Comments of China

1. General comments

Cybercrimes are increasingly transnational, anonymous and intelligent. Electronic evidence is volatile and easily lost. This poses extraordinary challenges to law enforcement, investigation and criminal justice. International cooperation mechanisms like mutual judicial assistance under the existing international legal framework need to adapt to these challenges. Certain practices of trans-border access to electronic evidence may bring worrisome impact on the principle of sovereignty and other fundamental principles of international law, on due process and the security of personal data. There is a pressing need for the international community to speed up international legislation, harmonize the laws and practices of all states on combating cybercrime and provide universally accepted solution to the problem.

The proposals put forward by United Nations Intergovernmental Expert Group on Cybercrime in the Draft Comprehensive Study on Cybercrime, such as the development of international model provisions on investigative power for electronic evidence, an international instrument on electronic evidence and a binding multilateral instrument on cybercrime, deserve full attention and deliberation. China supports that the Expert Group continue its work according to the work-plan for the period of 2018-2021, encourages member states to share practices and experience on cybercrime law enforcement and investigation, electronic evidence and criminal justice, and supports the Group to submit its recommendations and conclusions within the scheduled time frame to the Commission on Crime Prevention and Criminal Justice (CCPCJ）.

2. China's Practice on Cybercrime Law Enforcement and Investigation

On the legislation side, China has amended the criminal law to criminalize the acts of "failing to perform the information network security management obligation", "illegal use of information network" and "aiding information network crime". Judicial interpretations about these provisions are to be issued this year to provide legal basis for enhanced action against aiding and preparatory acts of cybercrime.

In order to facilitate the establishment of jurisdiction domestically, China has adopted relevant rules to clarify the scope of "situs of a crime " , including, among others, the location of the web server, the location where the network is connected, the location of the website builder or administrator, the location of the infiltrated computer system or its administrator, the location where the computer system is used by the criminal suspect, the location of the victim, and the location of the property loss.

In terms of law enforcement, China's Law Enforcement Authorities launched actions against cybercrime last year, targeting crimes of personal data infringement, hacker-attack, cyber-fraud, cyber-gambling, cyber-pornography and cheating in exams by means of internet.

With respect to international cooperation, China's Law Enforcement Authorities have received and responded to more than 1000 requests for investigation assistance and information from Interpol and mutual judicial assistance and bilateral police cooperation channels, and have established law enforcement cooperation networks with more than 70 countries and regions.

From the perspective of China's practices on cybercrime law enforcement and investigation, the following challenges are outstanding:

First, the difficulty of attribution and identification of criminal suspects due to increased covertness of cybercrime. Cybercrime offenders increasingly use proxy service, VPN service and encryption to mask true identification.

Second, the difficulties in international cooperation against the backdrop of increasing need for trans-border collection of evidence. A significant number of crimes are committed using cyber resources abroad, and leave key evidence outside China. Trans-border evidence collection through mutual judicial assistance and international police cooperation channels are complex and time-consuming due to differences in legal system and inefficiency of cooperation.

Third, the increasing difficulty in law enforcement and investigation, as cybercrime becomes more and more organized and sophisticated. Cybercrimes have formed a dark industry chain, infested with professional criminal groups who cooperate and share criminal proceeds. More and more crimes are committed by such groups in a coordinated manner from preparation, organization, execution to selling and splitting criminal proceeds.

3. China's Practice on Electronic Evidence and Criminal Justice of Cybercrime

China has adopted two specific regulations on electronic evidence since electronic data was introduced as admissible evidence by law in 2012. The Regulations define "electronic evidence" as data that is formed

during the commission of a crime, stored, processed, and transmitted in digital form and can prove the facts of the crime. Some common types of electronic evidence are also included in an open-ended list. More importantly, the Regulations further specified the rules on the collection and admissibility of electronic evidence in more detail.

In terms of electronic evidence collection, the Regulations provide for a series of methods such as gathering, taking, inspection, investigation reenactment, examination and identification. Specific requirements with respect to each methods are also provided.

The regulations establish specific procedures and standards to examine and assess the authenticity, integrity, legality, and relevance of electronic evidence, set out the rules on flawed evidence and exclusionary rules on illegal electronic evidence. According to the rules, the following data shall not be admitted: (1) electronic data that is manipulated, forged or the authenticity of which can not be confirmed, (2) electronic data that has been added, deleted or modified and the authenticity of which may be compromised, (3) any other scenarios in which the authenticity of electronic data can not be guaranteed.

In practice, the following are the major difficulties in collecting and using electronic evidence: first of all, with the development of cloud computing technology, more and more electronic evidence is stored in cloud and is difficult to be searched and seized. The problem is even more acute if the size of data is too large to collect or analyze. Secondly, electronic evidence is inherently intangible and can be easily manipulated, updated, modified or deleted. It is a challenge to ensure its authenticity and integrity. Thirdly, the criminals often delete the original electronic record, resulting in incomplete chain of electronic evidence and weakened weight

of proof.

4. Recommendations

Law Enforcement and Investigation

States shall respect and safeguard human rights and comply with the relevant criminal procedural provisions of its domestic laws during law enforcement and investigation on cybercrime.

States shall strengthen investigation and law enforcement against acts of aiding and preparation of cybercrime, so as to effectively address the whole chain of cybercrime.

States should deliberate on the impact of cloud computing, dark web and other emerging technologies on law enforcement and investigation of cybercrime, and work together to find feasible solutions.

States are encouraged to establish in their domestic legislation Internet Service Providers' obligation to cooperate with the government on preventing cybercrime and to support the law enforcement and investigation, e.g., encouraging the Internet Service Providers to take technical and other necessary measures to prevent cybercrime, make emergency response plans for cybersecurity incidents, and deal with system bugs, computer viruses, network attack, network intrusion and other security risks in a timely manner.

Scope of Electronic Evidence

States shall enact or improve legislation to recognize the admissibility of electronic evidence, and provide for the definition and scope of electronic

evidence.

States may consider including the following data as electronic evidence in their domestic legislation: traffic data, such as log files; content data, such as emails; subscriber data, such as user registration information, and other data stored, processed and transmitted in digital format which is produced during the commission of crime and can be used to prove the facts of the crime.

Capacity for collecting electronic evidence

States are encouraged to strengthen capacity-building for electronic evidence collection, cultivate professional teams equipped with both legal and technical expertise, and enhance experience sharing and training cooperation in this regard. UNODC is encouraged to play a role in this field.

Method of collecting electronic evidence

States are encouraged to provide in their domestic laws relevant methods for collecting electronic evidence, such as seizing and preserving the original storage medium, on-site collecting, remote collecting and verification. Member States are encouraged to freeze electronic evidence to prevent addition, deletion and modification through measures such as computing the checksum of the electronic evidence, locking the accounts of web applications and adopting write protection.

States are encouraged to establish technical norms and standards for electronic evidence collection.

States should ensure that the collection of electronic evidence is in

compliance with due process.

Admissibility rule of electronic evidence

States should establish rules for assessing the authenticity, integrity, legality and relevance of electronic evidence in their domestic legislation, and take into account the unique characteristics of electronic evidence when applying the rules of original evidence, hearsay and illegal evidence exclusion.

Trans-border access to electronic evidence

When collecting electronic evidence abroad, states shall respect the sovereignty of states where data is located, comply with due process and respect the legitimate rights of relevant persons and entities, and shall refrain from unilaterally using intrusive or destructive technical investigation measures in this regard.

States are encouraged to conduct consultation with other states to further improve international judicial assistance and enforcement cooperation by optimizing relevant procedures or other methods, to facilitate the investigation of cybercrime and collection of electronic evidence.

States should consider adopting international model provisions on investigative power concerning collection of electronic evidence, and explore the possibility of negotiating a global binding instrument on combating cybercrime under the UN framework, which may include universally accepted provisions on trans-border electronic evidence collection.