UN Ad Hoc Committee (AHC) to elaborate a comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes.

Indian contribution for 2nd Session of AHC

Criminalization, General Provisions and Procedural Measures and Law Enforcement

Background

1. Cyber space, being a complex environment of people, software, hardware and services on the Internet, has distinct and unique characteristics as compared to physical space. The cyberspace is virtual, borderless and offers anonymity. In the recent years, social media and mobile eco-system have emerged as one of the important public communication channels. Of late, use of social media has been seen all over the world as a key tool by criminals and anti-national elements to commit cyber crime. With a borderless cyberspace coupled with the possibility of instant communication and anonymity, the potential for committing cyber crime through the use of social media and internet is higher than ever in the country, like elsewhere in the world.

2. Cybercrime has also become a major issue while there is an upsurge in usage of information and communication technology (ICT) devices globally. The advancement of technology has made human dependent on ICTs for all their requirements. Unlike conventional crime, cyber crime has no geographical boundaries and the cyber criminals are unknown and even anonymous that affects all stakeholders including common citizens. The following section emphasis on the types of cyber-crimes that occur globally.

Classification of crimes committed through the use of ICTs

3. Cybercrime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic wracking to denial of service attacks. In general, cyber crime can be classified as "Cyber-enabled crime[1]" and "Cyber-dependent crime[2]. Further, cyber crime can also be classified viz. Cyber crimes against persons, Cyber crimes against property and Cyber crimes against government. However, it may be better to use crimes committed through the use of information communications technologies (ICTs) as it will be able to cover the new and emerging technologies also.

Criminalization:

4. 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 (The list given below is indicative and more crimes may be added that are committed through the use of ICTs).

---

[1] ***Such as theft, harassment, child exploitation, fraud, scams that can be committed without a computer but are enabled by a computer in certain circumstances***

[2] ***hacking, ransomware, DDoS attacks and malware, distribution of virus, cyber terrorism.***

4(a): Damage to computer, computer system, etc:-

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 without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

4(b): Failure to protect data:-

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person.

4(c): Tampering with computer source documents:-

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

4(d): Sending offensive messages through communication service, etc.:-

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 sends, by means of a computer resource or a communication device,–

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

4 (e) Dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device.

4(f): Identity theft (Impersonation).

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, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person.

4(g): Cheating by personation by using computer resource (Impersonation).

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, by means of any communication device or computer resource cheats by personation.

4(h): Violation of privacy.

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 the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person:

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast:

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that–

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

4(i): Cyber terrorism.

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 ,–

(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; or

(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.

(2) Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the commission or conspiracy to commit the offence as described in para 1 (A) and 1(B).

.

4(j): Publishing or transmitting obscene material in electronic form communications.

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, publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

4(k): Publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

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, publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct.

4(l): Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

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, ,–

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
(d) facilitates abusing children online, or
(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

Provided this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or
(ii) which is kept or used for bona fide heritage or religious purposes.

The age of "children" is as defined in the domestic legislation of that state.

4(m): Disclosure of information in breach of lawful contract.

Save as otherwise provided in this Convention 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.

5. **"Other Unlawful acts committed using ICTs:"**

Without prejudice to (Article on protection of Sovereignty) the Contracting Parties shall mutually agree on any other unlawful acts committed using ICTs for the purpose of cooperation established under this Convention. (There should be a provision in this Convention titled "Other Unlawful Acts" considering the advancement in ICT technologies). In addition, the following cyber crimes may be further extended as criminalization through the UNODC document [3] through this convention.)

Illegal access
Illegal interception: interception without right, made by technical means, of non public transmissions of computer data to, from or within a computer system, including electromagnetic
Illegal interference
Computer misuse tools
Identity offences
Personal harm
Racism and xenophobia
Terrorism support offences
Ransomware

[3] (**Source:** *United Nations Office on Drugs and Crime(UNODC).***Comprehensive Study on Cybercrime Draft**—February 2013. Page.22)

How Criminalization of cyber crimes can be managed at the international level:

6. The development of international model provisions on criminalization of core cybercrime acts, with a view to supporting States in eliminating safe havens through the adoption of common offence elements:

(i) The provisions could maintain the approach of existing instruments regarding offences against the confidentiality, integrity and accessibility of computer systems and data;
(ii) The provisions could also cover 'conventional' offences perpetrated or facilitated by use of ICTs.
(iii) The provisions could address areas not covered by existing instruments, such as criminalization of SPAM;
(iv) The provisions could be developed in line with the latest international human rights standards on criminalization, including in particular, treaty-based protections of the right to freedom of expression;
(v) Use of the provisions by States would minimize dual criminality challenges in international cooperation;

7. The development of international model provisions on investigative powers for electronic evidence, with a view to supporting States in ensuring the necessary procedural tools for investigation of crimes involving electronic evidence.[4]

Importance of legal and technical assistance specific to cyber crime committed through use of ICTs and the issues likely to be dealt in the convention:

8. 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. Without adequate criminalization, law enforcement agencies will not be able to carry out investigations and identify those who put security at risk.

9. States at the international scenario face issues on transnational investigations, sovereignty, jurisdiction, extraterritorial evidence, and cooperation. When the crime occurs or its footprints are in more than one country, the issue of cooperation between the LEAs of the countries becomes essential to investigate the crime and prosecute the offender.

10. While many national laws have extra territorial jurisdiction, many countries consider that their national laws are inadequate to criminalize the cyber crimes or handle transnational cyber crime.

11. Due to volatile nature of electronic evidences, many states face stiff challenge in prosecuting cyber crimes. Evidences are not available in time as there is lack of coordination among LEAs due to issues of jurisdiction and non-agreement on sharing the non-content and content data.

---

[4] (**Source:***United Nations Office on Drugs and Crime(UNODC).***Comprehensive Study on Cybercrime Draft**—February 2013.)

12. Some other instances of issues that are likely to be faced by the proposed convention are mentioned below:

(i) Definition and age limit of child may vary from country to country. Though many countries prohibit production and distribution of child pornography the criminalization of possession and access of child pornography varies significantly.
(ii) For infringement of copyright and trademarks, some countries that do not have specific IPR law that prevents infringements. Such states use their general criminal law for prosecution of such offences, which would be inadequate for prosecuting high level crimes of commercial scale.
(iii) There needs to be a balance between International human rights law, freedom of speech and expression and requirements of the States cooperation to exchange of data for crimes and on criminals for effective, efficient prevention and countering the crimes committed through the use of ICTs.
(iv) In light of technological developments, the biggest challenge in accessing data due to emerging technologies such as Big Data, artificial intelligence, usage of clouds and CDNs, and the Internet of Things, lies in the fact that they may operate outside the framework of traditional privacy principles and converge in the new privacy laws of the states.

13. **Terms of Usage:**

(i) "communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;
(ii) "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;
(iii) "computer network" means the inter-connection of one or more computers or computer systems or communication device through–
    a. the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
    b. terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained;
(iv) "computer resource" means computer, computer system, computer network, data, computer data base or software;
(v) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
(vi) "computer contaminant" means any set of computer instructions that are designed–
    a. to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
    b. by any means to usurp the normal operation of the computer, computer system, or computer network;

(vii) “computer data-base” means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(viii) “computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(ix) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

(x) “computer source code” means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.

(xi) “cyber security” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;

(xii) “data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network or cloud, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(xiii) “information” includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer-generated micro fiche;

(xiv) “body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(xv) “reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the State parties in consultation with such professional bodies or associations as it may deem fit;

(xvi) “sensitive personal data or information” means such personal information as may be prescribed by the State parties in consultation with such professional bodies or associations as it may deem fit.

(xvii) “electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

(xviii) Social Media Intermediary: An intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.

(xix) Electronic Record: It means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

(xx) Originator: It means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

(xxi) Property”: It means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including money in bank accounts, digital financial

assets, digital currency, including cryptocurrency and legal documents or instruments evidencing title to, or interest in, such assets or any part thereof.

(xxii) "Proceeds of Crime": It shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence or other unlawful act as established under this convention.

(xxiii) "Confiscation": It includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority.

(xxiv) "Predicate Offence: It shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in this Convention.

(xxv) "Child Pornography" means any representation, by whatever means, or a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

14. **Data Oriented Jurisdiction**:

Data oriented jurisdiction means that the country whose citizen's data is being stored/processed/screened/federated anywhere in the world should be having the broader jurisdiction of the data immaterial of where the data is physically stored/ processed/ screened/ federated. This Data Oriented Jurisdiction will ensure the primality of data ownership and the issue of privacy (an acknowledged fundamental right of a global citizen) and human rights.

(Brief Explanation: In the current day scenario, the classical Westphalian model-based jurisdiction does not hold good in cyberspace especially involving cloud resources that result in jurisdictional nightmare. An example of a typical scenario may involve a cybercrime executed involving the processing power in the cloud originating from one country; the storage aggregation at another country; with the cloud service provider registered in a third country and the user (the victim and the attacker) whose data is being held by the service provider may be the resident of a fourth country. Clearly in such situation, it is extremely difficult to ascertain Jurisdiction based on the classical territorial models. In view of the above, India proposes that rather than territorial based jurisdictional model, the Convention adopts Data Oriented Jurisdiction. The data ownership which is linked to the privacy is an acknowledged fundamental right of a global citizen. This has been acknowledged by the European Court of Justice whereby it recognized the individual's right to be forgotten. The right to privacy is also linked to human rights which has been raised by large number of countries in UN AHC and the Data Oriented Jurisdiction will help protect the right to privacy, fundamental rights and human rights.)

15. **"JURISDICTION" may be defined as follows:**

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over offences established in accordance with this Convention when:

(a) The offence is committed in the territory of that State Party or having a bearing in the territory of the state party; or

(b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.

2. Subject to this Convention, a State Party may also establish its jurisdiction over any such offence when:

(a) The offence is committed against a national and, legal person of that State Party; or
(b) The offence is committed by a national and, legal person of that State party or a stateless person who has his or her habitual residence in its territory; or
(c) The offence is committed outside its territory with a view to the commission of an offence established in accordance with this Convention within its territory;
(d) the offence is committed against the State Party; OR
(e) The offence is committed targeting computer resource located within its territory
(f) The offence involves the digital/electronic data of their nationals, irrespective of the place of its physical storage/processing/screening/federation."

3. For the purposes of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other State Parties are conducting an investigation, prosecution, or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions. For the Purpose of consultation under this Article, the Contracting Parties shall take into account the Data Oriented Jurisdiction i.e. data belonging to the victim of the cybercrime or unlawful act committed using ICTs.

6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

16. **Convention may propose that timely cooperation among the agencies of the governments is essential to investigate and prosecute cyber crimes.**

(i) Timely responses and the ability to request specialized investigative actions, such as preservation of computer data for a period specified (the proposed international convention can specify the period for which the data can be preserved).
(ii) The proposed convention may recommend constitution of proper notified channels or points of contacts of communications or designated officers who may receive and process the request in a specific time. Escalation levels may also be notified.
(iii) Such notified channels or points of contacts may serve 24/7 networks, offer important potential for faster response times.
(iv) LEAs of states may be trained regularly through international LEAs such as INTERPOL on how speedy assistance can be rendered in cases and their need to support the investigation process since the crimes are transnational in nature.
(v) Investigations that affect the state sovereignty, crimes against women and children, religious or communal content, or prohibited drugs must be accorded high priority that information is shared within a short timeline of not more than 24 hours.

(vi) States enact or modify their existing legislations to ensure that internet service providers and domain registrars or cloud service providers respond to the request of the state law enforcement agencies and provide the requisite information in the stipulated time. States shall develop SOPs in this regard.

(vii) States enact law in their jurisdiction that privacy protection in the WHOIS details of the domains/websites is not absolute and that the details sought by the LEAs (state and international) shall be duly provided by the domains/websites.

(viii) States shall treat requests of member Countries' Law enforcement agencies on par with the requests of their own state law enforcement agencies and ensure that they are attended to in shortest time frame.

(ix) States may only prescribe the permissibility of transfers of sensitive personal data where it finds that the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements / conventions, and the effectiveness of the enforcement by authorities with appropriate jurisdiction, and shall monitor the circumstances applicable to such information.

17. "SEARCH AND SEIZURE OF INFORMATION STORED OR PROCESSED ELECTRONICALLY"

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

(a) a computer system or part of it and computer data stored therein; and
(b) a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a) and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

(a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
(b) make and retain a copy of those computer data;
(c) To preserve / maintain integrity of the computer data

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

18. **REAL-TIME COLLECTION OF TRAFFIC DATA**”

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

(a) collect or record through the application of technical means on the territory of that Party; and

(b) compel a service provider, within its existing technical capability:

(i) to collect or record through the application of technical means on the territory of that Party; or

(ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1(a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

19. **“COLLECTION OF CONTENT AND META DATA”**

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

2. 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.

20. **“INTERCEPTION OF CONTENT DATA”**

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

(a) collect or record through the application of technical means on the territory of that Party, and
(b) compel a service provider, within its existing technical capability:
(i) to collect or record through the application of technical means on the territory of that Party; or
(ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

21. "**EXPEDITED PRESERVATION OF STORED COMPUTER DATA"**

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic and content data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 180 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

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

22. "MECHANISMS FOR FORFEITURE OF PROPERTY THROUGH INTERNATIONAL COOPERATION IN CONFISCATION"

1. 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, or the means of committing such an offence, shall, in accordance with its domestic law:
    a) Take such measures as may be necessary to enable its competent authorities to give effect to an order of confiscation issued by a court of another State party;
    b) 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;
    c) 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.

2. Each State party, for the purpose of providing mutual legal assistance, at the request of another State party, shall, in accordance with its domestic law:
   a) Take such measures as may be necessary to permit its competent authorities to seize property pursuant to an order of seizure issued by a court or other competent authority of the requesting State party that provides a reasonable basis for the requested State party to believe that there are sufficient grounds for taking such measures and the property would eventually be subject to a confiscation order for the purposes of paragraph 1(a) of this Article;
   b) Take such measures as may be necessary to permit its competent authorities to seize property upon request that provides a reasonable basis for the requested State party to believe that there are sufficient grounds for taking such measures and that the property would eventually be subject to a confiscation order for the purposes of paragraph 1(a) of this Article;
   c) Consider taking additional measures to permit its competent authorities to retain the property for confiscation purposes, for example, based on a foreign seizure order or criminal charges in connection with the acquisition of such property.

(The draft text is shared 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 Ad Hoc Committee.)

******