisdiction, to enable its competent authorities to confiscate property of foreign origin by judicial order in connection with the legalization of proceeds derived from an offence established in accordance with the provisions of this Convention;

(iii) Consider taking such measures as may be necessary to enable non-conviction-based confiscation of such property in criminal proceedings where the offender cannot be prosecuted by reason of death, flight or absence, or in other appropriate cases.[7]

3.8. Provided that reasonable basis for the requested State party to believe that there are sufficient grounds for taking such measures.

Article 55. Measures to enhance cooperation with law enforcement authorities

3.9. RRU seconds the provision on measures to enhance cooperation with law enforcement authorities. In addition to the depictions of the negotiating document, the Convention may propose that timely

[7] Indian contribution for 2nd Session of AHC, para 22, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf.

cooperation among the agencies of the Governments is essential to investigate and prosecute cybercrimes.

(i) States need to strengthen cooperative measures to prevent and counter more effectively the use of ICTs for criminal purposes by facilitating legal and technical assistance taking into consideration the border less nature of the ICT crimes.

(ii) Law enforcement can be facilitated if there is timely response and proper notified channels or points of contacts of communications or designated officers who may receive and process the request in a specific time. Such notified channels or points of contacts may serve 24/7 networks for faster response times.

(iii) Investigations that affect the state sovereignty must be accorded high priority that information is shared within a short timeline of not more than 24 hours.

(iv) If there is some special request, for instance a request to preserve computer data for a period specified; the proposed international convention can specify the period for which the data can be preserved.

(v) There can be training for speedy assistance.

Conclusion

3.10. Indeed, the ongoing elaboration process is an opportunity to align the legal, policy, and operational levels to address the criminal use of ICTs more effectively. RRU firmly believes in the concept of One Earth, One Family, and One Future. In light of the same, RRU is keen in providing holistic assistance, training, research, education, extension, awareness, and facilitating the capacity building in the area of fighting against cybercrime, and strengthening the entire domain of cyber security.

(The submission is made without prejudice to any future position / submission that the Republic of India may take / make during the course of future deliberations / negotiations of this convention in the informal sessions or substantive sessions of the Ad Hoc Committee.)

****