*Fourth session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*

Overview of written proposals submitted for Group B

CLUSTER 8

Article 26. Incitement to subversive or armed activities

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law a call issued by means of information and communications technologies for subversive or armed activities directed towards the violent overthrow of the regime of another State.

Article 27. Extremism-related offences

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences the distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic or religious hatred, the advocacy and justification of such acts and the provision of access to such materials by means of [a computer system] [information and communications technology system/device].

*Article 27 Alt: Prohibition of incitement to Violence*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, the dissemination or advocacy of national, racial or religious hatred, threat and insult that constitutes incitement to discrimination, hostility or violence or otherwise making available, racist and xenophobic material against (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristic, through an information and communication technology system.

(Pakistan)

Article 28: Denial, approval, justification or rehabilitation of genocide   
or crimes against peace and humanity

Each State Party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the [computer-related] [information and communications technology-related] intentional dissemination of materials that deny, approve, justify or rehabilitate actions that amount to genocide or crimes against peace and humanity, established by the Judgment of the International Military Tribunal formed under the London Agreement of 8 August 1945.

*Art. 28 bis - Fake news*

Each SP shall adopt such legislative and other measures as may be necessary to establish as criminal offences, committed intentionally, publishing or republishing or distributing of disinformation or fake news or false statements.

(a) A statement is false if it is a false or misleading, whether in whole or in part, or whether on its own or [x] its appears.

(b) Each MS shall, by enacting laws or taking other necessary measures, ensure that all information and communications tech service providers, especially transnational ICTs service providers, [xx] and take the necessary measures in the shortest possible time to prevent the spread of false and misleading news, such as tagging and deleting this content.

(c) Each SP may impose an aggravation of penalty for committing the above acts in circumstance that cause serious harm to the health or safety or society, or use robots or fake account to commit it, or are committed in an organized manner.

(Islamic Rep. of Iran)

CLUSTER 9

Article 29. Terrorism-related offences

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed by means of information and communications technologies, the commission of terrorist acts, the incitement, recruitment or other involvement in terrorist activities, the advocacy and justification of terrorism or the collection or provision of funds for its financing, training for terrorist acts, the facilitation of communication between terrorist organizations and their members, including the establishment, publication or use of a website or the provision of logistical support for perpetrators of terrorist acts, the dissemination of methods for making explosives employed in particular in terrorist acts, and the spreading of strife, sedition, hatred or racism.

*Art 29 bis*

1.Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed by means of information and communications technologies, producing, publishing, distributing, transmitting or otherwise making available of materials advocating terrorism, including but not limited to photographic, video and live-streaming media, as well as drawings, written material and audio recordings.

2. Terrorism and materials advocating terrorism shall be defined in accordance with domestic laws of each State Party.

3. A State Party may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed by means of information and communications technologies, possessing material as defined in para.1 of this article.

(China)

Article 30. Offences related to the distribution of   
narcotic drugs and psychotropic substances

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, illicit trafficking in narcotic drugs and psychotropic substances and materials necessary for their manufacture through the use of [an information and communications technology system/device] [a computer system].

Article 31. Offences related to arms trafficking

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, illicit trafficking in arms, ammunition, explosive devices and explosive substances by means of information and communications technologies.

Article 32. Illegal distribution of   
counterfeit medicines and medical products

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, the intentional and illegal distribution of counterfeit medicines and medical products by means of information and communication technologies.

*Trafficking in persons*

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences trafficking in persons, as it’s stipulated by the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, committing by means of information and communication technologies.

(Belarus)

[No title]

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, trafficking in persons through the use of information and communications technologies.

(Eritrea)

*Article 30 bis. Trafficking in persons*

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences trafficking in persons, as defined in the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, committed or facilitated by means of information and communication technologies.

(Philippines)

*Offenses related to organized or transnational crime committed using information and communications technologies*

Each State party shall adopt, in accordance with its domestic law, such legislative and other measures as are necessary to criminalize the following acts, where the means of ICTs are used to:

1. Promoting or trafficking in narcotic drugs or psychotropic substances;

2. Illicit distribution of counterfeit medicines or medical products;

3. Smuggling of migrants;

4. Illicit trafficking in persons;

5. Illicit arms trade; and

6. Illicit trafficking in cultural property.

(Egypt)

*Efforts to prevent and counter cyber–enabled crimes* (placing TBC)

1. State Parties shall undertake appropriate measures to prevent and counter the use of computers or computer systems for the commission of cyber–enabled crimes, including but not limited to fraud, identity theft, sexual exploitation and abuse, particularly against children, infringement of copyrights, incitement to discrimination, hostility or violence in all its forms and manifestations, acts related to terrorism, and trafficking in persons, drugs, firearms, cultural goods, counterfeit products, including medical ones, among others.

2. For the purpose set forth in paragraph 1, State Parties shall, inter alia, take advantage of appropriate provisions of existing international instruments.

3. State Parties shall keep under examination the evolution of the scale, reach and nature of all cyber–enabled crimes in order to adapt their responses accordingly.

*Article 2. Use of terms*

* Cyber-dependent crime: illicit conduct that in order to be committed requires the use of computers or computer systems;
* Cyber enabled crime: illicit conduct which can be increased in its scale, reach or nature by use of computers or computer systems;

(Mexico)

*Offences relating to other UN Conventions and Protocols*

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed in violation of applicable UN Conventions and Protocols using cyber or information technologies.

(South Africa)