SUBMISSION OF VIETNAM
FOR THE SECOND 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 first Session of 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 Ad Hoc Committee to provide draft provisions to be examined by the second Session, Viet Nam is pleased to propose some key elements to be included in the parts "**General Provisions**", "**Criminalization**" and "**Procedural measures and Law enforcement**" of the future Convention, as the followings:*

Chapter I. General Provision

1. Objectives

a. To promote and strengthen measures to prevent and combat use of ICTs for criminal purposes;

b. To promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against the use of ICTs for criminal purposes, including asset recovery, in accordance with fundamental principles of international law and in a manner of respecting human rights.

2. Scope of application

This Convention shall apply to the prevention, investigation and prosecution of use of ICTs for criminal purposes.

3. Protection of Sovereignty

a. Member States shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality, territorial integrity of States, non-threat or use of force, or non-intervention in the domestic affairs of other States.

b. Nothing in this Convention shall allow a Member State to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other Member State by its domestic law.

4. Definitions

a. **Cyberspace** means a network of information technology (IT) infrastructure which includes telecommunications networks, the Internet, computer networks, communication systems, information processing and control systems, databases;

b. **Information system** means a combination of hardwares, softwares and databases established to serve the creation, transmission, collection, processing, and storage of information in cyberspace;

c. **Cyberattack** means the use of cyberspace, information technology or electronic devices to sabotage or interrupt the telecommunications network, the Internet, computer network, communication systems, information processing and control systems, databases or electronic devices;

d. **Cyberterrorism** means an act of terrorism or financing of terrorism which involves the use of cyberspace, information technology or electronic devices;

e. **Personal information** means information associated with the identification of a natural person;

f. **Digital data** is composed of signals, letters, numbers, images, sound or similar elements created, stored and transmitted or acquired through electronic means;

g. **Cyberspace infrastructure** means a system of infrastructure serving creation, transmission, collection, processing and storage of information and data in the cyberspace.

Chapter II. Criminalization

5. Each Member State shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed unauthorizedly and intentionally:

a. To manufacture, trade, transfer instruments, equipment or software meant to attack a computer network, telecommunications network or an electronic device which to be used for criminal activities as governed in this Convention;

b. To spread a software program that is harmful to a computer network, telecommunications network or an electronic device;

c. To delete, sabotage or modify a software program or digital data;

d. To obstruct the transmission of data of a computer network, telecommunications network or an electronic device;

e. To obstruct or disturb normal operations of a computer network, telecommunications network or an electronic device;

f. To take control or interfere in the operation of an electronic device by bypassing security or protection system, abusing the rights of administration of another person, or any other means;

g. To steal, modify, sabotage or counterfeit information or data;

h. To uses a computer network, telecommunications network or electronic device for the following purposes:

(i) Using information of bank account or bank card of an organization or an individual to illegally appropriate assets;

(ii) Manufacturing, possessing, trading or using counterfeit bank card in order to illegally appropriate assets;

(iii) Unauthorized accessing accounts of government agencies, organizations and individuals for illegal appropriation of assets;

(iv) To committ frauds in e-commerce, electronic payment, online currency trading, online capital rising, online multi-level marketing or online securities trading for the purpose of property appropriation;

(v) Unauthorized establishing or providing telecommunication or Internet service for the propose of property appropriation;

i. To collect, possess, trade, transfer or publicize information of bank account of individuals and organizations.

j. To trade, transfer, modify, publicize private information of government agencies, organizations or individuals without a consent of the owners.

k. To use cyberspace, information technologies or electronic devices to undertake an act of terrorism or terrorist financing.

6. Nothing in this Convention shall prevent Member States to adopt such legislative and other measures as may be necessary to establish as criminal offences of any other act involving the use of ICTs for criminal purposes.

7. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention 24 and of the applicable legal defenses or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a Member State and that such offences shall be prosecuted and punished in accordance with that law.

Chapter III. Procedural measures and law enforcement

8. Jurisdiction

a. Each Member State shall take such measures as may be necessary to establish its jurisdiction over the offences referred to in articles … in the following cases:

(1) When the offences are committed in any territory under its jurisdiction or on board a ship or aircraft registered in that State;

(2) When the alleged offender is a national of that State;

(3) When the victim is a national of that State if that State considers it appropriate.

b. This Convention does not exclude any criminal jurisdiction exercised by a State in accordance with its domestic law.

9. Powers of competent authorities:

Member States shall:

a. To undertake measures of prevention, identification, investigation, prosecution and judicial proceedings of commissions relating to criminal offences covered by this Convention.

b. To collect evidence relating to offences covered by this Convention, including digital data in a manner of protection of sovereignty of other Member States./.