India Statement 2.9.2022

III. Preventive measures

Madam Chair,

32. Cyberspace has distinct and unique characteristics compared to physical space. It is virtual, borderless and offers anonymity to an extent. At present, social networking has emerged as a key tool used by people around the world. Its purpose is to promote and aid communication. However, it also has the potential to do a great deal of harm. Of late, use of social media has been seen as a key tool for engineering psychological manipulation of public and its opinion on issues that affect nation and society. It is being used to radicalise the youth and means of financing of terrorism.

With widespread proliferation of new technologies, there are some miscreants who are misusing these technologies for committing cybercrimes against vulnerable groups, particularly against children. Confronting the challenges of the cyber space and dealing with cyber crimes against children depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures for the safety and security cyber space require broad international cooperation to be effective. In light of the growing cyber crimes, particularly against children worldwide, there is a need for all of us to come forward to cooperate and collaborate. Capacity-building is of vital importance. Close international cooperation will be needed to build capacity in addressing these issues.

Therefore, through this convention, there is a need for provisions to prioritize cyber crimes against children and to resolve such cases swiftly and provide justice. A dedicated 24/7 channel can be deployed to deal with such crimes and there should be zero tolerance among the member states to crime against children.

The chapter on preventive measures can focus on :

a. Promotion of policies and best practices to prevent cyber crime.
b. Reduce opportunities for cyber criminals.
c. Increased participation and cooperation between states and private sector, civil societies.
d. Increasing awareness among end users, especially vulnerable groups including women, children, and the elderly.
e. Intelligence sharing of ongoing attacks, vulnerabilities.
f. Sharing of tools which can detect and remove harmful contents online including malwares and CSEM.
g. Developing and sharing analytical expertise concerning cybercrime with each other and though international and regional organizations.
h. Creation of multilateral repository for dissemination of good practices
33. Targeting critical infrastructure by cyber criminals requires high degree of international cooperation to avert and mitigate such incidents. This is possible only when the Convention builds faster exchange of non-content and content data and resolves the issues of jurisdiction on data for criminal purposes under this convention. Such incidents may be brought under the category of emergency request.

34. The Convention requires cooperation from civil society, private sector in all aspects including prevention, detection, investigation, intelligence gathering, sharing of standard techniques and awareness creation.

36. Yes India believes that private sector is the primary stake holder in ensuring that its resources and channels are not used for cyber crime. Some responsibility should be identified especially in case of financial institutions. The domestic laws should also be harmonized in accordance with the convention.

37. The convention should encourage States parties to raise awareness as follows:

(a) Enhancing the transparency of and promoting the contribution of the public to decision-making processes;

(b) Ensuring that the public has effective access to information related to cyber threat, awareness material and cyber hygiene;

(c) Undertaking public information activities that contribute to cyber safety, as well as public education programmes, including school and university curricula;

(d) Enhancing cooperation with all stakeholders including private sector financial institutions.