International Journal of Cyber Criminology
Vol 9 Issue 2 July – December 2015

Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime

Xingan Li[1]
Tallinn University, Estonia

Abstract

Since the advent of the network era, different countries adopted different stance on maintaining social order in cyber space; soft, strong, or medium. In China, as in some other countries in the same group, a tough approach has been taken from the beginning. The purpose of this article is, by studying a series of legal actions against cyber crime, to explore in to the Chinese model of regulation of cyber space. In order to exercise control over the Internet, China has implemented statutory laws and administrative regulations revolving activity criminalizing, content filtering and user monitoring so as to maintain security and stability at both community and state levels. A tight legal and regulatory network has gradually weaved through recruitment of cyber police, investment on security technology, regulations on communications enterprises, and surveillance over users. Regardless of critics, this model was proved to have the merits of effectiveness in the specific socio-legal context in a short term.

Keywords: Chinese Law, Cyber crime, Criminalization, Regulation of Cyberspace.

Introduction

Recent two decades witnessed a swift transforming of human and social landscape due to the pervasive use of digital networks, which connect individuals, institutions, businesses and agencies spreading over the world. The growing convenience for creating, depositing, processing, transmitting, and retrieving of information increased the quantity of data in both static and dynamic processes, improved virtual communication, developed social networks, and at the same time, risks, threats and dangers have also been un-ignorable problems.

Naturally, it was not strange that information systems in the background of Chinese history had been regarded as a modern instrument in an ancient territory. In fact, many countries were confronted with similar challenge at the dawn of the information age, when they were perplexed for how to benefit from the pervasive use of information systems while avoiding negative political and legal impact of unmonitored users, uncensored information, unchecked communications, uncontrolled activities and unsolicited visits. Such potentialities were also eroding footstones of the Chinese Great Wall.

Additionally, migration of criminal phenomena into information systems-facilitated cyber space has attracted increasing attention due to its high pace of expansion (Li, 2008;

[1] Associate Professor of International Law, School of Governance, Law and Society, Tallinn University, Tallinn, Estonia. E-mail: xingan.li@tlu.ee

Li, 2009). The 1997 Penal Law of China (which was usually translated as Criminal Law, but, Penal Law should be more exact translation) provided fundamental criteria and guidelines for convicting and sentencing cyber criminals. With assistance of a series of other statutory laws and administrative regulations, a legal and regulatory system has been taking shape to suppress the spread of cyber crime of multiple forms, the so-called new century's pestilence, in cyberspace. The explosion of new and pertinent laws and regulations over the past two decades reflected society's concerns on the ancient phenomenon in a modernized context, and efforts to wrestle with it. Yet, it remained uncertain whether the current approach to deter and redress cyber crime would prove to be successful.

In the following sections, this article will review the process of establishing the legal framework on cyber crime in China, examine the features of Chinese laws and regulations tackling cyber crime, and analyze the policy for preventing cyber crime through control over cyber space in China. The article will also analyze the subject, the means, the mechanism and the main purpose of control over cyberspace, with review of its actual effects and defects.

1. Criminalization and Penalization of Cyber Crime

The "chance encounter" of communist China based on its ancient land and people with the information network had multiple potentialities of changing the politico-social order, which were unexpected and unprepared events in the late 20th century. According to official statistics, to the end of 2014, the number of Internet users in China reached 649 million and the number of mobile Internet users reached 557 million (China Internet Network Information Center, 2015). The use of mobile instant message apps had grown steadily, attracting 91.2% of the mobile Internet users (ibid.). Cyber security accidents and cyber criminal cases are both increasing stubbornly (The National Computer Network Emergency Response Technical Team/Coordination Center of China, 2014). Crimes and criminals come in all varieties on the Internet, ranging from the catastrophic to the merely annoying (Icove et. al., 1995). Therefore, defined broadly, the term "cyber crime" could reasonably cover an extensive variety of criminal offences, activities, or issues. In China, the term has been the same from the beginning, pronounced as "jisuanji fanzui" (computer crime). Now, the term more frequently used is "wangluo fanzui" (network crime). Nevertheless, there has never been an official term for it. The crimes promulgated in the Penal Law of China are more complicated, because the Penal Law itself did not give simplified names to any offences.

In Chinese academic world, a variety of definitions were introduced from the Western countries, or some new definitions were proposed, including those either in broad sense or in strict sense. Most of these definitions have been derived from the Western countries, with their books and articles translated into Chinese and published in China. The subsequent study witnessed some rational thinking about the issue, and some definitions came into being which possessed the Chinese style. The definitions introduced to China and proposed by Chinese scholars had profound academic significance before the amendment of the Penal Law in 1997. The following sections will comprehensively review these terms and definitions through taxonomic analysis.

1.1. Three layers of cyber crime conception

Cyber crime, as a conception with broad interpretation, has been defined at three different levels in China's laws:

At the first level, computer crime was prescribed by Articles 285, 286, 286-1, 287, 287-1 and 287-2 of the 1997 Penal Law in Chapter VI, "Crimes of Disrupting the Order of Social Administration" (1997 Penal Law; 2015 Penal Law Amendment IX). According to the 1997 Penal Law, computer crime is a crime in which computer information systems are targets of the crime. But the 2015 Amendment IX expanded criminalization and penalization to network service providers' failure to perform their network security obligations resulting in serious consequences, knowingly providing technical or material support to online criminals, using networks to teach or facilitate criminal behaviour, as well as setting up or utilizing a wireless station (stand) without authorization, or utilizing a wireless frequency without authorization, to disturb wireless communication order. Considering criminalization and penalization of cyber crime at this level, the criminalizing scope was too narrow to cover the practical illegal acts related to computer, and necessitated enlargement in the legislation.

At the second level, it can be stated that the definition of computer crime in the Penal Law is of only nominal meaning. In effect, cyber crime in China covers extraordinarily wide range of offences. When discussing the problem of cyber crime, we should use the term in the criminological sense but not limited to that in the Penal Law. As Li (1992) pointed out that, the traditional Penal Law of China could be interpreted and adjusted to punish cyber criminal offences according to different existing clauses. Actually, it has been usual practice in China as well as in some other countries where there were no existing law dealing with computer crime but computer crimes occurred. It was very rare that perpetrators were left unpunished when offences were detected and convictions were established. Of course, this did not neglect the fact that many existing cases were never detected, and many detected cases were never punished due to substantive law and procedural law obstacles.

At the third level, there were still some more categories clustered in academic research. Computer-related crimes could exist in every chapter of special part of the Penal Law, from offences against national security to those against economy, from offences against person to those against property, etc. (Li 1992) Moreover, as it was concluded that a clear difference between law and policy did not even exist in China, while policy could be similarly effective as those formally enacted law (Clarke 1999). This was determined by the methodology of Chinese mode of thinking, which was on the same basis as the system of guilty analogy that was repealed in 1997.

All the three levels of meanings of cyber crime were similarly important when we analyse Chinese laws, regulations and policy pertinent to cyber crime. It is necessary to indicate that some researchers eccentrically asserted that, "China does not seem to possess any written law or code specifically outlining its computer crime statutes...trials are held by the force of military law..." (Kim, 1997) Unfortunately, this claim was based on a noticeable misunderstanding of the present status of Chinese legal system, which has been developing rapidly and in fact closely following the track that many industrialized countries went along (Li, 2014; Li, 2015). Military offences, which were once prescribed by a single act, which paralleled the Penal Law, were shrunk into one chapter of the whole Penal Law in 1997. Before that, according to this analysis, most computer crimes

could have been penalized according to many pertinent clauses of the Penal Law, or in rare cases, penalized according to military offences.

Obviously, criminal punishments on all offences were harsh in China. Criminal punishment in China ranged from fixed-term imprisonment to death penalty, decided by the types of crimes that were committed. Concerning cyber crime, the Supreme People's Court (2001) ruled that capital punishment might be applied to those who provided state secret to foreign individuals or institutions via the networks and cause particularly serious harm.

1.2. System of cyber criminal Law

Computer crime emerged in China in mid-1980s and was punished within the previously existing legal framework. According to Chinese law, computer was only an object or a tool of various crimes, which could cover counter-revolutionary offence, offence against public security, offence against personal rights and democratic rights, offence against property, offence against social management order, and offence of malfeasance. Different situations, where computer played different roles and caused different harmful results to different targets, can be criminalized and penalized according to provisions on different offences. The old law has since challenged and developed under pressure of the pervasion of the information systems and the emergence of crimes connected with the cyberspace.

Specific regulation on cyber crime started in 1994 when the State Council promulgated the Ordinance on Security Protection of Computer Information System (State Council Decree No. 147, 18 February, 1994). The Ordinance prescribed legal liability for five types of activities: (1) violating security ranking protection systems of computer information systems, and threatening the computer information systems; (2) violating the registration system of computer information systems international networking; (3) not reporting cases happened in the computer information systems according to the prescribed time; (4) refusing to improve after receive the notice from the public security agency requiring improving the security situation; and (5) other acts threatening the computer information systems (Ordinance on Security Protection of Computer Information System, Chapter 4).

These acts were punishable by public security for admonition or rectification upon stopping the computer (Ibid, Article 20). If the conduct violated the public security management, it would be punishable according to Regulations on Public Security Management; if the conduct constituted an offence, it should be held criminally liable according to the then effective 1979 Penal Law (Ibid, Article 24), in which apparently no such an offence like a computer crime was ever mentioned.

Problems involved in such provisions could be analyzed from two aspects:

In case the conduct constituted an offence, it was punishable according to Penal Law. However, the Penal Law of the time did not provide relevant punishment for any offence involving computer system or computer networks (Penal Law of People's Republic of China, 1979). The provision of "when the conduct constitutes an offence, it should be held criminally liable" was in want of immediate legal sources, but was possible to be solved by the potentiality of the existing Chinese law dogmatism through analogical interpretation of existing offences in the Penal Law by the Supreme Court (but note,

conviction through analogy was formally repealed in 1997), or to be solved by a quick amendment of it.

Another problem was that subjects of liability, i.e., those perpetrators who would be held liable for the offence, were not clearly and reasonably defined. For example, in the provision on the offence of "not reporting cases happened in the computer information systems according to the prescribed time" (Ordinance on Security Protection of Computer Information System, Article 24 (3)) obviously imposed liability on the victimized party. That is to say, the users were both the target of the offence and the subject of liability.

However, the interpretation function of the Chinese law was so strong that any legal loopholes could be filled through interpreting and applying the existing law. Consequently, hacking could be a conduct punishable according to the 1979 Penal Law, where provisions were very vague, the openness was strong enough to cover new offences that were initially not defined clearly. However, investigation and conviction of computer crime were treated very carefully due to concerns on the legal gaps, because innovative, enlightened and progressive theoretical, legislative and judicial blueprints would soon change the whole system.

The amendment of Penal law in 1997 added two clauses on computer crimes, one was illegal intrusion into computer information systems in Article 285 and the other, destruction of computer information systems in Article 286. The Penal Law was promulgated at the beginning of the year, when use of the Internet was expanded extraordinarily fast. As soon as some computer crimes were criminalized by the new Penal Law, newer problems on the Internet posed newer challenges instantaneously. As a reaction to new problems, in 2000, the Standing Committee of the National People's Congress promulgated a comprehensive law to maintain the Internet security, Decision on Maintaining Internet Security, which was the only law on Internet security passed by the legislature, besides the 1997 Penal law. It has been 20 years when the 9th Amendment of the Penal Law formally extended criminalization in 2014, by adding three new Articles 286(1), 287 (1) and 287 (2) to cover offences committed by network service providers of failure to perform their network security obligations resulting in serious consequences of causing NSP security failures, providing technical support to criminals, and spreading criminal information.

(i) Criminalizing Intrusion into Computer Information Systems

The offence of intrusion into computer information systems was the conduct of intrusion into computer information systems of national affairs, national defence construction, and of the field of advance science and technology, violating national provision (The Penal Law, Article 285). In a document ratified by the Ministry of Public Security in 1997, Management Measures of Security Protection of International Networking of Computer Information Networks, the conduct of entering the computer information networks or using the computer information network resources without permission was listed as one of the activities threatening computer information networks security and hence prohibited (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 6 (1)). In provisions regulating the Internet online services business locations, managing units and online users were prohibited from illegal intruding into computer information systems or destructing function, data and applied programs of computer information systems and

threatening security of information networks (Ordinance on Management of Internet Online Services Business Place, Article 15 (2)). Obviously, these provisions demonstrated the necessity for extending the prohibition of hacking activities to the extent that Article 285 of the Penal Law could not cover, and added the prohibition of using resources of computer information networks without permission. Acts violating law, administrative regulations, without permission, entering into computer information networks or using resources of computer information networks, should be given warning by the public security agency; when those acts involving illegal income, illegal income should be confiscated; and individual or unit should be combined with a certain sum of fine. In case the situation was grave, when interruption of online services and rectification beyond shutting down the computers were caused, combined punishment should be imposed for an imprisonment not longer than six months. If necessary, the previous institutions that granted the certificate or license might be proposed to withdraw the managing license or abrogate the qualification of online services; if the conduct constituted the conduct violating public security management, it should be punishable according to the Ordinance on Public Security Management Sanctions; if the conduct constituted a crime, penal liability should be imposed according to the Penal Law (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 20).

The decision on Maintaining Internet Security restated that if the conduct of intrusion into computer information systems of national affairs, construction of national defence, and advanced science and technology constituted a crime, penal liability should be imposed according to the Penal Law (Decision on Maintaining Internet Security, Article 1 (2)). However, the decision would not punish general hacking activities, which targeted computer information systems not belonging to China, or targeted computer information systems not belonging to the above three specific categories.

(ii) Criminalizing Information-Related or Content-related Offences

In China, as in some other countries in the world, freedom of speech had specific implications and was evaluated with specific criteria. Free speech in one country might be banned in another country. Therefore, online contents were thought to be posing great challenge to state security and social stability according to the official concerns of China. Due to the significance of information or contents themselves, this made up the single most important category of cyber crime in Chinese law, which could also be used to demonstrate how laws and regulations were affected and alarmed by the Internet, and how laws and regulations would deal with new challenges posed by the Internet.

The first provisions concerning the online contents were implemented in the Temporary Provisions on Management of International Networking of Computer Information Networks of 1996 (promulgated by State Council Decree No. 195 on 1 February 1996, amended on 20 May, 1997). The Provisions required that units and individuals that were engaged in Internet business should abide by related law and administrative regulations, strictly enforce security and secrecy systems, must not engage in transgress and criminal activities of threatening state security and revealing state secret and other activities with the Internet, must not create, retrieve, duplicate and spread information that disturbs the social security and obscene and erotic and other information (Article 13). The Provisions provided that, acts violating these provisions, and violating

other laws and administrative regulations as well, should be punished according to related laws and administrative regulations; if constituting a crime, penal liability should be imposed according to the Penal Law (Article 15).

According to China's law, the provisions presented the determination of the Chinese government to punish the criminal activities on the Internet. In the meantime, it was obvious that emphasis of the provisions was on control of Internet contents, particularly, three categories of information, which was related to state security, public security, and which was obscene and erotic information, were prohibited. It implied the possibility of punishing the activities of creating and spreading computer virus, instructing hacking knowledge, as well as creating and spreading information impeding public security. More seriously, simply to browse certain information was also prohibited according to these provisions.

In Management Measures of Security Protection of International Networking of Computer Information Networks, prohibition on online contents was expanded to nine aspects, primarily covering state security, social stability and personality and reputation, but no reflection to economic interests. Abuse of the Internet was first of all regarded as a potential political threat, while the influence on economy was so far not considered. The Management Measure prescribed that no unit or individual might use the Internet to create, replicate, retrieve, or transmit the following kinds of information (Article 5): (1) inciting to resist or undermine the implementation of constitution, laws, or administrative regulations; (2) inciting to overthrow the government or socialist system; (3) inciting to split the country, threatening national unification; (4) inciting hatred or discrimination among nationalities or harming the unity of nationalities; (5) making falsehoods or distorting the truth, spreading rumours, destroying order of society; (6) promoting feudal superstitions, sexually suggestive material, gambling, violence, murder, terrorism or inciting other criminal activities; (7) openly insulting other persons or distorting the truth to defame other persons; (8) damaging the reputation of state organs; (9) other activities breaching Constitution, laws or administrative regulations.

Since 2000, prohibitions of online contents were re-grouped, however, still into nine categories. The most significant change was addition of prohibition of "breaching state religious policy, advocating teachings of evil cults." Prohibition of online contents was further strengthened and the coverage was broadened. In a series of governmental documents implemented afterwards, nine new prohibitions were specially underlined. These governmental documents involved provisions on Internet services of different departments and in different fields. In September 2000, the State Council passed simultaneously Ordinance on Telecommunications (passed on 31st Standing Meeting of State Council on 20 September 2000, and promulgated by State Council Decree No. 291 on 25 September 2000) and Management Measures on Internet Information Services (passed on 31st Standing Meeting of State Council on 20 September 2000, and promulgated by State Council Decree No. 292 on 25 September 2000). The Ordinance provided that no organization and individual might create, duplicate, publish and spread messages containing these contents via the telecommunications networks (Ordinance on Telecommunications, Article 57). The Management Measures provided that providers of Internet information services must not create duplicate, publish and spread messages containing these contents (Management Measures on Internet Information Services, Article 15). Ministry of Information Industry's Management Provisions on Internet Electronic Bulletin Services (November 2000) provided that no one might publish

messages containing one of these contents in the electronic bulletin service system (Article 9). Ministry of Information Industry's Temporary Provisions on Management of Internet Website Engaged in Business of News Publication (November 2000) provided that news published on Internet websites must not contain these contents (Article 13). Ministry of Education's Notice on Printing and Distributing "Management Provisions on Electronic Bulletin Services of Colleges and Universities Computer Networks" (Jiao She Zheng (2001) No. 10 on 21 October 2001) provided that users of bulletin board system websites should abide by provisions by pertinent laws and regulations, and must not create, duplicate, publish and spread messages containing these contents (Article 13). Management Measures on Internet Domain Names (Ministry of Information Industry, Management Measures on Internet Domain Names, entering into force on 30 September, 2002) provided that no organizations or individuals might register and use domain names containing these contents (Article 19).

The nine new prohibitions covered the following categories: (1) information that breaches basic principles of the Constitution; (2) information that endangers national security, divulges state secrets, subverts the government, or undermines national unity; (3) information that is detrimental to the honour and interests of the state; (4) information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity; (5) information that undermines the state's policy towards religions or that advocates the teachings of evil cults or that promotes feudalistic and superstitious beliefs; (6) information that disseminates rumours, disturbs social order, or undermines social stability; (7) information that spreads pornography or other salacious materials; promotes gambling, violence, homicide, or terrorism; or instigates crimes; (8) information that insults or slanders other people, or infringes upon other people's legitimate rights and interests; or (9) other information prohibited by laws or administrative regulations.

In sum, some governmental documents pertinent to regulation on cyberspace supplemented the nine new prohibitions. Subsequently, ten prohibitions took a shape with the addition of one more prohibition, i.e., prohibition on "threatening social morality or national excellent cultural tradition", listed before the previous ninth prohibition, elaborated by such documents as Ordinance on Management of Internet Online Services Business Place (promulgated by State Council Decree No. 363, entering into force on 15 November 2002), which provided that no management units of Internet online services business place and online consumers might use the Internet online services business place to create, download, duplicate, retrieve, publish, spread or use messages containing these contents by other means (Article 14); Article 17 of the General Office of Press and Publications and Ministry of Information Industry's Temporary Provisions on Internet Publication Management (entering into force on 1 August 2002) provided that Internet publications must not publish these contents (Article 17); Ministry of Culture's Temporary Provisions on Internet Culture Management (entering into force on 1 July 2003) provided that Internet culture units must not provide cultural products containing these contents (Ibid, Article 17). From these laws and regulations, a clear picture on how the Internet affected Chinese law and how Chinese law dealt with the Internet was painted.

In Management Measures on Video and Audio Programs Spread on Internet and other Information Networks issued by General Bureau of State Broadcasting and Television (entering into force on 10 February 2003), these prohibitions were further extended to 12

categories by adding false information and overseas programs received and recorded from the networks or overseas media as programs forbidden to spread through information networks (Article 19). However, shortly afterwards, these measures were repealed by new document of the same name issued in July 2004, entering into force in October of the same year, when these two new categories were removed and only ten prohibitions left.

As an important law criminalizing certain (regarded as harmful) activities on the Internet, the prohibitions in the Decision on Maintaining Internet Security could be summarized into three categories nine aspects. The law provided that if any one, who committed one of these acts and constituted a crime, should be held liable according to the Penal Law. Here is a panorama of the legal system containing criminalized activities that mainly involved online information and contents alone:

(1) Maintaining state security and social stability: (a) The acts of exploiting the Internet to disseminate rumours, slander or publish, to spread other harmful information, to instigate to subvert state regime, to overthrow socialist system, or instigate to split the state, to undermine the state unity (Decision on Maintaining Internet Security, Article 2 (2)), was indictable as the offence of instigating to subvert state regime (Punishable according to the provisions of Articles 105 (2), 106, 56 and 113 of Penal Law) and offence of instigating to split the state (Punishable according to the provisions of Articles 103 (2), 106, 56 and 113 of Penal Law).

(b) The conduct of stealing, divulging state secret, intelligence or military secret (Decision on Maintaining Internet Security, Article (2)), might constitute offence of stealing, spying out, purchasing, illegally providing state secret, intelligence (Penal Law, Articles 111, 113, and 56), offence of illegal obtaining of secret (Ibid, Article 282 (1)), offence of illegal possessing of state secret (Ibid, Article 282 (2)), offence of internationally divulging state secret (Ibid, Article 398), offence of negligently divulging state secret (Ibid, Article 398), offence of illegally obtaining of military secret (Ibid, Article 431 (1)), offence of stealing, spying out, purchasing, illegally providing military secret (Ibid, Article 431 (2)), offence of intentionally divulging military secret (Ibid, Article 432), and offence of negligently divulging military secret (Ibid, Article 432).

(2) Information that instigated ethnic hatred or ethnic discrimination, or that undermined national unity, or violated national customs and habits: (c) The conduct of exploiting the Internet to instigate ethnic hatred, ethnic discrimination, undermine ethnic solidarity (Decision on Maintaining Internet Security, Article 2 (3)), constituted the offence of instigating ethnic hatred or ethnic discrimination (Penal Law, Article 249).

(d) The acts of exploiting the Internet to organize evil cult organizations, making contact with members of evil cult organizations, undermining the enactment of state law and administrative regulations (Decision on Maintaining Internet Security, Article 2 (4)), constituted the offence of organizing or exploiting superstitious sects and secret societies or evil cult organizations, or exploiting superstitions to undermine the enactment of law (Penal Law, Article 300 (1)), and the offence of organizing or exploiting superstitious sects and secret societies or evil cult organizations, or exploiting superstitions to cause death (Ibid, Article 300 (2)).

(3) Maintaining socialist market economic order and social management order: (e) The acts of exploiting the Internet to marketing false and interior products, or falsely propagate products or services (Decision on Maintaining Internet Security, Article 3 (1)), constituted the offence of producing or marketing false and interior products (Penal Law, Articles 140-150), and offence of false advertising (Ibid, Articles 222 and 231).

(f) The conduct of exploiting the Internet to damage others' commercial credit or merchandise reputation (Decision on Maintaining Internet Security, Article 3 (2)) constituted the offence of damaging commercial credit or merchandise reputation (Penal Law, Articles 221 and 231).

(g) The conduct of exploiting the Internet to infringe others' intellectual property (Decision on Maintaining Internet Security, Article 3 (3)) might be punished according to the offences of infringing trademark right, copyright, patent right or business secret (Penal Law, Articles 213-220).

(h) The conduct of exploiting the Internet to fabricate and spread false information that influences the transaction of securities or futures, or other information that disordered the financial order (Decision on Maintaining Internet Security, Article 3 (4)), constituted the offence of manoeuvring transaction price of securities or futures (Penal Law, Article 181).

(i) The conduct of setting up obscene website or webpage, providing link services of obscene website, or spreading obscene books and periodicals, film, phonotape and videotape or pictures (Decision on Maintaining Internet Security, Article 3 (5)), might constitute the offence of creating, duplicating, publishing, selling, or spreading obscene goods to seeking interests (Penal Law, Articles 363 (1) and 366), and the offence of spreading obscene goods (Ibid, Article 364 (1)).

(4) Protecting personal rights, property rights and other legal rights of individuals, corporations and other organizations: (j) Insulting or fabricating facts to libel others with the Internet (Decision on Maintaining Internet Security, Article 4 (1)) constituted offence of insult and libel. Except those gravely endanger the social order and state interests, these offences are disposed only upon charge of the victim (Penal Law, Article 246).

The Temporary Provisions on Internet Publication Management prescribed that no Internet publication contents primarily targeting the juveniles might contain contents that induced juveniles to imitate activities breaching social morality or activities of transgress and crime, as well as the contents of terror, cruelty or other contents that were harmful to juvenile health of body and mind (Temporary Provisions on Internet Publication Management, Article 18). If the Internet publishing institutions published or transmitted these prohibited contents, however, no criminal liability was prescribed. The illegal income should be confiscated by related authorities. Different sum of fine could also be imposed according to the sum of illegal dealing (Ibid, Article 27).

(iii) Criminalizing the Offence of Interfering the Functioning of Computer Information Systems

The conduct of violating the state provision, deleting, modifying, adding, or interfering the functioning of computer information systems, and causing the abnormal functioning of computer information systems, with the grave after-effect, was punishable by imprisonment of less than five years or penal servitude; with specially grave after-effect, was punishable by imprisonment of no less than five years (Penal Law, Article 286 (1)). Decision on Maintaining Internet Security incorporated the acts of violating state provisions, interrupting computer networks or communications services without authorization, and causing the computer networks or communications systems unable to function normally, into one offence (Decision on Maintaining Internet Security, Article 1 (3)).

(iv) Criminalizing the Offence of Destructing Data and Programs

The conduct of violating state provisions, deleting, modifying or adding to the data and applied programs deposited, processed, or transmitted in the computer information systems, with grave after-effect, was punishable by imprisonment of less than five years or penal servitude; with specially grave after-effect, was punishable by imprisonment of no less than five years (Penal Law, Article 286 (2)).

According to Management Measures of Security Protection of International Networking of Computer Information Networks, and Ordinance on Telecommunications, the above activities were punishable by warning, fine, shutting down business no more than six months; in case involving grave situation, no more than six months of disconnection and rectification could be imposed. If necessary, the previous institution that issued the certificate, or the institution responsible for examination and approval, could be recommended to withdraw the management license or cancel the qualification of connection; if the conduct constituted a conduct violating public security management, it was punishable according to Ordinance on Public Security Management Sanctions; if the conduct constituted crime, the perpetrator should be held criminally liable according to law (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 20).

(v) Criminalizing the Offence of Creating or Spreading Computer Virus

The Management Measures on Computer Virus Prevention (passed by Ministry of Public Security on 30 March 2000) prohibited any unit or individual to create (ibid, Article 5), spread computer virus (ibid, Article 6), and publish false computer viruses epidemic situation to society (ibid, Article 7). Activities of spreading computer virus included: intentional inputting computer virus, threatening security of computer information systems; providing others with files, software, or media containing computer virus; selling, renting, or presenting media containing computer virus; other activities of spreading computer virus (ibid, Article 6). The Management Measures of Security Protection of International Networking of Computer Information Networks prohibited intentional creation or spreading computer virus or other destructive programs (Article 6 (4)). Ordinance on Management of Internet Online Services Business Place also prohibited management unit of business place of Internet online services and online consumers to intentionally create or spread computer and other destructive programs, and threaten the security of information networks (Article 15 (1)).

Ordinance on Security Protection of Computer Information System, also prescribed relevant sanction to such activities (Articles 24 and 20). The Penal Law prescribed that intentional creation or spreading computer virus and other destructive programs, influencing the normal functioning of computer system, with grave after-effect, was punishable according to the provision on the offence of destructing computer information systems (Penal Law, Article 286 (2)). In Decision on Maintaining Internet Security, a similar provision was restated (Article 1 (2)). In publishing false epidemic situation of computer virus to society, different sums of fine could be imposed to both unit and individual perpetrators (Management Measures on Computer Virus Prevention, Article 17).

(vi) Criminalizing the Offence committed by exploiting Computer and the Internet

According to Article 287 of Penal Law, in case where other offences were committed involving the factor of a computer, the acts were punishable according to the pertinent provisions. The other articles of the Penal Law did not contain the term "computer", but some offences could be committed with the help of a computer. Due to validity of Article 287, such activities have been naturally covered by the Penal Law.

The Penal Law prescribed that if a computer was exploited to commit financial fraud, theft, embezzlement, defalcation, theft of state secret or other offences, the perpetrator was punishable according to related provisions of the Penal Law (Article 287). Decision on Maintaining Internet Security prohibited theft, fraud, and racketeering exploiting the Internet (Article 4 (3)).

The coverage of Management Measures of Security Protection of International Networking of Computer Information Networks was even broader. No unit and individual might exploit the Internet to threaten state security, divulge state secret, infringe state, social, collective interests and citizens' legal interests or engage in activities of transgress and crime (Article 4). The conduct violating this provision was punishable according to laws and statutes (ibid, Article 22).

Exploiting the Internet to commit other offences not explicitly listed in Articles1-4 of Decision on Maintaining Internet Security, could also be held criminally liable according to pertinent provisions of the Penal Law (Decision on Maintaining Internet Security, Article 5). This article reserved the spirit of Article 287 of the Penal Law; further extending the application scope to offences committed exploiting the Internet (besides a computer) as an instrumentality.

(vii) Criminalizing the Offence of Infringing Freedom of Communications

The users' freedom and secret of communications were protected by law. No unit or individual might violate the provision of law, exploiting the Internet to infringe users' freedom and secret of communications (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 7). The conduct violating the provisions of law, exploiting the Internet to infringe the users' freedom and secret of communications was punishable according to laws and statutes (ibid, Article 22).

Decision on Maintaining Internet Security criminalized the conduct of illegal interception, modification and deletion of others' electronic mail or other data and information, infringing the citizen's freedom and secret of communications (Decision on Maintaining Internet Security, Article 4 (2)).

These activities were punishable according to pertinent provisions in the Penal Law (Penal Law, Article 252). The electronic mail and other data were brought into the field of communications. The Internet was the means, only by which this offence was committed.

(viii) Criminalizing the Conduct of Network Service Providers failing to perform their Obligations

In 2014, the 9th Amendment of the Penal Law added a new provision holding network service providers liable for their failure to perform their network security obligations resulting in serious consequences. If network service providers did not perform information network security management duties as provided by law or administrative regulations, and upon being ordered by the oversight and management department to

adopt rectification measures still do not make corrections, they were punishable by up to three years imprisonment, short-term detention or controlled release, and/or a fine. One of the following situations must be met for the conviction: (a) where it resulted in the transmission of a large volume of unlawful information; (b) where it resulted in disclosure or user information causing serious consequences; (c) where it results in the destruction of evidence in a criminal case and the circumstances are serious; or (d) there are other serious circumstances (Penal Law, Article 286-1).

(ix) Criminalizing the conduct of using Information Networks to Commit other Offences

Use of information networks to commit any of the following conduct, where the circumstances are serious, is punishable by up to three years imprisonment or short-term detention, and/or a fine: (a) setting up a website or mail list used to conduct fraud, transmit criminal methods, make or sell prohibited or controlled items, or other illegal activities; (b) publishing illegal or criminal information related to producing or selling drugs, guns, obscene items or other prohibited or controlled items; and (c) publishing information for committing fraud or other illegal or criminal activities (Penal Law, Article 287-1).

(x) Criminalizing the Conduct of spreading Criminal Information

Clearly knowing that others are using information networks to perpetrate crimes, and providing them with technical support such as internet access, server hosting, web storage, or communications transfer, or providing help such as in advertising and promotions or paying bills, where circumstances are serious, is sentenced by up to three years imprisonment or short-term detention and/or a fine (Penal Law, Article 287-2).

(xi) Criminalizing other conducts threatening Computer Information Networks Security

Management Measures of Security Protection of International Networking of Computer Information Networks prescribed that violating laws and administrative regulations, any other conducts threatening the computer information networks security, should be imposed a warning, fine, or shutting-down of business for no more than six months; in grave situation, no more than six months of disconnection and rectification might be imposed. If necessary, proposal could be made for the previous institution that issued the certificate, or the institution examined and approved, to withdraw the management license or cancel the qualification of networking; if the conduct constituted a conduct violating public security management, it was punishable according to Ordinance on Public Security Management Sanctions; if the conduct constituted crime, the perpetrator should be held criminally liable according to law (Article 6 (5) and 20). Here, the term "law" that could impose criminal penalties included but was not limited to the Penal Law.

2. Control over the Internet

From the very beginning, China has been making efforts to create a giant domestic intranet while barring out the global Internet in order to control the network by central government (Franda, 2002, p. 187). The goals of China's operations against online activities, which were regarded as harmful, were more concentrated on maintaining state security than any other aspects. As long as cyber security was concerned in the Chinese context, it has frequently been understood as a critical part of state security. The authority

tended to view the single access to information that was different from political interests as potential threats to stability, and thus showed no tolerance. Thus, freedom of speech bears different meaning from the notion in the Western world. As introduced in previous parts of the article, dozens of laws, rules, and regulations have been installed to normalize the use of the information network services. Traditional official agencies have been granted new functions, while brand new agencies and institutions have been established to exercise control over the Internet.

In regulating information network services, particularly online speech and business information caused great anxiety from enterprises and human rights organizations.

2.1. Central Players: Cyber Police

In order to exercise control over the information networks, i.e., to control users and Internet service providers (ISPs), many traditional agencies and new agencies found their way into the new domain and coordinated in the new battlefield. One of them is, state security agency, a less publicized intelligence agency, has been said to play a critical role in fight against conducts threatening state security. Within public security agencies, cyber police teams, armed with knowledge and skills of information technology, were established. From publicly available information, state security agency was relatively a small entity, and of course was not the only and the primary agency to exercise control over conducts on the Internet. Comparatively, cyber police forces were by far the strongest among all the agencies with the task of tackling malicious online conducts. The actual control over the Internet went beyond the imagination of people from outside world. Users should always go online with great care for fearing that they would be shadowed by the police, listed in the blacklist, and secretly detained and investigated, or even publicly arrested. Those who actually violated laws and regulations might face punishment of different severities.

On the other hand, actual controllability of online conducts has been proved to be weak. Early surveillance of computer networks in China was hampered by such obstacles as insufficient cyber police force, out-dated computer protection equipment imported in the 1980s and 1990, and slow development of computer protection products. Once lagging behind in science and technology of computing, today's China has changed dramatically in recent two decades. With the growth of cyber police in number, power, knowledge and skills, techniques, experience, more and more websites and messages might be monitored and blocked, and more and more users might be investigated and punished. Of course, the factor that the government might become more tolerant of some of the online conducts and messages has also changed more or less the nature and feature of laws, regulations and particularly policies.

3.2. Major Means: Blockade of the Information Network

Blockade was a term used in International law to denote the action of the outside world to block a certain state. But the Chinese blockade of the information network did not mean the same. On the contrary, it meant that China blocked itself from the outside information network. The original idea was to create a *"Chinternet"*, the information network with Chinese characteristics. Once it proved to be impossible, China turned to fence the information network with such things as those walls built around private yards and between neighbours in old times to function as let-in and let-out switch. The term

"blockade" of information networks covered a wide scope of meaning, from limiting access to banning certain contents. Blockade was not the only effect that illegal contents might cause, but breach of which was also the reason for further legal actions. Merely breach of the blockade might already incur punishments at various levels, which might take many forms such as being deprived of the permit to use the network, or fines, confiscation of equipments as well as prison terms.

The most efficient way of exercising control over online activities was through control over access to the network. In China in late 1990s and early 2000s, cyber café was a very popular business, facilitated with the then newest generations of computer and fastest network connections. These cyber cafés could become the focus of law enforcement because most of the online conducts and messages would take place there. As a method of blockade, close-down of net cafés was warmly welcomed by the police forces, which could benefit by ways of transferring equipments under their control, or in many cases by taking bribes from owners of the businesses. It depended on how the state policy was: if the policy permitted such businesses to continue, a sum of bribery would ensure that the business would continue; or if the policy prohibited such businesses some day, the business owners might lose anything due to breach of the new policy. Many possibilities existed, but one of the most interesting requirements on business owners was to keep a list of their customers, who were registered in the list by showing their identification cards. Once there were suspected offences, the list should be submitted to authorities so as to make it more convenient to investigate the cases. However, thousands of net cafes throughout China were forced to close down throughout 2000s. In addition, authorities required users of online services to buy specific personalized identity cards, enabling close monitoring the websites that they surfed. A user must register her/his personal details, such as name, age and address, which would be kept in a central database. Control over the online services proved to be costly, a fact that the authorities have already realised. However, it seemed to be identified as the most effective method and all attempts were made to be practised.

From those laws and regulations cited in previous sections, it was obvious that it was not a secret that the government made great efforts to regulate online contents. Cyber police were responsible for sniffing out and blocking access to those proxy servers located outside China. A broad range of new filtering techniques were introduced, including filtering a list of keywords, which were adjusted over time according to development of detailed political and social situations. Some online forums and bulletin board system (BBS) have practised corresponding self-control mechanism. For example, it was almost impossible to register a user account not to say to publish a message in Qiangguo Forum especially from a foreign computer.

What worried the authorities was that the WWW, email, BBS, instant messages (IMs) and social network services (SNSs) have been used by political dissidents, exiles from minority territories, as well as others, to circulate information and to publicize their cause or to seek supports for online petitions. To deal with all these activities, China sought to cooperate with global giant enterprises of online commerce to control the flow of information imported to or exported from China over the networks. This kind of cooperation occurred in both routine filtration and occasional case investigation. In order to survive in the specific online environment in China, many online business companies adopted strategies in subjection to the official requirements, refusal of which might lead to banned access or termination of business within Chinese border. For example, retreat of

Google from Chinese market in 2010 could partly be attributed to strict requirements that Google could not meet.

Some BBSs and forums were strictly limited access within China. In some cyber cafés, the keepers also screened their machines from browsing foreign websites, including free email service providers in a relatively flexible way. Upon negotiation with the managers, they would authorize the use of free web-based email systems. Owners of some cyber cafés formulated two standards of charge, the lower one for services of limited surfing, and the higher one for services of unlimited browsing, due to different levels of risks they might face. In China, it was possible to retrieve adult websites, but it was strictly not possible to retrieve political websites with contents that were identified as threatening communist rule and socialist system. Keepers of cyber cafés had also a stake in serving their customers.

2.3. Core of the Mechanism: Joint Liability

Concerning the responsibility mechanism of control over the online services, joint liability has been established, both macroscopically and microscopically, both in central and local governments. The responsibility and liability bound all pertinent governmental ministries and basis units. If officials were regarded as negligent when malicious conduct took place with grave results, they could face criminal or administrative liabilities. These responsibility and liability were regulated in almost all the laws and regulations concerning control over information networks.

Article 8 of Regulations on Protection of State Secrets in Computer Information Systems on the Internet stipulated the principle that responsibility was borne by the person who placed it on the Internet. It was the basis for punishment of the conduct of revealing state secrets on the Internet. However, this did not exempt the obligation of individual ISPs to monitor the Internet. Under Article 10, ISPs, BBSs, chat rooms or newsgroup organizers were required to set up their own management mechanisms to assist ensuring that their users transmit no state secret on the Internet.

Nonetheless, this kind of joint liability was similar to personal liability in cases of someone breaching the birth control policy. However, if the criminal fled, the liability would be transferred to certain scapegoats. Chapter IX of the Penal Law of China provided the liability for neglecting duty for government functionaries, under which officials must be careful in exercising their duties, and under the pressure of which they must also closely monitor a school of other players involved in online services, regardless of their identities as providers or users.

2.4. Purpose of Regulation: State Stability

What posed a great challenge to the artificial political system was that more people than ever used the information networks to propagate their "anti-revolutionary", "liberalist", and "separatist" ideas, made complaints and express their discontent. "Chinese people" was not a term that tallied with the Chinese territory. All over the world, there were Chinese who owned various national, political and religious views inherited from each historical period. Although policies of China have taken a big stride toward democracy and freedom within the past four decades when it carried out reform and openness to the outside world, various views still could not be in harmony with the official stance. In particular, Chinese government has never publicly admitted that it made any of its policy

under any outside pressure or in accommodation to the views of any dissident groups. That was an issue of "face", which meant no compromise under pressure.

Free information was not limited to that was useful to commerce and technology. However, in the context of China, regulation on the Internet was designed to eliminate harmful information while reserving useful information. People from some other countries worried that this kind of regulation would have negative effect on protection of human rights and development of economy, just contrary to the spirit of the Internet.

In fact, besides the action against information breaching state political interests, China also contributed to maintain the security of information systems. Most of the prosecuted cases have been criminal offences involving embezzlement, fraud, hacking and defacing, and virus spreading. Therefore, by emphasizing that China concerned and thus did a lot in maintaining state stability, it did not reject all the efforts of the Chinese authorities in combating cyber crime in recent years, when more and more perpetrators, who were involved in both domestic and international offences, have actually been investigated by Chinese cyber police.

2.5. Negative Implications of the Regulation

People always had scruples when they went online, worrying that they might retrieve web pages with contents that the government might impose a ban. Laws and regulations provided only rough principles on identifying contents that were banned. Users had to judge by themselves whether or not the retrieved contents were prohibited. For example, if users opened an online forum full of messages with various opinions, they must judge at the first sight which category the web pages belonged to: separatism, terrorism, dissidents, or national secret. The users could only skip those web pages, close them with great care, and leave the machine with great panic. This kind of side psychological effect brought about by strict regulation frightened many users.

3. Critics on Substantive Law System on Cyber Crime

Chinese laws on cyber crime covered a wide range of conducts and implement various penalties. However, there were still many loopholes in these previsions. The main problems were: overlap of provisions, missing of referred regulations and laws, narrow criminalization, narrow constituents, and laggard penalties. The following sections present these problems in detail.

The first aspect involved overlap of provisions. Article 286 of the Penal Law provided different activities. The first paragraph criminalized the conduct of destructing computer information systems. The second paragraph outlawed the conduct of destructing system data and applied programs. The third paragraph prohibited the conduct of intentionally creating and spreading viruses. The first two paragraphs were termed from the aspect of objects of the conduct, while the latter one was termed from the aspect of form of the conduct. By comparing these three paragraphs, we could find that they were overlapped. Generally, creating and spreading computer viruses could result in abnormal operation of the systems, and could also destruct data and applied programs in the systems. At present, most of the abnormal operation of the computer systems and the destruction of data and applied programs were committed by the use of computer viruses. This resulted in the simultaneous application of the two paragraphs. Scholars proposed that a solution to this problem is to divide conducts covered by this Article into two different offences; one was direct destruction of computer systems, and the other, destruction with computer viruses.

The second aspect mentioned the legal gap formed in referring to other laws and regulations. Compared with European Convention on Cyber crime (CETS No.185), Chinese laws and regulations on cyber crime in fact fully criminalized the activities covered by the Convention. These laws and regulations outlawed various cyber crimes and gave appropriate punishments, including public security management punishments, administrative punishment, penalty and measures limiting the qualification of holding a post. Problems were that when the nature and situation of these criminalized activities were grave, they should be punished by penal law. When the penal law was not perfect (of course no law was perfect, by default, conducts not prohibited by law were permitted), the provision "holding criminally liable according to law" became invalid. Possible problem was that a lighter cyber crime (transgress) would be imposed public security management punishment or administrative punishment, while some of the graver cyber crime (crime) could be held "criminally liable" "according to law," due to missing of such laws.

The third aspect was concerning the narrow scope of criminalization. Huang and Chen (2005) pointed out that Article 285 of the Penal Law limited objects of the offence to computer information systems of national affairs, construction of national defence, or belonging to the field of top science and technology. With development of the Internet, security of other computer information systems has also been necessary to enjoy protection. Therefore, the protection scope should be extended (Huang and Chen 2005).

The fourth aspect criticized narrow legal constituents. According to the Penal Law, subject of computer crime was limited to natural persons. The corporate liability should be added (Huang and Chen 2005). According to Article 17 (2), a person who was older than 14 years old but younger than 16 years old, was only criminally liable for eight kinds of severe offences: intentional homicide, intentional injury resulting in grave bodily harm and death, forcible rape, robbery, sales of drug, arson, explosion, and spread poison. Many of the perpetrators of cyber crime were younger than 16 years old. Some scholars proposed that the scope of subjects of cyber crime should be extended, that is to say, applying a lower liable age. In 2015, when the ninth Amendment of the Penal Law was issued, this problem was partially solved, because a unit now could be held liable for cyber crimes according to the revised clauses.

Finally, the laggard penalty provision was also a focus of criticism. Huang and Chen (2005) also pointed out that the Articles 285 and 286 of Penal Law provided the imprisonment as the only punishment for offences against information systems, without possibility of imposing fine and disqualification. In many other countries, all of the three types of punishments were possible to be imposed. Considering the deterrent effect, they proposed that Chinese law should also be revised to add more types of punishments (Huang and Chen 2005), which were partially realised by adoption of the ninth Amendment of the Penal Law.

Conclusion

In control over the online services, China took a series of actions characterized by content filtering and activity monitoring, for the purpose of maintaining state stability as well as cyber security. A close network was formed to prevent and deter cyber crime by recruitment of cyber police, investment on security technology, imposing requirements on the e-commercial enterprises, and surveillance on users.

These countermeasures that China adopted to fight against cyber crime had commonness with other countries. First of all, criminalisation has been a significant way to incorporate the actions into the legal framework. Notwithstanding the difference with regard to the social system, legal framework in China was developing with a fast step. The penal law was not an exception. Promulgation of the 1997 revision and more subsequent amendments of the Penal Law and a series of regulations helped form a systematic legal framework against cyber crime. Second, Chinese law covered most of the cyber crime offences that have been criminalized in industrialised countries. Therefore, if there was the necessity of international coordination between China and other countries, substantive law basis has been to some extent prepared. Furthermore, Chinese control over the Internet was not without precedents. In practice, many control measures adopted in China were similar to those in the United States and some European countries, despite that there were still differences based on socio-legal contexts.

Certainly, control mode of China had its speciality. Firstly, focuses of legal actions in China were characterised by emphasizing the maintenance of state stability and social order. The core of all focuses was on online speech that breached state regulation. Anxiety of the authorities was that absolute free speech would erode the foundation of state politics, for which criminalisation of content-related offences took an unparalleled coverage than many other countries. Secondly, Chinese legal system was more flexible than many other countries. The forms (or "sources" in jurisprudence) of laws were diversified, including the penal code, special statutes, legislative and judicial interpretations, and administrative regulations, all being integrative parts in criminalizing the pertinent conducts. Thirdly, combat and prevention were designed to be combined with each other. The deterrence system did not only play a role on preventing potential perpetrators from committing cyber crimes but also play a role in detecting occurred offences. Fourthly, strike-hard strategy was used occasionally. Strike-hard strategy has been used in China since early 1980s to clamp down rising waves of crime. At present, this strategy was also used in fighting against various specific crimes, including offences endangering public order, offences of illegal publications, offences related to pornographic materials, etc. Generally, various computer- and network-related offences were fought together with content-related offences during strike-hard actions.

References

China Internet Network Information Center. (2015). 35*th Statistical Survey Report on the Internet Development in China*, Beijing: China Internet Network Information Center.

Clarke, D. (1999). Private Enforcement of Intellectual Property Rights in China. *Intellectual Property Rights in China: Evolving Business and Legal Frameworks*, *10*(2), National Bureau of Research Analysis.

Franda, M. (2002). *Launching Into Cyberspace: Internet Development and Politics in Five World Regions*, London: Lynne Rienner Publishers.

Huang, Z., & Chen, X. (2005). The Defects of Criminal Law Regulation and Theoretical Reaction to Computer Crime. *Jianghai Xuekan*, *3*, 112-118.

Kim, M. W. (1997). How Countries Handle Computer Crime. *Ethics and Law on the Electronic Frontier*, Fall 1997.

Li, X. (1992). A Study on the Application of Criminal Law to Computer Crime, *China University of Political Science and Law Graduate Law Review*.

Li, X. (2008). *Cyber crime and Deterrence: Networking Legal Systems in the Networked Information Society*. Turku, Finland: University of Turku.

Li, X. (2009). *Social Order in Cyberspace*. Hyderabad, India: ICFAI University Press.

Li, X. (2014). Zhongguo Falv Zhidu Daolun (An Introduction to Chinese Legal System). Turku, Finland: Informyth.

Li, X. (2015). Chinese Legal System: A Way Forward. In X. Li (ed.), Selected Readings in Chinese Legal System (pp. xvii-xx). Turku, Finland: Informyth.

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC). (2014). *Report on China Internet Network Security 2013*. Beijing: CNCERT/CC