Preparatory Colloquium
Helsinki (Finland), 10-12 June 2013.
Section IV : International Criminal Law

NATIONAL REPORT ON CYBER CRIME IN CHINA FOR PREPARATORY COLLOQUIUM SECTION IV AT HELSINKI UNIVERSITY*

GUO JING*

Jurisdictional issues

(1)(a) How does your country locate the place of the commission of a crime in cyberspace?

According to Criminal Law

Article 6.

This law is applicable to all who commit crimes within the territory of the PRC except as specially stipulated by law.

This law is also applicable to all who commit crimes aboard a ship or aircraft of the PRC.

When either the act or consequence of a crime takes place within PRC territory, a crime is deemed to have been committed within PRC territory.

According to "Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling",

Section IV. Jurisdiction over the criminal cases of internet gambling

The "place of a crime" shall include the place where the server of the gambling website is located, the place of network access, the place where the establisher or manager of the gambling website is located, the place where the agent of the gambling website and the gamblers commit internet gambling, etc.

In other words, the place of commission includes where the server of the website in question is located, the place of network access, the place where the establisher or manager of the website in question is located, the place where the agent of the website in question and the user commit illegal internet act, etc.

(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

According to "Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling",

Section IV. Jurisdiction over the criminal cases of internet gambling

For the territorial jurisdiction over criminal cases of internet gambling, the principle of taking the place of a crime as the first choice and the place of abode of the defendant as the second choice shall be adhered to.

Where the public security organs have disputes about the jurisdiction over a criminal case of internet gambling which involves two or more regions, they shall, on the basis of the principle of being conducive to ascertaining criminal facts and conducive to

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Guo Jing is a lecturer at the College for Criminal Law Science at the Beijing Normal University. She received her Ph.D. at the Faculty of Law of the University of Macau.

legal proceeding, resolve the disputes through serious negotiation. If they can not reach an agreement after negotiation, they shall report the case to their common public security organ at the higher level for designated jurisdiction. Where the investigation of a major internet gambling case which involves two or more provinces (autonomous regions, or municipalities directly under the Central Government) is about to conclude, the Ministry of Public Security may, when necessary, designate the jurisdiction over the case after consulting with the Supreme People's Court and the Supreme People's Procuratorate.

Examining current cases in practice, most of them were investigated and the trial was conducted in the place where the natural victim or the victim company was physically present.

(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?

There is no specific legal document that clearly stipulates this issue. However, the general principles of jurisdiction also apply to cyber crime. In other words, there is no particular rule for cyber crime. Cyber crime can only do with a determination of the locus delicti.

(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?

The general principles of jurisdiction also apply to cyber crime. In other words, there is no particular rule for cyber crime.

According to article 6-9 of Criminal Law,

Article 6. *This law is applicable to all who commit crimes within the territory of the PRC except as specially stipulated by law.*

This law is also applicable to all who commit crimes aboard a ship or aircraft of the PRC.

When either the act or consequence of a crime takes place within PRC territory, a crime is deemed to have been committed within PRC territory.

Article 7. *This law is applicable to PRC citizens who commit the crimes specified in this law outside the territory of the PRC; but those who commit the crimes, provided that this law stipulates a minimum sentence of less than a three-year fixed-term imprisonment for such crimes, may not be dealt with.*

This law is applicable to PRC state personnel and military personnel who commit the crimes specified in this law outside PRC territory.

Article 8. *This law may be applicable to foreigners who, outside PRC territory, commit crimes against the PRC state or against its citizens, provided that this law stipulates a minimum sentence of not less than a three-year fixed term of imprisonment for such crimes; but an exception is to be made if a crime is not punishable according to the law of the place where it was committed.*

Article 9. *This law is applicable to the crimes specified in international treaties to which the PRC is a signatory state or with which it is a member and the PRC exercises criminal jurisdiction over such crimes within its treaty obligations.*

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

There is national law, to be more specific a judicial interpretation, "Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling", settling the domestic disputes about jurisdiction

Section IV. Jurisdiction over the criminal cases of internet gambling

Where the public security organs have disputes about the jurisdiction over a criminal case of internet gambling which involves two or more regions, they shall, on the basis of the principle of being conducive to ascertaining criminal facts and conducive to legal proceeding, resolve the disputes through serious negotiation. If they can not reach an agreement after negotiation, they shall report the case to their common public security organ at the higher level for designated jurisdiction. Where the investigation of a major internet gambling case which involves two or more provinces (autonomous regions, or municipalities directly under the Central Government) is about to conclude, the Ministry of Public Security may, when necessary, designate the jurisdiction over the case after consulting with the Supreme People's Court and the Supreme People's Procuratorate.

There is no national law dealing with cyber crime jurisdiction dispute with foreign countries.

(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

Cyber crime should follow the jurisdictional principles in Chinese criminal law, which are written in article 6-9 in particular. Hence, no exceptional jurisdictional rules apply to cyber crime.

(C) Substantive criminal law and sanctions

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?

It is controversial to say which cyber crime is transnational. Some believe all cyber crimes are transnational in nature. Some believe the crimes against internet information are transnational due to the fact that the internet does not have any boundaries. In comparison, traditional crimes with cyber as a tool are not transnational in nature.

To what extent do definitions of cyber crime offences contain jurisdictional elements?

As we can see from articles 285-287 of criminal law, the definitions do not contain jurisdictional elements.

To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

General part rules on commission, conspiracy or any other form of participation do not contain jurisdictional elements. However, due to the specialty of cyber crime, some participation acts, for instance providing programs or tools for others to commit illegal intrusion or controlling computer information system, constitute an independent crime.

There are additional requirements for participation acts to constitute cyber crime. For instance, according to "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems",

Article 9 *Whoever, knowing that any other person is committing an act as mentioned in Articles 285 and 286 of the Criminal Law, falls under any of the following circumstances shall be deemed an accomplice in a crime, and be punished in accordance with the provisions of Article 285 or 286 of the Criminal Law:*

(1) Providing any other person with any program or tool used for sabotaging the functions of, data in or application programs of a computer information system and obtaining illegal income of 5,000 yuan or more, or providing the program or tool to 10 or more other persons;

(2) Providing any other person with assistance in a field such as internet access, server hosting, network storage space, communication transmission passage, settlement of expenses, transaction services, advertising service, technical training or technical support, and obtaining illegal income of 5,000 yuan or more; or

(3) Providing any other person with funds of 5,000 yuan or more through promotion of software, publication of advertisement, etc.

Whoever commits an act as mentioned in the preceding paragraph with the quantity or amount reaching 5 times the standard as prescribed in the preceding paragraph shall be deemed to have fallen under the "especially serious circumstances" or have caused the "particularly serious consequences" as mentioned in Article 285 or 286 of the Criminal Law.

Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

The answer to this question should be really careful. Due to the non-boundary nature of cyber crime and the application of double criminality, it is very difficult to regulate cyber crime on its own. However, traditional crimes committed through cyber are more suitable for states to regulate on their own.

Does your national criminal provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?

According to China criminal law,

Article 30. *A company, enterprise, institution, organization, or group which commits an act endangering society that is considered a crime under the law shall bear criminal responsibility.*

Companies, enterprises, institutions, organizations or groups take responsibility only when the law clearly says the crime can be committed by a corporation. However, the four kinds of cyber crime do not fall within this group, and therefore, there is no corporation liability for cyber crime in China.

Nevertheless, according to "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems",

Article 8 *Where a crime of endangering the security of a computer information system is committed in the name of or in the form of an entity, and the standards for conviction and sentencing as prescribed in this Interpretation are met, the directly liable person in charge and other directly liable persons shall be subject to criminal liability in accordance with Articles 285 and 286 of the*

Criminal Law.

(D) Cooperation in criminal matters

As is the case with jurisdictional issues, there are no special rules for cooperation in criminal matters regarding cyber crime. The existing mutual legal assistance instruments between China and other sovereign states also apply to cyber crime. Besides, the cooperation regime that is offered by International conventions such as the UN Convention on Transnational Organized Crime can also be utilized for combating cyber crime, if the cyber crime can be identified as a transnational crime.

Detailed answers to questions in this part are being prepared by other specialists in preparation for the Section 3 Preparatory Colloquium, planned to be held in Turkey.

(E) Human rights concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology? Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted? How is the responsibility or accountability of your state involved in international cooperation regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

The two SCNPC decisions require the protection of the privacy rights of the individual online. The human rights provisions on the international level, and of the states where actual harm is caused, as well as of the states where the conduct occurs, all need to be taken into consideration. Whatsoever, these are interesting questions that involve human right standards, state sovereignty, state immunity, and so on.

(F) Future developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why? Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice? Is there any other issue related to Information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

We believe that the development of information society would bring an innovation to rules on mutual assistance. New techniques and skills which may facilitate court hearings and the presentation of evidence will be used in legal proceedings in the near future. Right now, there is no practice of this kind; however, the future is very promising.

A. Report References

Legislations, Enforcement and Judicial Documents

1. Decision of the Standing Committee of the National People's Congress

"Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security", issued by the Standing Committee of the National People's Congress, on 28th December 2000.[1]

"Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks", issued by the Standing Committee of the National People's Congress, on 28th December 2012.[2]

[1] On 28 December 2000, the Standing Committee of the National People's Congress issued the "Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security"(hereinafter "2000 Decision"), which was amended on 27 August 2009. The 2000 Decision is the first comprehensive legal document regarding internet security in China. It contains seven clauses, which stipulate what acts may constitute crime or illegal acts breaching public security administration regulations. Prohibited acts include five major categories: (a) crimes disrupting the safe operation of computer networks; (b) crimes of using the internet to fabricate and disseminate information harmful to national security and social stability; (c) crimes of using the internet to disrupt the socialist market economic order and the management of social order; (d) crimes of using the internet to violate personal, property, and other legal rights of individuals, legal entities, and other organizations; (e) illegal acts, using the internet , that are not serious enough to warrant criminal punishment, but could be alternatively punished under the 1986 Provisions on Administrative Punishment concerning the Management of Public Security. Specific crimes include hacking, damaging a computer system, use internet disseminating spy, espionage, pornographic information, infringing intellectual property, online slander and so on.

[2] On 28 December 2012, the Standing Committee of the National People's Congress issued the "Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks" (Hereinafter "2012 Decision"). The SIPN decision has 12 clauses, which clearly provides that the state protects electronic information by which individual citizens can be identified and which involves the individual privacy of citizens. All organizations and individuals may not obtain electronic personal information of citizens by theft or any

2. Criminal Law

Article 285 (The crime of illegally intruding into computer information systems) Whoever violates state regulations and intrudes into computer systems that contain information with respect to state affairs, construction of defense facilities, and sophisticated science and technology, is be sentenced to not more than three years of fixed-term imprisonment or criminal detention.

(The crime of illegally obtaining computer information system data, illegal control computer information system) Whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to fixed-term imprisonment not less than three years but not more than seven years, and be fined.[3]

(The crime of providing program and tool intruding or illegal control computer information system) Whoever provides special programs or tools specially used for intruding into or illegally controlling computer information systems, or whoever knows that any other person is committing the criminal act of intruding into or illegally controlling a computer information system and still provides programs or tools for such a person shall, if the circumstances are serious, be punished under the preceding paragraph.[4]

Article 286 (The crime of sabotaging computer information systems) Whoever violates state regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems, and causes grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.

Whoever violates state regulations and deletes, alters, or adds data or application programs installed in or processed and transmitted by the computer systems, and thus causes grave consequences, is to be punished according to the preceding paragraph.

Whoever deliberately creates and propagates a computer virus or other programs that sabotage the normal operation of the computer system, and cause grave consequences, is to be punished according to the first paragraph.

Article 287 (Crimes using internet as a tool) Whomever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing of state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

3. Judicial Interpretations

"Interpretation (II) of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations", issued by the Supreme People's Court and the Supreme People's Procuratorate, on 2 October 2010.

"Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations", issued by the Supreme People's Court and the Supreme People's Procuratorate, on 3 September 2004.

"Interpretation from the Supreme People's Court and Supreme People's Procuratorate on the Application of Law in Criminal Cases Concerning Gambling", issued by the Supreme People's Court and the Supreme People's Procuratorate, 2005.

Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling, 2010.

---

other illegal means and may not sell or illegally provide others with electronic personal information of citizens. It uses five clauses to regulate the behaviour of network service providers, who should share a main responsibility to obtain, rightfully use and protect users' information from theft or illegal acquisition by criminals. Citizens who discover any network information infringing their lawful rights may ask the network service provider to stop the infringement, report to relevant organs or may file lawsuits in accordance with law. Public security organs may give public security administration punishment, such as warning, fine, confiscation of illegal income, licence forfeiture or cancellation of registration, closure of website or prohibition of relevant liable persons from engaging in network service, may be imposed on responsible enterprises and institutions.

[3] Added by the 7th Amendment to 97 Criminal Law.

[4] Added by the 7th Amendment to 97 Criminal Law.

"Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems", issued by the Supreme People's Court and the Supreme People's Procuratorate, on 1 August 2011.

4. Administrative Regulations of the State Council

Ordinance for Security Protection of Computer Information System, issued by the State Council, on 18 February 1994.

"Interim Regulations of the People's Republic of China on the Management of International networking of Computer Information (97 Amendment)", issued by State Council, on 20 May 1997.

Regulation on Internet Information Service, issued by State Council, on 25 September 2000.

"Regulations on Administration of Business Premises for Internet Access Services", issued by State Council, on 29 September 2002.

5. Rules and Regulations of Ministries and Commissions

"Administrative Measures on the Testing and Selling License of Special Products for Computer Information System Security", issued by Ministry of Public Security, 12 December 1997.

"Computer Information System International Access Security Safeguard Administration Provisions", issued by Ministry of Public Security, 30 December, 1997.

"Interim Provisions on the Administration of Maintenance Secrets of Computer Information System", issued by State Secrets Bureau, on 26 February 1998,

"Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions", issued by State Secrets Bureau, on 1 January 2000.

"Rules of Computer Virus Protection and Disinfections Management", issued by Ministry of Public Security, on 20 March 2000.

"Evaluation criteria for anti-virus products of computer system", issued by Ministry of Public Security, on 20 March 2000.

"Administration of Engagement by Internet Sites in the Business of News Publication Tentative Provisions", issued by Ministry of Information Industry, on 8 November 2000.

"Interim Provisions on the Administration of the Internet Publications", issued by the General Administration of Press and Publication and Ministry of Information Industry, on 27 June 2002.

"Measures of the Protection of Railway Computer Information System", issued by the Ministry of Railway, on 15 July 2013.

"Measures for the Administration of IP Address Archiving", issued by Ministry of Information Industry, 8 February, 2005.

"Measures for the Administrative Protection of Internet Copyright", issued by Ministry of Information Industry, on 29 April 2005.

"Provisions for the Administration of Internet News Information Services", issued by Ministry of Information Industry, 25 September 2005.

"Provisions on the Technical Measures for the Protection of the Security of the Internet", issued by Ministry of Public Security, 13 December 2005.

"Measures for the Administration of Internet E-mail Services", issued by Ministry of Information Industry, 20 February 2006.

"Notice of the General Administration of Press and Publication, Ministry of Public Security, State Administration for Industry and Commerce, Ministry of Information Industry on Regularizing use Internet in Press Business", issued by General Administration of Press and Publication, Ministry of Public Security, State Administration for Industry and Commerce, Ministry of Information Industry, on 1 August 2007.

"Notice of State Administration of Radio Film and Television on Strengthening Content Administration of Internet Audio Video Program", issued by State Administration of Radio Film and Television, on 31 March 2009.

"Notice of the Ministry of Information Industry on Issuing 'Measures of implementation the Internet Network Security Information Report Mechanism'", issued by Ministry of Information Industry, on 13 April 2009.

"Notice of the Ministry of Industry and Information Technology on the Pre-installation of Green Network Filtering Software", issued by the Ministry of Industry and Information Technology, on 19 May 2009.

"Notice of the State Tobacco Monopoly Bureau, Ministry of Industry and Information Technology, Ministry of Public Security, State Administration for Industry and Commerce on crack down on the illegal use of the Internet and other information networks operating tobacco monopoly commodities", issued by the State Tobacco Monopoly Bureau, Ministry of Information Industry, Ministry of Public Security, State Administration for Industry and Commerce, on 24 June 2009.

"Notice of the Ministry of Public Security, Ministry of Industry and Information Technology and State Administration for Industry and Commerce on strengthening administration of sale information of Precursors and Chemicals used in Production of Narcotic Drugs and Psychotropic Substances", issued by Ministry of Public Security, Ministry of Information Industry and State Administration for Industry and Commerce, on 21 September 2010.

"Notice of the Ministry of Finance on Issuing Interim Measures for the Administration of Sales of Lottery via Internet", issued by the Ministry of Finance, on 26 September 2010.

"Interim Provisions on the Administration of Internet Culture", issued by the Ministry of Culture, on 17 February 2011.

"Notice of the State Food and Drug Administration, Ministry of Industry and Information Technology, Ministry of Public Security, State Administration for Industry and Commerce on further Crack Down on the Use of Internet Publishing Fake Drugs Information and Illegal sale Drugs", issued by State the Food and Drug Administration, Ministry of Information Industry, Ministry of Public Security, State Administration for Industry and Commerce, on 18 May 2011.

"Mobile Internet Malicious Program Monitoring and Response Mechanisms", issued by the Ministry of Information Industry, on 9 December 2011.

Several Provisions on Regulating the Market Order of Internet Information Services, issued by the Ministry of Information Industry, on 29 December 2011.

6. Local Legislations

"Computer Information System Security Administration Ordinance in Liaoning Province", issued by the Liaoning Provincial People's Congress and the Standing Committee of Liaoning Provincial People's Congress, on 30 June 2004.

"Computer Information System Security Protection Ordinance in Chongqing", issued by the Chongqing Municipal People's Congress and the Standing Committee of Chongqing Municipal People's Congress, on 29 September 2006.

"Computer Information System Security Protection Ordinance in Guangdong Province", issued by the Guangdong Provincial People's Congress and the Standing Committee of Guangdong Provincial People's Congress, on 20 December 2007.

"Computer Information System Security Protection Ordinance in Shanxi Province", issued by the Shanxi Provincial People's Congress and the Standing Committee of Shanxi Provincial People's Congress, on 20 December 2007.

"Computer Information System Security Protection Ordinance in Xuzhou City", issued by the Xuzhou People's Congress, on 22 January 2009.

"Computer Information System Security Protection Ordinance in Hangzhou City", issued by the Hangzhou People's Congress, on 1 April 2009.

"Computer Information System Security Protection Ordinance in Ningxia Hui Autonomous Region", issued by the Ningxia Hui Autonomous Region People's Congress and the Standing Committee of Ningxia Hui Autonomous Region People's Congress, on 31 July 2009.

7. Provincial and Municipal Government Regulation

"Interim Administrative Provisions on Computer Information System Security in Hohhot City", issued by the Hohhot Municipal Government, on 23 July 1993.

"Administrative Provisions on Control and Prevention of Computer Virus in Chongqing", issued by the Chongqing Municipal Government, 5 September 1994.

"Administrative Measures on Computer Information System Security Protection in Sichuan Province", issued by the Sichuan Provincial Government, on 28 March 1996.

"Measures on Computer Information System Security Protection in Chengdu", issued by the Chengdu Municipal Government, on 25 December 1996.

"Measures on Control and Prevention of Computer Virus in Tianjin", issued by the Tianjin Municipal Government, on 25 November 1997.

"Interim Provisions on Control and Prevention of Computer Virus in Hebei Province", issued by Hebei Provincial Government, 1 January 1998.

"Administrative Measures on Computer Information System Security in Fujian Province", issued by Fujian Provincial Government, on 30 May 1998.

"Measures on Computer Information System Security Protection in Anhui Province", issued by Anhui Provincial Government, on

22 December 1998.

"Interim Measures on Computer Information System Protection in Henan Province", issued by Henan Provincial Government, on 22 November 1999.

"Interim Measures on Computer Information System Protection in Xiamen City", issued by Xiamen Municipal Government, on 21 May 1999.

"Administrative Measures on Computer Information System Security Protection in Jiangsu Province", issued by Jiangsu Provincial Government, on 14 June 2002.

"Measures on Control and Prevention of Computer Virus in Tianjin", issued by Tianjin Municipal Government, 18 January 2002.

"Regulations of Tianjin Municipality on Protecting the Safety of Public Computer Information Networks", issued by Tianjin Municipal Government, on 25 January 2002.

"Regulations of Shenzhen Economic Special Zone on the Administration of Public Safety of Computer Information System", issued by Shenzhen Municipal Government, on 26 August 2004.

"Measures on Computer Information System Security Protection in Jiangxi Province", issued by Jiangxi Provincial Government, on 23 September 2004.

"Administrative Provisions on Computer Information System Security Protection in Heilongjiang Province", issued by the Heilongjiang Provincial Government, on 20 October 2006.

"Administrative Measures on Computer Information System Security Protection in Guiyang City", issued by the Guiyang Municipal Government, on 25 May 2012.

"Measures on Computer Information System Security Protection in Inner Mongolia Autonomous Region", issued by the Inner Mongolia Autonomous Region Government, on 6 December 2011.

8. Industry Self-regulation

"Public Pledge on Self-Discipline for the China Internet Industry", issued by Internet Society of China, on 3 December 2001, Beijing.

"Self-Disciplinary Norms on Prohibition of Disseminating Pornographic and Other Undesirable Information", issued by the Internet Society of China on 10 June 2004.

"Self-Disciplinary Convention of Internet Terminal Software Service Industry", issued by Internet Society of China, on 1 August 2011.

"Opinions of the China Law Society on Further Strengthening and Improving the Computer Information Network", issued by China Law Society, 5t December 2011.

Cases

Guangzhou People's Procuratorate of Guangdong Province VS. Lv Xuewen for sabotaging computer information systems in Guangzhou Intermediate People's Court on 19 August 1999.

Hebei Province Zhang Jiakou City Xuanhua District People's Procuratorate VS. Liu Jian for online fraud in Hebei Province Zhang Jiakou City Xuanhua District People's Court, on 12 February 2001.

Kunming City Wuhua District People's Procuratorate VS. Lin X for sabotaging computer information system, in Kunming City Intermediate People's Court, on 4 December 2001.

Wuxi City Binhu District People's Procuratorate VS. Ni X for sabotaging computer information system, in Wuxi City Intermediate People's Court, on 25 December 2001.

Suzhou City Canglang District People's Procuratorate VS. Luo X for sabotaging computer information system, in Suzhou City Canglang District People's Court, on 28 October 2002.

Quanzhou City Fengze District People's Procuratorate VS. Chen X Zhang Jianfeng for sabotaging computer information system, in Quanzhou City Fengze District People's Court, on 17 September 2003.

Shanghai X District People's Procuratorate VS. X Internet Company for disseminating pornographic material for profit, in Shanghai X Intermediate People's Court, in 2004.

Shanghai Pudong New Area People's Procuratorate VS. Shanghai Seven Continent Information Ltd. Company for disseminating pornographic materials for profit, in Shanghai No.1 Intermediate People's Court, on 3 Feburary 2005.

Tangshan City Lubei District People's Procuratorate VS. Xu X for sabotaging computer information system, in Tangshan City

Lubei District People's Court on 18 August 2005.

Shanghai Huangpu District People's Procuratorate VS. Mengdong and He Likang for online stealing in Shanghai Huangpu District People's Court, on 26 June 2006.

State VS. Chen XX for Illegal logging in on the online game "Dream Westward Journey aka *menghuanxiyou*" users' account, stealing users account and password, illegal obtaining 310,000 RMB, in 2007.

Xiantao City People's Procuratorate of Hubei Province VS. Li X for sabotaging computer information systems, in Xiantao City Intermediate People's Court of Hubei Province, on 26 September 2007.

Guangzhou Yuexiu District People's Procuratorate VS. A Unit for sabotaging computer information system, in Guangzhou Intermediate People's Court, on 30 October 2007.

Wuxi Binghu District People's Procuratorate VS. Ma Zhisong etc. for illegally intruding into computer information systems in Wuxi Intermediate People's Court, on 30 October 2008.

Beijing Haidian District People's Procuratorate VS. Zhang X for sabotaging computer information system, in Beijing Haidian District People's Court on 19 December 2008.

Nanning Qingxiu District People's Procuratorate VS. Chen X for fabricating and deliberately spreading false terrorist information, in Nanning Intermediate People's Court, on 12 December 2008.

Shanghai Yangpu District People's Procuratorate VS. Pu X for Sabotaging Computer Information System in Shanghai No. 2 Intermediate People's Court, on 22 June 2009.

Suzhou City Huqiu District People's Procuratorate VS. Hulei and Liquan for sabotaging computer information system in Suzhou City Huqiu District People's Court, on 12 November 2009.

Shanghai Jiading District People's Procuratorate VS. Zhou Xiongfeng for sabotaging computer information system, in Jiading District People's Court, in 2009.

Fujian Province Changting County People's Procuratorate VS. Tongli and Cai Shaoying for sabotaging computer information system, in Changting County People's Court, in 2009.

Suqian City Sihong County People's Procuratorate VS. Sun Xiaohu for sabotaging computer information system, in Suqian City Intermediate People's Court, in 2011.

Changsha City Wangcheng District People's Procuratorate VS. Li X for illegally obtaining computer information system data, in Wangcheng County People's Court, on 9 March 2012.

Changzhou City Wujin District People's Procuratorate VS. Weng lingqi for illegally obtaining computer information system data in Changzhou City Wujin District People's Court on 23 November.

Qianjiang District People's Procuratorate of Chongqing VS. Yang X for sabotaging computer information systems in Qianjiang District People's Court, on 1 February 2013.

Books

1. Yu Tongzhi, Cyber Crime, Hot and Difficult Cases Analysis Series, Law Press China, 2008.

2. Huang Zelin, The Implementation of Criminal Law to Cyber Crime, Chongqing People's Press, 2005.

3. Wang Yunbing, Cyber Crime, Economic Administration Press, 2002.

4. Zu Xiuzhong, Network and Cyber Crime, Zhongxin Press, 2003.

5. Yu Zhigang, Judicial Response to Difficult Issues in Computer Crime Cases, Jilin People's Press, 2001.

Articles

1. Bin Liang & Hong Lu, Internet Development, Censorship, and Cyber Crimes in China, *Journal of Contemporary Criminal Justice* 26 (1)103-120, 2010.

2. Zhang Jianwen, The Current Situation of Cybercrimes in China, part of the International Centre for Criminal Law Reform and Criminal Justice Policy and GeoSpatial SALASAN Programme, November-December 2006.

3. Cyber Crime Strategy, presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, March 2010.

4. Charles Doyle, Cybersecurity: Cyber Crime Protection Security Act (S.2111, 112th Congress)-A Legal Analysis, *Congressional Research Service Report for Congress* 28th January, 2013.

5. Cyber Crime: Its Impact on Government, Society and the Prosecutor, An Aid for Assisting the Prosecutor in the Investigation, Trial and Conviction of the Cyber/Computer Criminal.

6. Jessica Habib, Cyber Crime and Punishment: Filtering out Internet Felons, Fordham Intellectual Property, *Media and Entertainment Law Journal* Spring 2004, 1051.

7. Tammy J. Schemmel, WWW.STOPCYBERCRIME.COM: HOW The USA Patroit Act Combats Cyber-Crime, *William Mitchell Law Review* 2003, 921.

8. Donald R. Mason, Sentencing Policy and Procedure as Applied to Cyber Crimes: A Call for Reconsideration and Dialogue, *Mississippi Law Journal* Winter 2007, 903.

9. Robert H. Humphrey, Cyber Crimes: Bullying, Stalking, Sexting & Texting, *Rhode Island Bar Journal* March/April, 2011, 29.

10. Debra Wong Yang & Brian M. Hoffstadt, Countering the Cyber-Crime Threat, *American Criminal Law Review* Spring 2006, 201.

11. Charlotte Decker, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, *Southern California Law Review* July 2008, 959.

12. Li Weidong, Network Crime and its Determination, *Journal of Political Science and Law* April 2006, 37.

13. Er Peng, On Determination of Cybercrime Jurisdiction, *Journal of Yunnan University law Edition* 2004 (17) 23.