



# **New China Criminal Legislation against Cybercrime in the Common Internet**

**By Prof. Dr. PI Yong  
Wuhan University of China**



# Abstract

## **A. Cybercrime in China**

## **B. China criminal legislations against Cybercrime**

I. Provisions on Cybercrime in China criminal Law

II. China criminal procedure law on Cybercrime

III. Provisions on Jurisdiction and International Cooperation

## **C. Conclusion**

# A. Cybercrime in China

---

- In China, as the development of information technology, Cybercrime has been changing along with the time.
  - China moved back to the normal route in 1980s, which made the application of Computer in China later than that in the west world, so did even much more late the application of Internet.
  - Before 1994, most of the crimes violate the computer system without network or use them as its tools.
  - In 1994, Internet entered into China. Computer crimes in China begin to have two new characteristics:
    - Internetization of crimes
    - Cybercrimes in economic field happened much more frequently.

# A. Cybercrime in China

---

- Cybercrimes in China rushed into Internet economy field and has formed an industrial chain with different divisions.
- Many criminals use the network resources outside China to commit Cybercrime:
  - over 90 % network sites, which were used to committing fraud, phishing, pornography crimes and Internet gambling, locate their server system outside China.
  - over 70 % Botnet control sides were set up in foreign countries.

Resource: Statistics of Cybercrime by China Ministry of Public Security in 2010

## **B. China criminal legislations on Cybercrime**

---

- As Cybercrime in China has been changing, China legislations on Cybercrime were amended frequently:
  - In 1994, first law on computer crime: Ordinance on protecting the safety of computer system.
  - In 1997, 2000, 2009 China Criminal Law was amended to increase new Cybercrimes
  - In 2011 China Supreme People's Court and Supreme People's Procuratorate issued the judicial interpretation on Cybercrime.
- China Criminal Procedure Law responses to Cybercrime slowly.
  - There is no rules on collecting electronic evidence or admissibility rules relating to electronic evidence.
  - China judicial practice goes ahead of criminal procedure law.
- Neither China make agreement on cooperation of combating Cybercrime with foreign countries, nor join any international convention.

# **B. China criminal legislations on Cybercrime**

---

## **I. Provisions on Cybercrime in China Criminal Law**

Five Cybercrimes were prescribed :

- **illegal access:**
  - **illegal invading the computer system in the fields of State affairs, national defense construction or sophisticated science and technology.**
- **illegal obtain computer data:**
  - **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.**
- **illegal controll computer system:**
  - **illegal controlling the computer system.**
- **provide computer program or tools for illegal accessing or controlling computer system:**
- **destruct computer system:**
  - **destructing the functions of computer system or computer data in the computer system, which results in the failure of computer system.**

## **B. China criminal legislations on Cybercrime**

---

- 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.
  - 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.
- If the ISP or advertising company willfully provide for criminals of Cybercrimes the technical support or financial help, they shall be convicted and punished as the accomplice.

## **B. China criminal legislations on Cybercrime**

---

- Result of comparative research between China and European Union:
  - The aforementioned provisions reaches and goes beyond the standard set by Council of European Union Framework Decision on attacks against information systems,
  - They reach most of requirements of Council of Europe Convention on Cybercrime.



## **B. China criminal legislations on Cybercrime**

---

### **II. China criminal procedure law on Cybercrime**

- There is no independent criminal evidence law in China.
- Only few judicial interpretation prescribe the rules on electronic evidence. for example,
  - **Provisions on the problems related to examine and identify evidence in the death penalty cases**
  - **Provisions on the judicial problems related to Internet gambling cases**
- The rules in other law field such as civil law, administrative law and judicial interpretations in fact play the role of instructing the police to collect electronic evidence and influencing the decision of Judge.

## **B. China criminal legislations on Cybercrime**

---

### **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.
  - **It is not a criminal investigative measure, but it plays key role in the process of investigation to Cybercrime**
- On the measure of copying and detaining electronic data, now new judicial interpretation in 2010 prescribed special measures to copy, collect and preserve electronic data.
  - **Before 2010 electronic data was treated as video and voice data and was detained according to the rules prescribed to video and voice data.**

## **B. China criminal legislations on Cybercrime**

---

- On the measure of real time collecting electronic data, the draft of new amendment of China Criminal Procedure Law, which will be passed in 2012, prescribed electronic evidence and technical investigative measures, which include the electronic surveillance.
  - **Now 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 surveillance cannot be used as evidence in the court, because it is not the evidence prescribed in the criminal procedure law, so they can only be used to find other evidence such as oral statement.**
  - **The provisions of the Draft are similar to the related legislation of foreign countries and the Convention on Cybercrime.**

## **B. China criminal legislations on Cybercrime**

---

On the measure of production order, Chinese legislations prescribe that the units and persons should truthfully provide evidence.

- **These provisions are similar to the related regulations in the Convention on Cybercrime.**

### **2. Rules on adopting electronic evidence**

- **Now there are no rules on adopting electronic evidence.**
  - **Chinese judges adopt the electronic evidence according to the common rules on evidence.**
  - **Only few new judicial interpretation prescribed the principle and rules on the legality of the electronic evidence.**
- **Neither is there rule of probative force of electronic evidence, judges make free decision on the probative force of electronic evidence**
  - **Rules on probative force of electronic data in other law field affect the chinese judges to make their decision.**

# B. China criminal legislations on Cybercrime

---

## Summary

- China criminal procedural legislation 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 harmony with them.
- On the aspect of the force, operability and balance between controlling crime and protecting civil right, China criminal legislation still should be improved.

## **B. China criminal legislations on Cybercrime**

---

### **III. Provisions on Jurisdiction and International Cooperation**

- There are no special provisions on jurisdiction of Cybercrime in China Penal Code, for Cybercrime Article 6 to Article 12 of China Penal Code are applied.
    - **If the place of the act or the consequence 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 harmony with the Article 22 of Convention on Cybercrime and Article 10 of Framework Decision mentioned above, which make sure that Cybercrime in China can be ruled absolutely.**
- .

## **B. China criminal legislations on Cybercrime**

---

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

# C. Conclusion

---

## I

- Cybercrime becomes the common threat of the world, that makes the harmonization of legislation of all countries necessary.
- The 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.
- The progress of harmonization of criminal legislation against Cybercrime cannot be quick.



## C. Conclusion

---

- CoE is a regional international organization and has limited effect on the countries outside of European.
- Convention on Cybercrime is only a response to Cybercrimes in the countries who participated in the drafting of the convention. Conditions and programs are hard to achieve after the convention became effective
- 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.
- 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.

# C. Conclusion

---

## II

- China is in the common Internet world and faces the same challenge from 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, 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.

## C. Conclusion

---

- On the aspect of jurisdiction and international cooperation, China did not reach agreement with foreign countries and did not join the relevant international treaty.
  - That make China criminal judicial authorities face difficulties when they handle with transnational Cybercrime cases.
  - China left outside of the international judicial cooperation system on combating Cybercrime, 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.

# C. Conclusion

---

## III

- Cybercrime is the common challenge of world, it cannot be efficiently controlled unless the extensive international judicial cooperation is set up.
- China, such a great network country, cannot be absent.
- China and International organizations especially UN and COE should communicate and cooperate more closely on combating Cybercrime.
- One of the choices is building a more extensive new international treaty on combating Cybercrime which is beyond the scope of European countries and in the scope of United Nations.

武汉大学

Wuhan University



**Thanks!**