New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime

PI Yong* (December 2011)

Cybercrime is a new type of crime occurring in this information age. In China, as the development of information technology, Cybercrime has been changing along with the time. Because China moved back to the normal route in 1980s, which made the application of Computer in China later than that of the west world, so did even much more late the application of Internet. Therefore computer crimes seldom occurred in China during the beginning period, most of the crimes violate the computer system without network or use them as its tools. In 1994, Internet entered into China, thereafter the number of Chinese Internet users is increasing everyday and now we have the largest internet users all over the world. In the newly blooming internet society, the computer crimes in China have two new characteristics: The first one is Internetization of crimes. There are more crimes using Internet, more interregional or transnational computer crimes appeared. The other one is that Cybercrimes in economic field happened much more frequently. Along with the development of China network economy, Cybercrimes in China rushed into the new field and has formed an industrial chain with different divisions. Many criminals use the network resources outside China to commit Cybercrime, according to statistics of Cybercrime by China Ministry of Public Security in 2010, over 90 percent of network sites, which were used to committing fraud, phishing, pornography crimes and Internet gambling, locate their server system outside China, and over 70 percent of Botnet control sides were set up in foreign countries.[1] In order to combat Cybercrime that has been changing, since 1994 China legislations were amended frequently.

A. China criminal legislations against Cybercrime

In 1994, the State Council issued the first law on computer crime, which is Ordinance on protecting the safety of computer system. In 1997, 2000, 2009 China Criminal Law was amended to increase new Cybercrimes,[2] in 2011 China Supreme People's Court and Supreme People's Procuratorate issued the judicial interpretation on Cybercrime. [3]

However China Criminal Procedure Law responses to Cybercrime slowly, now there is no rules on collecting electronic evidence or admissibility rules relating to electronic evidence, until 2011 Draft of amendments to China Criminal Procedure Law began to stipulate technical detection

* Professor of School of Law, Wuhan University, China.
[Shared with the Council of Europe for publication in December 2011. The views expressed are not necessarily those of the Council of Europe]

[1] See general statements of Chinese delegation in the first meeting of the Intergovernmental Group of Experts of United Nations Crime Prevention and Criminal Justice Program in January, 2011.

[2] In 1997 China Penal Code was amended to add Article 285, 286 and 287, which stipulated two CIA Cybercrimes (Illegal Access and Sabotaging computer system) and other tool-type Cybercrime, in which computer systems are used as the tools of crime. In 2000 Decision on Protecting Security of Network was passed by National Council to combat 21 tool-type Cybercrime. In March 2009 the 7th Amendment of China Penal Code became effective, which stipulate three new Cybercrime to combat new types of Cybercrime in the China networked economy.

[3] See Interpretation to the Judicial Problems on Dealing with Criminal Cases related to Endangering the Safety of Computer System, which became effective on 1th, September 2011 and interprets the application of China Penal Code to new Cybercrime in 7th Amendment of China Penal Code.

measures that include electronic surveillance. [4]But China judicial practice already goes ahead of criminal procedure law, China Supreme People's Court and Supreme People's Procuratorate issued several judicial interpretations on electronic evidence.[5]

In the field of international judicial cooperation, there is no agreement between China and foreign countries on cooperation on combating Cybercrime, China does not join any international convention or treaty on Cybercrime also.

More details are given as below:

I. Provisions on Cybercrime in China Criminal Law

In China Criminal Law, five Cybercrimes were prescribed, which are illegal accessing, illegal obtaining computer data, illegal controlling computer system, providing computer program or tools for illegal accessing or controlling computer system, and sabotaging computer system:

(1) According to the first paragraph of Article 285 of China Penal Code, Crime of illegal accessing is, illegal invading the computer system in the fields of State affairs, national defense construction or sophisticated science and technology;
(2) According to the second paragraph of Article 285, Crime of illegal obtaining computer data is illegal invading the computer system that is not belong to the computer system described above or using other technical method to obtain computer data in the computer system;
(3) According to the second paragraph of Article 285, Crime of illegal controlling is illegal controlling the computer system, which is described in the crime of illegal obtaining computer data;
(4) According to the third paragraph of Article 285, Crime of providing computer program or tools which is used to illegal access or control computer system is, providing computer program or tools which is especially produced for the aim to illegal invade or control computer system, and in the case of knowing the computer program and tools will be used for illegal invading or controlling computer system, deliberately providing them;
(5) According to the Article 286, Crime of sabotaging computer system is, sabotaging the functions of computer system or computer data in the computer system, which results in the failure of computer system.

In addition to the above provisions, there is a kind of Cybercrime in the field of China network economy, the criminals transfer, purchase or help to sell illegal acquired data or control of computer system, in order to seek illegal interests. In order to control the new kind of crimes, the aforementioned judicial interpretation prescribed that the criminals shall be convicted and punished according to provision in Article 312 of China Penal Code, which prescribes the crime of concealing illegally acquired goods. [6]If the ISP or advertising company willfully provide for

[4] See http://www.npc.gov.cn/npc/xinwen/lfgz/2011-08/30/content_1668503.htm, 2011 Draft Amendment of China Criminal Procedure Law and its interpretation.
[5] See Provisions on Problems related to Examine and Identify Evidence in the Death Penalty Cases and Provisions on the Judicial Problems related to Internet Gambling Cases, which were issued by China Supreme People's Court.
[6] See Article 7 of Interpretation to the Judicial Problems on Dealing with Criminal Cases related to Endangering

criminals of Cybercrimes the technical support or financial help, they shall be convicted and punished as the accomplice. [7]

I made a comparative research of criminal legislations between China and European community, the result is that: the aforementioned provisions reaches and goes beyond the standard set by Council of European Union Framework Decision on attacks against information systems, and reaches most of requirements of Council of Europe Convention on Cybercrime.

II. China criminal procedural law on Cybercrime

There is no independent criminal evidence law in China, collecting and adopting electronic evidence shall follow the common rules on evidence in China criminal procedure law and related judicial interpretations, now there are only few judicial interpretation that prescribe the rules on electronic evidence, for example, Provisions on Problems related to Examine and Identify Evidence in the Death Penalty Cases and Provisions on the Judicial Problems related to Internet Gambling Cases, which were issued by China Supreme People's Court. Since there are not sufficient rules on electronic evidence, the rules in other law field such as civil law, administrative law and the related judicial interpretations in fact play the role of instructing the police to collect electronic evidence and influencing the decision of Judge.

1. Rules on collecting electronic evidence

On the measure of retention of electronic data, China Internet regulations prescribe that ISP should record and save electronic data and provide them to the authorities if they are required. [8]The measure is not a criminal investigative measure, but it plays key role in the process of investigation to Cybercrime, without it the investigative authority cannot efficiently find Cybercrime and collect necessary evidence. So in the view of function of regulations, [9]these Internet administrative regulations do help to collect electronic evidence.

On the measure of copying and detaining electronic data, before 2010 China investigative authority treated electronic data as video and voice data, so that electronic data was detained according to the rules prescribed to video and voice data. Now new judicial interpretation in 2010 prescribed special measures to copy, collect and preserve electronic data.[10]

On the measure of real time collecting electronic data, there is no measure of real time collecting electronic data in China criminal procedure law, but electronic surveillance is used in the criminal investigation of serious crimes. The electronic data that is collected by using electronic

---

the Safety of Computer System.

[7] See Article 9 of Interpretation to the Judicial Problems on Dealing with Criminal Cases related to Endangering the Safety of Computer System.

[8] See Article 14of Management Measures on Internet Information Services, Article 19 of Implement Measures of Interim Provisions on International Networking of Computer Information Network, Article 14 of Management Measures on Internet Surfing Service Units and Article 14 of Management Measures on E-Bulletin Board Service, etc.

[9] Vgl. Ulrich Sieber, Strafrechtsvergleichung im Wandel, Strafrecht und Kriminologie unter einem Dach, Kollquium zum 90. Geburtstag von Professor Dr. Dr. h.c. mult. Hans-Heinrich Jescheck, S.78-130.

[10] See Article 5 of Provisions on the Judicial Problems related to Internet Gambling Cases.

surveillance cannot be used as evidence in the court, [11]because it is not the evidence prescribed in the criminal procedure law, so the electronic data can only be used to find other evidence such as oral statement. The draft of new amendment of China Criminal Procedure Law that will be passed in 2012 prescribed electronic evidence and technical investigative measures, which include the electronic surveillance. The draft prescribed its scope, implementation units, applicable object, period and its extension, security clause, aim and effect of the electronic data.[12] These provisions are similar to the related legislation of foreign countries and the Convention on Cybercrime.

On the measure of production order, Chinese legislations such as Criminal Procedure Law, [13]Nation Security Law[14] and People's Police Law[15] prescribe that the units and persons should truthfully provide evidence when the judge, prosecutor or police require the evidence. These provisions are similar to the related regulations in the Convention on Cybercrime. [16]

2. Rules of adopting electronic evidence

On the aspect of rules on adopting electronic evidence, now there are no rules on adopting electronic evidence, the judges adopt the electronic evidence according to the common rules on evidence, only few new judicial interpretation by China Supreme People's Court prescribed the principle and rules on the legality of the electronic evidence, these interpretation play an important role in the cases of Cybercrime. Neither is there rule of probative force of electronic evidence, judges make free decision on the probative force of electronic evidence according to all related evidences. However, the rules on probative force of electronic data in other law field affect the Chinese judges to make their decision. For example, electronic data is usually saved, transferred, processed electronic data through some electronic equipments, if these equipments conform to the national or industry standard, that will help judges believe the strong probative force of electronic evidence.

Generally speaking, on the aspect of criminal procedure law, China criminal procedural legislations on electronic evidence develop slowly. In the cases of Cybercrime, the special regulations in the China criminal procedural law, administrative law and judicial interpretation play the similar role as the related procedural provisions in the Convention on Cybercrime, and in majority part they are already in harmonization with Convention on Cybercrime. But on the aspect of the force, operability and balance between controlling crime and protecting civil right, China criminal legislation still should be improved.

III. Provisions on Jurisdiction and International Cooperation

There are no special provisions on jurisdiction of Cybercrime in China Penal Code, for which Article 6 to Article 12 of China Penal Code are applied. If the place of the act or the consequence

[11] See Article 3 of Interpretation on Judicial Problems of Criminal Investigation implemented by Criminal Investigative Units According to China Criminal Procedure Law.
[12] See Article 5,56 of 2011 Draft Amendment of China Criminal Procedure Law and its interpretation.
[13] See Article 45 of China Criminal Procedure Law.
[14] See Article 18 of Nation Security Law.
[15] See Article 34 of People's Police Law.
[16] See Convention on Cybercrime of Council of Europe of 23.11.2001 (ETS No. 185), Article 18.

of Cybercrime is in China, China Penal Code should be applied. If Chinese outside of China commits Cybercrime and the highest penalty of the crime is less than 3 years, China Penal Code may not be applied. China legislation is in harmonization with the Article 22 of Convention on Cybercrime and Article 10 of Council of European Union Framework Decision mentioned above, which make sure that Cybercrime in China can be ruled absolutely. Now there is not agreement between China and foreign countries or international treaty that prescribed the handling mechanism on the Cybercrime cases in which more than one country have the jurisdictions.

On the aspect of judicial cooperation on Cybercrime, there is not special judicial cooperative mechanism between China and foreign countries or international organization. But in the special transnational Cybercrime cases, China criminal investigative authorities have cooperated with foreign criminal authorities in the field of criminal investigation and help, from 2004 to 2010 China criminal investigative authority help more 40 countries investigative authorities in more than 700 Cybercrime cases. [17]

B. Challenge of Harmonization of Criminal legislation against Cybercrime and the Role of China

In the era of Internet, Cybercrime becomes the common threat of the world, because the technical base such as computer and Internet technique on which Cybercrime relied on is same for all the countries, so Cybercrimes in all countries have the same characteristics and trends. The common challenge makes the harmonization of the relevant criminal legislation of all countries necessary. Due to the work of CoE, CoEU and UN, some country's criminal legislation on Cybercrime began to harmonize, now legislation standard set by Framework Decision mentioned above becomes the basic standard which many country's legislations have already reached, Convention on Cybercrime represents the higher legislation standard, so the countries who reached the later standard are less. On the aspect of harmonization of criminal procedure law, even the countries who already ratified the convention, for example Germany, don't totally fulfill the obligation of transplanting the provisions in the convention to domestic law yet, it is almost sure that it will be much later for the ratified countries to build a transnational judicial cooperation programs that are strictly conformed to Convention on Cybercrime. Even in the scope of European community the progress of harmonization of criminal legislation against Cybercrime cannot be quick.

Convention on Cybercrime is an open international treaty, countries outside of Europe such as USA, Japan, Canada and South Africa also become its parties, so in the past, the present and the future CoE was, is and will still be the mover and one of the important leader in the progress of harmonization of criminal legislations of countries against Cybercrime. But CoE is a regional international organization and has limited effect on the countries outside of European, in addition, Convention on Cybercrime is only a response to Cybercrimes in the countries who participated in the drafting of the convention, and conditions and programs are hard to achieve after the convention became effective, therefore now the convention is effective to some European

[17] See general statements of Chinese delegation in the first meeting of the Intergovernmental Group of Experts of United Nations Crime Prevention and Criminal Justice Program in January, 2011.

countries and USA,[18] who is a ally of European countries. Those countries, which are outside of Europe and have not the relationship of ally with European countries, for example China and Russia etc., are not the parties of the convention. It means that COE can not solely lead the progress of harmonization of criminal legislations against Cybercrime, need work together with worldwide international organization such as UN, to push the far-reaching project of harmonization of criminal legislation and judicial cooperation system against Cybercrime.

China is in the common Internet world and faces the same challenge from Cybercrime, China has been amending the criminal legislation on Cybercrime with the change of China Internet society and Cybercrime. Now China Penal law on Cybercrime reaches and goes beyond the standard set by CoEU Framework Decision, and in most area reaches the requirement of standard set by Convention on Cybercrime. On the aspect of criminal procedure law, in recent years China has been pushing progress of legislation on collecting and adopting electronic evidence, now besides the measure of expedited preservation of stored electronic data, the legislation of other measure on collecting electronic evidence will soon reach the requirement of Convention on Cybercrime. On the aspect of jurisdiction and international cooperation, China did not reach any agreement with foreign countries on judicial cooperation of combating Cybercrime and did not join the related international treaty, that make China criminal judicial authorities face difficulties when they handle with transnational Cybercrime cases. China stands outside of the international judicial cooperation system on combating Cybercrime, it leads to a lot of transnational Cybercrimes move from other countries into China. The situation will not only do harm to safety of China network society but also make China the springboard to attack computer systems of foreign countries, because the key technique of Internet security is not in the hand of China, and it is forbidden to export to China by U.S and European countries, so China Internet system in fact is vulnerable and weak.

Cybercrime is the common challenge of world, it cannot be efficiently controlled unless the worldwide international judicial cooperation is built up, in which China, such a great Internet country, cannot be absent. China and International organizations especially UN and COE should communicate and cooperate more closely in the field of judicial cooperation against Cybercrime. Cybercrime is the challenge of the whole world, one of choices can be a more extensive new international treaty against Cybercrime, which is more than the scope of European countries and in the scope of United Nations, and based on the research of worldwide Cybercrime, especially reflects the status of Cybercrime of main Internet countries such as USA, European countries, China and Russia.

December 2011

[18] See PI Yong, Comparative Research on Measures of Collecting Evidence in the Convention on Cybercrime and China Criminal Procedure Law, China Legal Science, 2003. vol. 4.