SUBMISSION OF VIETNAM
FOR THE THIRD SESSION OF AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF ICTS FOR CRIMINAL PURPORSES

*Viet Nam welcomes results from the second Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes. In response to the request of the Ad Hoc Committee to provide draft provisions to be examined by the third Session, Viet Nam is pleased to propose some key elements to be included in the parts "**International Cooperation**", "**Technical Assistance**", "**Preventive Measures**" and "**Mechanism of Implementation and Final Provisions**" of the future Convention, as the followings:*

A. Preventive Measures

1. Policies and practices to prevent and combat cybercrime/the use of ICTs for criminal purposes

1. States Parties shall endeavour to establish and promote best practices and policies aimed at the prevention of cybercrime/using ICTs for criminal purposes and other unlawful acts relating to ICTs use.

2. States Parties shall endeavour to prevent their own territory or computer systems/ICTs systems/ICTs devices located on their territory from being used for criminal purposes against the other third parties and/or citizens of other Parties.

3. States Parties shall endeavour, in accordance with fundamental principles of their domestic law, to reduce existing or future opportunities for cyber criminals/criminals using ICTs to participate in lawful markets with proceeds of crime, through appropriate legislative, administrative or other measures. Such measures should include the promotion of regulations and procedures designed to supervise virtual assets trading and cryptocurrency exchange platforms.

4. States Parties shall endeavour to take appropriate measures to prevent reoffending, including reoffending targeting victims in other States Parties.

5. States Parties shall, as appropriate and in accordance with the fundamental principles of their legal systems, collaborate with other member states, governmental organizations, relevant international and regional organizations in promoting and developing the measures referred to in this article.

6. States Parties shall endeavour to promote the reintegration into society of persons convicted of offences covered by this Convention.

2. Raising public awareness of cybercrime prevention

1. States Parties shall endeavour to promote public awareness regarding the existence, new forms, characteristics, gravity of and the threat posed by cybercrime/the use of ICTs for criminal purposes.

2. State Parties shall encourage government agencies to cooperate with private organizations and other individuals in running education, training and public awareness raising programs on preventing and combating cybercrime/using ICTs for criminal purposes.

3. Public sector

1. States Parties shall take appropriate measures, in accordance with the fundamental principles of its domestic law, to prevent offences covered by this Convention and other acts of cybercrime/using ICTs for criminal purposes in governmental organizations.

2. States Parties shall take appropriate measures, in accordance with the fundamental principles of its domestic law, to prevent computer systems/ICTs systems/ICTs devices and resources under control of governmental organizations from being abused in offences covered by this Convention and other acts of cybercrime/using ICTs for criminal purposes.

4. Private sector

1. Each State Party shall take appropriate measures, within its means and in accordance with fundamental principles of its domestic law, to promote the active participation of private sector, including internet service providers, in the prevention of and the fight against cybercrime/the use of ICTs for criminal purposes.

2. Each State party shall take appropriate measures, in accordance with the fundamental principles of its domestic law, to prevent offences covered by this Convention and other acts of cybercrime/using ICTs for criminal purposes in the private sector.

5. Products control

States Parties shall endeavour, in accordance with fundamental principles of their domestic law, to establish policies of quality control of products applied in the protection of computer systems/ICTs devices before such products are released to public.

B. International Cooperation

6. International Cooperation

1. States Parties shall cooperate in investigating offences covered by this Convention as well as any other acts of cybercrime/using ICTs for criminal purposes. Where appropriate and consistent with their domestic legal system, States Parties shall consider assisting each other in investigations of and proceedings in civil and administrative matters relating to cybercrime/the use of ICTs for criminal purposes.

2. In matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the

same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties[1].

7. International cooperation in raising awareness of public

1. States Parties shall cooperate in the promotion of public awareness regarding the existence, new forms, characteristics, gravity of and the threat posed by cybercrime/the use of ICTs for criminal purposes.

2. State Parties shall cooperate in running education, training and public awareness raising programs on preventing and combating cybercrime/using ICTs for criminal purposes.

8. Information exchange

Each State Party shall, in accordance with fundamental principles of their domestic law**,** adopt effective measures to enhance and, where necessary, to establish as well as utilize existing channels of communication between its competent authorities and competent authorities of another State Parties in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including early warning to the other Parties, if the Parties concerned deem it appropriate, links with other criminal activities.

9. Freezing, seizure and confiscation

Article 31 of UNCAC and Article 12 of UNTOC may be applied, *mutatis mutandis*, to acts of cybercrime/using ICTs for criminal purposes. However, the notion of proceeds of crime should be defined so as to cover crypto currency or other data the value of which can be identified in the market.

10. General provisions on asset recovery

States Parties shall afford one another the widest measure of cooperation and assistance regarding the return of assets.

11. Measures for direct recovery of property

Article 53 of UNCAC may be applied, *mutatis mutandis*, to acts of cybercrime/using ICTs for criminal purposes.

12. Mechanisms for recovery of property through international cooperation in confiscation

Article 54 of UNCAC may be applied, *mutatis mutandis*, to acts of cybercrime/using ICTs for criminal purposes.

13. International cooperation for purposes of confiscation

Article 55 of UNCAC may be applied, *mutatis mutandis*, to acts of cybercrime/using ICTs for criminal purposes.

C. Technical assistance

[1] For example, the server used for operating online gambling and the organization which operate such platform located in a State Party where online gambling, even unregulated online gambling operation, is not a crime as such, involve tax evasion, labor abuse, human trafficking, etc.

14. Technical assistance

1. State Party shall endeavour to provide, subject to availability of resources, technical assistance programmes to developing and least developed State Parties, upon request from such developing or least developed State Parties, to enhance capabilities of competent authorities charged with the prevention, detection and control of the offences covered by this Convention. Such programmes may include the following:

a. Capacity building and capacity development in policies making;

b. Sharing experience and best practices to prevent, detect, investigate, punish acts of cyercrime/using ICTs for criminal purpose, including collecting, analyzing, recovering digital data, and investigative methods in cyber space.

c. Effective response in cyber incidents;

d. Effective measures to safeguard national critical information infrastructure;

e. Data security solutions including personal data;

f. Training of experts in cyber security and computer network defense;

g. Enhancing public awareness and best practices for safe use of Internet

2. States Parties shall assist one another in planning and implementing research and training programmes designed to share expertise in the areas referred to in paragraph 1 of this article and to that end shall also, when appropriate, promote cooperation and to encourage discussion on issues of mutual interest through regional and international conferences and seminars.

3. States Parties shall encourage dialogue and exchanges between relevant authorities, including through personnel secondments, capacity building and development programs.

4. States Parties shall promote the transfer of technologies, equipment, software, technical solutions aiming at prevention and countering cybercrime/act of using ICTs for criminal purposes./.