(Translation)

China's Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes

China welcomes the invitation by the Chair of the UN *Ad Hoc* Committee on the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communication Technologies (ICTs) for Criminal Purposes to Member States to submit their views on the scope, objectives and structure (elements) of the Convention. In accordance with the General Assembly Resolution 75/282, the *Ad Hoc* Committee shall submit a draft convention to the General Assembly at its 78th session. China looks forward to constructive discussions under the leadership of the Chair to reach a new convention that is universal, authoritative and acceptable by all parties as scheduled, so as to provide a legal framework for strengthening cooperation in combating cybercrime worldwide.

Up to now, Member States have conducted in-depth discussions on combating cybercrime in relevant United Nations mechanisms and reached some agreed conclusions and recommendations. A draft comprehensive convention has also been put forward by one Member State to provide an important reference for the negotiation of the Convention. China appreciates the efforts of the Chair for encouraging Member States to actively submit their views and draft proposals, and supports the Chair to prepare a zero draft of the convention based on the submissions of Member States, so as to initiate negotiations on the text of the Convention as soon as possible.

In order to support the work of the Chair and the *Ad Hoc* Committee, China has drafted its views on the scope, objectives and structure (elements) of the Convention, and is willing to carry out constructive negotiations with all parties.

I. Objectives

To promote and strengthen measures to prevent and combat the use of ICTs for criminal purposes more efficiently and effectively with the aim to uphold the vision of a community with a shared future in cyberspace;

To promote, facilitate and support international cooperation in preventing and combating the use of ICTs for criminal purposes, bearing in mind the particularity of ICTs and the need to combat related criminal activities. Those international cooperation may include coordinating criminalization among Member States, providing guidance for resolving jurisdictional conflicts, and developing more targeted institutional arrangements in law enforcement cooperation, legal assistance, extradition and asset recovery;

To strengthen cooperation in capacity building and technical assistance, and promote the exchange of information in this field, based on the needs of broader international cooperation and the interests of the developing countries;

II. Scope of Application

This Convention shall apply to the prevention, investigation and prosecution of the use of ICTs for criminal purposes committed by individuals or criminal groups, as well as the sealing, freezing, seizure, confiscation and return of the proceeds of relevant crimes.

The use of ICTs for criminal purposes should at least include crimes against ICTs facilities, systems and data as well as crimes committed using ICTs.

III. Structure (Elements)

This Convention can be divided into seven chapters: General Provisions, Prevention, Criminalization and Law Enforcement, International Cooperation, Technical Assistance and Information Exchange, Implementation Mechanism and Final provisions.

The preliminary suggestions on the elements of relevant chapters are as follows:

1. General Provisions

In addition to the objectives and scope of application, it shall also include the following content:

① Protection of Sovereignty. The principle of sovereign equality enshrined in the Charter of the United Nations is the basic norm of contemporary international relations. The application of the principle of sovereignty to cyberspace has also been widely supported by Member States. This Convention should specify that the States Parties shall carry out their obligations under this Convention in accordance with the principles of sovereign equality and territorial integrity and non-interference in the domestic affairs of other States.

② Terminology. Definitions may be given to important terms mentioned in this Convention such as "electronic evidence", "personal information", "critical information infrastructure", "cloud storage", "network service provider", "malware", "botnet", "harmful information" and "cyberattack".

2. Prevention

The importance of preventing the use of ICTs for criminal purposes should be highlighted. The basic principle should be "putting prevention first while combating crime simultaneously". The responsibilities of governments and the private sector in crime prevention should be clarified; governments should formulate targeted crime prevention measures, while encouraging social participation and public-private cooperation. The following points should be included:

① Member States are encouraged to designate specialized agencies for developing policies on the prevention of the use of ICTs for criminal purposes, and conducting assessments on a regular basis. Member States should establish the security protection system of critical information infrastructure and network security system based on leveled evaluation. Different information security technologies and management measures should be adopted for different network facilities, and protect critical information infrastructure from being attacked by criminals or criminal groups. The capacity-building of relevant government departments should be strengthened in crime prevention.

② Member States should enact or improve domestic legislations to clarify the responsibilities of the private sector, such as network service providers, in preventing the use of ICTs for criminal purposes. Those responsibilities may include security

precautions (for example, formulating emergency plans for network security accidents, dealing with system and hardware vulnerabilities, computer viruses, network attacks and network intrusion in a timely manner, and take real-time measures when its services are found possibly to be used for criminal activities), log information retention (governments shall specify the content standard and duration of log information retention), etc. When determining the responsibilities of network service providers, leveled arrangements consistent with the principle of proportionality shall be made by taking full consideration of the differences in capabilities of network service providers of different sizes.

③ Governments, private sector and communities are encouraged to carry out various forms of public-private cooperation. In particular, more efforts should be made available to enhance the public's awareness of crime prevention.

3. Criminalization and Law Enforcement

At present, more criminals and criminal groups are abusing ICTs to commit crimes. This also breeds a dark "product chain" that specializes in the development of ICTs for criminal purposes and transaction of such technologies and relevant data. This Convention should, based on the current and future development of ICTs and the needs of combating crimes, provide a more flexible and forward-looking framework in coordinating criminalization. The Convention should also provide relevant mechanisms in terms of jurisdiction, law enforcement and electronic evidence.

① Member States are requested to criminalize the intrusion and destruction of ICTs facilities, systems, data or critical information infrastructure. This may include illegal access to computer information systems, illegal interference with computer information systems, illegal acquisition of computer data, illegal interference with computer data, infringement of critical information infrastructure, etc.

② This Convention may enumerate, as appropriate, the criminal activities committed by using ICTs and broadly recognized by the international community, including cyber extortion, cyber fraud, cyber pornography, especially child pornography, the use of ICTs to infringe copyright and neighboring rights, the use of Internet to incite, commit acts of terrorism, disseminate harmful information, etc.

③ With regard to other crimes committed by using ICTs, it may be noted that Member States could prevent and combat relevant crimes, which are not listed in this

Convention, and carry out international cooperation in accordance with this Convention, other international conventions and their respective domestic laws.

④ In view of the increasing "industrialization" of crimes committed by using ICTs, the dark "product chain" should be included in the scope of criminalization, and the crackdown on aiding and preparatory acts should be toughened, including the development, sale and dissemination of ICTs and data for crime.

⑤ With regard to "electronic evidence", the rules for identifying electronic evidence in criminal judicial procedures should be stipulated, including how to identify the authenticity, integrity, legitimacy and relevancy of electronic evidence.

⑥ Member States should be requested to formulate or improve domestic legislations to clarify the obligations of private sector, such as network service providers to cooperate with law enforcement authorities in monitoring, investigating and combating crimes. Such obligations may include retaining log information, preserving data, crystalizing evidence in accordance with unified content standards and durations, and cooperating with law enforcement, etc. When determining the obligations of network service providers, leveled arrangements consistent with the principle of proportionality shall be made by taking full consideration of the differences in capabilities of network service providers of different sizes. If a network service provider fails to perform its relevant obligations, Member States shall impose effective administrative and criminal penalties on it in accordance with their domestic laws.

⑦ Guidance should be provided for resolving jurisdictional conflicts. Based on the particularity of cyberspace and ICTs, it is advised to provide guiding standards on how to determine jurisdiction and avoid jurisdictional conflicts. Jurisdiction should be based on the "true and sufficient" link with criminal activities, giving priority to the place where the consequence of criminal activity occurs, the place where the crime is committed and the place where the perpetrator (criminal group) is located. If it is difficult to form relevant standards, it is advised to put forward exclusion standards, for example, a State cannot claim jurisdiction over relevant cases only on the ground that the data pass through that State. In case of jurisdictional conflicts, the jurisdiction should be determined through consultation in accordance with the principles of *forum conveniens* and facilation of asset recovery.

⑧ Provisions on abetting and aiding in crime, crime preparation, attempted crime,

crime committed by an entity, etc., should be included in this convention.

4. International Cooperation

The use of ICTs for criminal purposes is highly transnational and is a common challenge to the international community. In addition, the anonymity and intelligence of criminal activities and the instability and perishability of electronic evidence bring greater challenges to international cooperation mechanisms such as mutual legal assistance under the existing international legal framework. Member States should cooperate with each other to the widest extent in preventing and combating the use of ICTs for criminal purposes, uphold the principle of reciprocity, actively explore institutional innovation and propose new mechanisms for more targeted international cooperation.

① Cross-border electronic evidence collection is necessary for combating the use of ICTs for criminal purposes, but Member States should respect the sovereignty of the State where the evidence is located. Member States should also abide by due process, respect the legitimate rights of relevant individuals and entities, and should take no invasive and destructive technical investigation means in cross-border electronic evidence collection. States shall not directly collect the data stored in foreign States from enterprises or individuals or by technical means bypassing network security protection measures if such measures are against the laws of that Foreign State. Member States should explore new institutional arrangements for collecting overseas electronic evidence. This may include mutual entrustment for electronic evidence authentication and video (audio) evidence collection, unified and authoritative guidance for cross-border electronic evidence collection while balancing different aims of respecting national sovereignty and combating crime.

② Member States should formulate mechanisms for rapid law enforcement cooperation. Member States can designate specific agencies for liaison, allowing rapid exchange of criminal clues, provision of technical advice and other law enforcement cooperation in case of special needs.

③ In order to improve the efficiency of mutual legal assistance in criminal cases, Member States can establish a rapid liaison and response mechanism between competent authorities to ensure real time correspondence. Transfer of legal documents and electronic evidences required for cross-border evidence collection could be done

online through technical means such as electronic signature, under the framework of the national cross-border data transmission security management system. Mutual legal assistance in emergency cases could also be formulated, including expedited preservation of electronic evidence, expedited disclosure after data preservation, etc.

④ Member States, especially those with advanced network resources, should take the lead in strengthening international cooperation. If ICTs facilities, systems or networks owned by network service providers of State A are used by suspects of another State for crime, as long as State A also criminalizes such acts, State A shall, on its own initiative or at the request of the other State, require relevant network service providers to take technical measures and other necessary measures to effectively respond to criminal activities. Such measures should be in line with the domestic laws as stipulated in para 2 of Prevention.

⑤ Relevant measures should be strengthened to prevent and block the international transfer of proceeds of crime and strengthen international cooperation in asset recovery. Member States should follow the principle of rapid and effective asset recovery, and should not set other preconditions for asset recovery other than judicial procedures.

5. Technical Assistance and Information Exchange

In order to effectively prevent and combat the use of ICTs for criminal purposes, it is essential to provide technical assistance to developing countries and strengthen the exchange of information.

① Technical assistance to developing countries should include:

Training of law enforcement and judicial personnel;

Training of professional teams with both legal literacy and technical knowledge;

Strengthening the capacity-building of electronic evidence collection;

Providing relevant equipments and technology, as appropriate, to help developing countries strengthen their capacity to combat crimes;

Encouraging international organizations such as UNODC, private sector, experts and scholars to participate in technical assistance and capacity-building.

② Member States are encouraged to share their experiences in the formulation and implementation of laws and policies, and share data related to preventing and

combating crimes and crime trends.

6. Implementation Mechanism

In order to promote the implementation of this Convention, the Conference of the State Parties and relevant expert groups or working groups, such as the working group on technical assistance and the working group on international cooperation, should be established. These meetings could also provide a platform for State Parties to exchange experience and promote cooperation.

7. Final Provisions

N/A