International Conference on Cyberlaw, Cybercrime & Cybersecurity

Phones: +91 11 46584405
Email: info@cyberlawcybercrime.com
Office: S-307, Greater Kailash-1,
New Delhi-110048

28th April, 2022

To

The Secretariat of Ad-hoc Committee
CybercrimeAHC@un.org

SUBJECT: **MY SUBMISSIONS DURING THE MEETING OF THE FIRST INTERSESSIONAL CONSULTATION OF THE AD HOC COMMITTEE, HELD ON 24TH & 25TH MARCH, 2022 IN VIENNA**

Dear Sir,

It is most respectfully submitted as under:-

The proposed Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes could consider having the following essential elements as integral parts thereof:-

PREAMBLE

1) There needs to be an appropriate Preamble where the main objectives of the Convention need to be appropriately well elaborated.

2) The Preamble needs to be self explanatory and needs to highlight the growing use of ICT for criminal purposes and hence, the need for a comprehensive international Convention.

DEFINITIONS

3) In general provisions, there is a need for coming up with a very detailed and comprehensive set of definitions. That these definitions be detailed is very important, since there is not complete unanimity globally amongst different ICT laws on defining various concepts, phenomenon and technologies.

4) Hence, detailed elements pertaining to definitions need to be an integral part of the general provisions.

OBLIGATIONS OF PARTIES

5) Another essential element of the proposed Convention should be that it must elaborate in crystal clear terms the obligations of the parties to take effective steps at national

levels to mirror the elements and salient features of the Convention under the national legislations or domestic laws and connected legal regimes and frameworks.

CATEGORIES OF ICT CRIMES TO BE COVERED

6) Broadly speaking, the use of ICT for criminal purposes can be divided into five broad categories.

   a) ICT crimes against persons;
   b) ICT crimes against property;
   c) ICT crimes against nations;
   d) ICT Social media crimes;
   e) Newly emerging technologies crimes

   The Convention should try to address various essential elements and salient features of these five different categories in the distinctive provisions of its framework.

ICT NETWORK CRIMES ELABORATION

7) It is imperative that the Convention must criminalize certain activities, that need to be well recognized and well regulated.

8) Misuse of technology platforms to target ICT devices specifically needs to be recognized as a distinctive ICT crime.

9) Aiding, abetting and conspiring to do any of the criminal activities detailed in the Convention must be made a distinctive crime and nation states need to encouraged to so declare the same in their national legal frameworks.

EMERGING TECH MISUSE TO BE COVERED

10) There needs to be criminalization of the misuse of emerging technologies whether it is Artificial Intelligence, Blockchains, Quantum Computing or Internet of Things or any other kind of emerging technology which uses the cyberspace to operate.

MENS REA AND ACTUS REA

11) The entire issue of mens rea and actus reus has to be given importance, since mens rea and actus reus are important elements for the consideration of the Convention. Most of the national penal laws are drafted keeping in mind the essential elements of mens rea and actus reus or the factum of an act and also intention of the intended consequences of such act. Whether intention needs to be an integral component of ICT crimes is something that the Convention needs to deliberate upon, because in many cases, the technological paradigm can be misused, without really having an intention to misuse it but nonetheless, such unintentional misuse still results in criminal use of ICT networks. That kind of criminal use of ICT networks, which is without the intention to cause such misuse, also needs to be criminalized as a penal offence and therefore the Convention

needs to recognize that the signatory nations need to come up with appropriate national laws which incorporate the specific elements of the Convention.

ROLES OF ICT SERVICE PROVIDERS

12) The entire role and responsibility of ICT service providers and technology service providers needs to be specifically targeted and addressed by the Convention. This is so because unlike other crimes, in ICT crimes, the ICT service providers or platforms are huge data repositories and this data has a direct impact upon not just detection, investigation but also further prosecution of ICT crimes. Hence, protection and preservation of ICT records by ICT service providers and platforms has to become a top most priority and area for the Convention to potentially address.

13) Also, any activity by the service provider or any legal entity which tantamount to aiding, abetting or assisting the commission of an ICT crime also needs to be recognized and criminalized and appropriate provisions need to be made an integral component of the Convention.

ENFORCEABILITY PARAMETERS

14) The Convention should aim to come to a harmonious balance as to what kind of criminalization or conduct leads to what kind of consequences and given the fact that there is no international law on cybercrime, the issues pertaining to the enforceability

of the Convention are also issues that need to be dealt with as an integral component of the principles and foundations of the Convention.

ICT JURISDICTION

15) The entire issue of internet jurisdiction or ICT jurisdiction needs to be specifically addressed. This is so because ICT crimes are transnational crimes and ICT networks are today ubiquitous. Therefore, by relying upon the said ubiquitous networks, cyber criminals can go ahead and conduct their criminal activities with impunity. Hence, issues of how jurisdiction of law enforcement agencies needs to be invoked in ICT crimes, also needs to be specifically addressed.

16) Typically, under the national penal laws, the moment a particular activity on ICT networks impacts computer resources or communication devices physically located within the territorial boundaries of that country, that becomes the basis for the law enforcement agencies to invoke the criminal jurisdiction.

17) The specific issues pertaining to ICT based jurisdiction need to be specifically highlighted as an integral part of the proposed Convention. This is so because the invention of the internet has made geography history and therefore, it is imperative that the Convention must stipulate the powers and responsibilities of each party on how to invoke internet jurisdiction in the boundary-less cyberspace medium in the context of the commission of ICT crimes that are targeted on computers, computer systems,

computer networks, computer resources and communication devices, located within the territorial boundaries of the relevant party to the Convention.

18) There needs to be specific provisions that the jurisdiction of the proposed Convention should not and does not exclude any crime or offence, over which criminal jurisdiction is exercised by parties to the Convention in accordance with domestic laws.

19) Data based jurisdiction provisions needs to be made the foundation of the proposed Convention.

20) Today, jurisdiction is based on the territorial foundations or on the basis of location or storage or processing of data.

21) As time passes by and as data breaches more and more ubiquitous in the data economy, it will be imperative for the Convention to consider data based jurisdiction so as to give level playing field on jurisdictional issues to all member states of the proposed Convention.

ISSUES REGARDING DETECTION, INVESTIGATION AND PROSECUTION OF ICT CRIMES

22) The entire issues pertaining to detection, investigation and prosecution of ICT crimes needs to be specifically addressed by the proposed convention.

ATTRIBUTION

23) The entire issue of attribution of ICT crimes is a fundamental issue that needs to be addressed. How to attribute a particular cyber or ICT crime to a particular cyber or ICT actor is one contentious area, where the proposed Convention must potentially throw light on. This is so because internationally, as on date, there is no unanimity on how these principles of attribution of criminal liability needs to be universally accepted and implemented in the context of cybercrimes.

24) Attribution of ICT crimes today has become even more complicated, given the fact that there is increased reliance on new technologies by cyber criminals to wipe their electronic footprints. This results in lack of effective incriminating electronic evidence to implicate such cyber criminals. For example, there is increasing propensity to use technologies and Virtual Private Networks (VPNs) for the purposes of obliterating electronic footprints.

DIGITAL DUST ISSUES

25) The use of emerging technologies for the purposes of obliterating or removing the digital dust or electronic footprints itself needs to be considered as a criminal activity or an offence.

26) Deletion of incriminating electronic evidence is another thrust area which needs to be brought within the ambit of criminality.

27) The voluntary assisting of criminal use of ICT networks also needs to be brought within the ambit of criminal activities, under the provisions of this convention.

EMERGING TECH

28) The proposed Convention needs to be examined and made applicable to crimes committed due to emerging technologies, more so in the context of advent of technologies like Quantum Computing. Technologies may exist which can be misused for criminal purposes.

29) Use of ICTs for criminal purposes by appropriate programming of the said technologies needs to be brought within the ambit of criminal activities, under the provisions of the proposed convention.

30) Using ICT purposes for hurting the cause of humanity or for deliberately targeting humanitarian causes and actions should also be considered to be brought within the ambit of criminal activities, under the provisions of this convention.

31) Appropriate responsibility for misuse of ICTs so programmed needs to be apportioned on or attributed to the relevant human actors behind the same.

CRIMINAL LIABILITY OF CODERS

32) There is also a need for recognizing the criminal liability of the coders of Artificial Intelligence in the sense that such coders of Artificial Intelligence which code Artificial Intelligence for criminal or illegal purposes need to be brought within the ambit of criminality.

CYBERCRIME AS A SERVICE COVERAGE

33) Cybercrime-as-a-service is also a paradigm that needs to be brought within the ambit of criminal activities, under the provisions of the proposed convention. Countries need to come up with appropriate legal frameworks so as to regulate and target Cybercrime-as-a-service.

INTERMEDIARIES LIABILITY

34) The specific liability of intermediaries and service providers need to be stipulated as part of Convention for criminal activities done either on their networks or as a result of their negligence or contravention.

35) This becomes important as different countries have come up with differing legal approaches on how to deal with liability of corporates and intermediaries.

SANCTIONS AND MEASURES

36) The proposed Convention should specifically come up and elaborate with sanctions and measures encouraging the parties to the Convention to adopt such national legislative and other measures as may be necessary to ensure that the ICT crimes detailed under the Convention are punishable by effective, proportionate and dissuasive sanctions, including but not limited to deprivation of liberty. It would be prudent for the proposed convention to encourage its signatory member states to announce criminal measures and sanctions including monetary fines and imprisonment for the various ICT crimes detailed in the proposed convention.

PROCEDURAL PROVISIONS

37) The Convention also needs to have specific focus on procedural provisions which need to be specifically emphasized upon by every negotiating party.

SYNC WITH INTERNATIONAL LAW AND COVENANTS

38) The Convention needs to also recognize the fact that the principles of international law are applicable to misuse of ICTs for criminal purposes and hence build on the work that has already been done by the United Nations Group of Governmental Experts (UN GGE) in this regard.

39) Utmost pressure needs to be maintained on parties to the Convention to provide for adequate protection of human rights and liberties, in sync with 1966 United National

Covenant on Civil and Political Rights and other applicable human rights instruments which have been negotiated and accepted at international levels.

40) Issues pertaining to protection of human rights, fundamental freedoms, privacy of individuals, protection of data and protection of victims of cybercrimes need to be intrinsically made integral parts of the proposed Convention.

SUPERVISION PROVISIONS

41) There must also be general provisions on judicial and other independent forms of supervision and also, such forms of supervisions must be seen as integral part of conditions and safeguards at national levels of signatory member states.

42) The proposed Convention must also encourage parties to it, to consider the adoption of the powers and procedures under the Convention at national levels and the impact of the same on the rights, duties, responsibilities and legitimate interests of third parties.

ELECTRONIC EVIDENCE

43) Considering the advent of the data economy, it is important for the proposed Convention to focus on the preservation and retention of incriminating electronic evidence as also stored computer data.

44) Given the fact that data has now become the foundational basis for ICT crimes to be detected, investigated and prosecuted, there is a necessity that the parties to the Convention must come up with appropriate national legal provisions mandating the concerned legal entity or service provider to preserve or maintain the integrity of the relevant computer data for a minimum period of 180 days to enable the authorities within the country and outside to seek disclosure and further retention as also preservation.

45) The proposed convention must stipulate that Computer logs and data traffic needs to be expeditiously preserved and then appropriately disclosed, after following the appropriate stipulated processes and procedures.

46) Electronic evidence issues including the issues pertaining to detection, collection, preservation, retention and proof of electronic evidence in the context of ICT crimes need to be specifically focussed on as a major thrust area of the proposed Convention.

47) The issues pertaining to providing access to subscriber information has to be balanced with the prevailing data protection and privacy norms at international and also at regional and national levels in the proposed Convention.

48) The Convention further needs to adopt specific detailed provisions in requiring its parties to adopt legislative and other measures at national levels to facilitate search and seizure of relevant electronic evidence, computer logs and stored computer data.

49) Search and seizure provisions in the proposed convention needs to be stipulated in sync with the prevailing international legal frameworks and convenants and applicable national laws.

50) The Convention must call upon countries that are parties to it, to adopt legislative and other measures at national levels pertaining to detection, collection, retention and preservation as also proof of the relevant incriminating electronic evidence, computer logs and traffic data.

INTERCEPTION AND MONITORING PROVISIONS

51) The proposed Convention also needs to have such provisions that call upon countries that are parties to it, to adopt legislative and other measures at national levels pertaining to interception, decryption and monitoring of data including content data as also its blocking, in sync with principles and covenants of prevailing international instruments.

INTERNATIONAL COOPERATION

52) Principles pertaining to international cooperation need to be specifically elucidated in the Convention, especially with regard to ICT criminal activities.

53) The Convention needs to be mindful of the fact that Mutual Legal Assistance Treaties (MLAT) frameworks are non-existent and non-effective remedies in today's times and therefore, the Convention must come up with more cogent, proactive, practical

measures pertaining to international cooperation in the context of the commission and continued perpetuation of ICT based crimes.

54) There must be broad principles of international cooperation pertaining to mutual assistance in the detection, investigation and prosecution of ICT crimes that needs to be incorporated in the proposed Convention.

55) The world is already going through a New Cyber World Order. In my book "New Cyber World Order Post Covid-19" I have talked about the New Cyber World Order evolving after the end of Covid-19 where cybercrimes will be the new default normal and cyber security breaches will be our daily companion.

56) In a scenario like this, it will be imperative that the Convention must facilitate proactive and spontaneous actions that would be taken by its signatory parties, so as to protect and preserve the disclosure of information concerning initiation and carrying out of investigations or proceedings concerning ICT crimes in accordance with the proposed Convention.

57) Other proactive international cooperation mechanisms also need to be explored and specifically elaborated in the Convention, given the imminent failure of the Mutual Legal Assistance Treaty route and given the fact that Mutual Legal Assistance Treaties are also dependent upon the subjective will of the concerned countries, whether or not to share any information in this regard or not, with the requesting nation.

58) Issues pertaining to maintaining confidentiality in respect of sharing of information on ICT crimes need to be incorporated in the proposed Convention.

59) Provisions pertaining to expedited preservation, retention and disclosure of relevant incriminating electronic evidence, computer logs and computer data including traffic data needs to be made an integral part of the proposed Convention.

60) The Convention also needs to be mindful of certain national provisions in different nations which have extra territorial applicability and the proposed Convention need to explore the possible impact of such legal frameworks on the proposed Convention and its effective implementation.

ACCESSION PROVISIONS

61) The proposed Convention must have legal provisions pertaining to its signatures, ratifications and acceptance and also approval of the concerned negotiating parties and must provide detailed provisions pertaining to accession to the Convention as also its territorial applicability.

62) The interplay of the proposed Convention with the applicable multilateral and bilateral treaties and arrangements between contracting parties, needs to be also addressed.

63) Seamless exchange of information amongst contracting parties to the proposed Convention pertaining to ICT crimes needs to be facilitated so as to regulate misuse of ICTs for criminal purposes.

AMENDMENT PROVISIONS

64) The proposed Convention must also have provisions pertaining to how the Convention could be potentially amended by parties to it.

DISPUTE RESOLUTION

65) There is a possibility of potential disputes under the Convention between contracting parties. There must be appropriate alternate dispute resolution mechanisms stipulated as part of the Convention for settlement of all disputes.

66) The Convention must have effective parameters for its effective implementation and exchange of information pertaining to ICT crimes, including on the collection of electronic evidence amongst the contracting parties.

DENUNCIATION PROVISIONS

67) The proposed Convention could also have provisions pertaining to its denunciation.

68) The proposed Convention needs to specifically deal with different cyber attacks like ransomware, malware, spyware, distributed denial of service attacks and other ICT crimes which are aimed at targeting the authenticity and veracity of computer systems, computer resources as also data residing therein.

69) Financial ICT crimes, reputational ICT crimes and ICT crimes targeting national Critical Information Infrastructure and also national sovereignty are important crimes that need to be featured as integral parts of the proposed Convention.

PROTECTING DISADVANTAGED GROUPS

70) Specific provisions need to be prepared in the Convention for protection of especially disadvantaged group of people like old people, women and children.

71) It should be the duty of the contracting parties to make sure that the domestic laws are in sync with the provisions of the proposed Convention.

72) The Convention must specifically deal with emerging challenges of today's times including misuse of ICTs for ICT bullying, trolling, ICT harassment, ICT nuisance and other related criminal activities.

CRYPTO AND DARK NET PROVISIONS

73) Misuse, both present misuse and possible future misuse, of crypto ecosystem including crypto-currencies and crypto-assets for ICT crimes need to be specifically addressed as part of the Convention.

74) Dealing with the misuse of the darknet for criminal purposes, also needs to be part of the proposed Convention.

75) There must be general provisions dealing with the applicability, aims and objectives of the Convention.

76) Further, the authors of the Convention need to recognize that crypto ecosystems including crypto-assets and crypto-currencies, virtual assets and cloud funding platforms need to be regulated, so that they are not used to assist terror financing, at international, regional and national levels.

CYBER FORENSICS

77) Importance of cyber forensics in detection, investigation and prosecution of ICT crimes needs to be recognized by the proposed Convention.

78) Issues pertaining to admissibility and proof of incriminating electronic evidence in the context of planning, execution and implementation of ICT based crimes needs to be specifically addressed as part of the proposed Convention.

FUTURISTIC LANGUAGE

79) The provisions of the Convention must be drafted in broad generic futuristic terms. By the time the Convention comes into actual existence, technology and ICT networks would have substantially further changed. We are already going in the direction of Quantum Computing and therefore there will be increasing need that the provisions of the proposed Convention must be broad, generic and holistic so that they can withstand with the test of time. It is further necessary to ensure that such provisions must be made equally relevant and topical in the context of misuse of ICT networks for criminal purposes.

OTHER MISCELLANEOUS PROVISIONS

80) The Convention must facilitate sharing of non-content data/meta data with efficiency and efficacy without going through the Mutual Legal Assistance Treaty route or Letters Rogatory Route which are both time consuming and ineffective.

81) The authors of the Convention need to crystallize their respective thought processes on the fact that non-content data does not breach the right to privacy. Rather, it assists law enforcement agencies in the detection, investigation and prosecution of ICT crimes done with criminal intention.

82) Appropriate obligations of member states need to be made an integral part of the proposed Convention so as to preserve the data on receipt of any request from any law enforcement agency of any member state.

83) Specific obligations of preservation and retention of the relevant incriminating electronic evidence, computer data, traffic data and non-content data of private sector needs to be made an integral part of the proposed Convention, since the private sector is the huge repository of data in today's times.

84) The Convention must also recognize that it is also ultimately aimed for vindication of rights of the victims of ICT crimes and hence stands for vindication of human rights, fundamental rights and right to privacy and protection of data of victims of such ICT crimes.

85) The authors of the Convention need to recognize that there is a need to empower the law enforcement agencies enough so that they can effectively detect, investigate and prosecute ICT crimes and also yet provide justice to the victims of the malicious use of ICT rights in the poor, vulnerable and less informed sections of the population including children, women and older people in developing and under-developed countries. The special needs of the vulnerable, poor and less informed sections of the society needs to be recognized when the proposed Convention is talking about the misuse of ICTs for criminal purposes.

86) The proposed Convention also must come up with effective and efficient mechanisms for international cooperation of sharing of information with speed, efficiency and effectiveness to combat the crimes committed with the use of ICTs.

87) The Convention should also look at the need for piercing the anonymity wheel and the transnational nature of the use of ICTs while dealing with the issue of regulating ICT crimes.

88) The Convention must propose its provisions to maintain open, inclusive, free, fair, transparent, secure and accessible ICT ecosystem.

89) The proposed Convention should specifically address issues pertaining to misuse of ICTs for terrorist purposes, fake news, misinformation and disinformation campaigns, deep fakes and false narratives aimed at exciting hatred violence and cyber radicalization.

90) The proposed Convention must recognize the need for strengthening the hands of the law enforcement agencies to fight the menace of misuse of encryption message services, Virtual Private Networks (VPNs), darknet and also blockchain and related technologies by ICT criminals.

CAPACITY BUILDING

91) The Convention also must have provisions to recognize the need for enhancing capacity building in the field of ICTs for all stakeholders specifically amongst developing and under-develop countries to counter the malicious use of ICTs for criminal purposes.

The aforesaid are some of the more significant issues and aspects that need to be appropriately addressed by the proposed Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Thanking you

For International Conference on Cyberlaw, Cybercrime & Cybersecurity

Dr. Pavan Duggal
Advocate, Supreme Court of India
Conference Director, International Conference on Cyberlaw, Cybercrime & Cybersecurity