July, 2008

CYBERSPACE GOVERNANCE IN THE PEOPLE'S REPUBLIC OF CHINA

Kam C. Wong

CYBERSPACE GOVERNANCE IN CHINA

by

Dr. Kam C Wong
Associate Professor
Department of Criminal Justice
Xavier University
Ohio Cincinnati USA

June 29, 2008

Paper under publication review.

CYBERSPACE GOVERNANCE IN THE PEOPLE'S REPUBLIC OF CHINA

CYBERSPACE GOVERNANCE IN THE PEOPLE'S REPUBLIC OF CHINA

I. INTRODUCTION

Computer mediated communication (CMC) in the new Information Age connected by the Internet has brought us closer together as people in a virtual world; transcending geographical distance, time zone differences, social inhibitions[1] or cultural barriers.[2] Compare with traditional communication, e.g. mail or fax, CMC is much faster, cheaper, and effortless. People can share a large amount of information almost instantaneously with the click of a mouse. With the synergetic integration of computer technology and telecommunication technologies, the Internet progressively advances and radically

[1] In the cyberspace, social conventions give way to computer etiquette, which is known for its casualness and informality.

[2] The cyberspace has its own norms and culture, not shared by the real world.

transforms the traditional information infrastructure; allowing people to communicate with each other anywhere, anywhere and in multifarious and interactive ways. In this way Internet becomes a catalyst of reform and development in many social, political, economic, cultural, scientific and government arenas. The catalytic impact of Internet was followed by chained reactions and domino effects, rippling across different loci and penetrating every layer of the society. In this way, the Internet has generated heretofore unexpected consequences and registering far reaching influences. The impact, influence and implications of Internet is quite beyond what has been contemplated originally or acknowledged subsequently. It is still a history in the making. As one perceptive scholars observed, in the 21st century, "attention grows to the potential of the Internet as a public space, with implications not only for purposeful activity (business, education, and so on) but for personal activity, including social interaction and play".[3]

In China, the growth in the use of CMC particularly Internet has been tremendous over the past few years. The growth is exponential, not incremental. Statistics released by the China Internet Network Information Center (CNNIC) recorded a total of 33.7 million Internet users at the year-end of 2001.[4] Some other interesting findings regarding Internet activities in China are also reported by ChinaOnline, a US-based independent organization. For examples, China will have 300 million Internet users by 2005 - by then, the U.S. will have just 200 million; the Chinese Web will be larger than the English Web by 2010; over 64% of Chinese Internet users reported they spent less time watching TV and 67% reported sleeping less since getting the opportunity to use the Internet; E-commerce will grow from 1999's US$42 million to $3.8 billion by 2003; China will have more Internet users than any other Asia Pacific nation by 2001, with 40 million people online; and by 2005, China will have the most Internet users in the world.[5] Although the

---

[3] See Marjory S. Blumenthal, "Communications and Computers", ***Encyclopedia of Computer Science***, ***Fourth Edition (2000)***, (U.K.: Nature Publishing Group, 2000), pp. 243-250.

[4], "The Semiannual Survey Report on the Development of China's Internet (January 2002)", ***The China Internet Network Information Center*** (***CNNIC***), at http://www.cnnic.net.cn. (Visited on February 27, 2002).

[5] Citation by Omar Saleem, "The Establishment of a U.S. Federal Data Protection agency to Define and Regulate Internet Privacy and its Impact on U.S.-China Relations: Marco Polo Where Are You?", ***The John Marshall Journal of Computer & Information Law***, 2000 (Footnote n90: ChinaOnline, "Interesting Facts About China", www.chinaonline visited on

predicted number of 40 million Internet users by 2001 differs from the CNNIC statistics of 33.7 million, by now China does have the largest number of Internet users among nations in Asia Pacific region. The number is still increasing rapidly and the growth rate is estimated to be exponential.

China is fast learning that information technology is the core factor in a successful economic reform, political development, and social change process. PRC Premier Zhu Rongji made a remark that "the use of information technology is vital for the world economy and social development".[6] China scholars of IT have likewise observed that: "Investments in information goods and services are key sources of productivity improvements and economic growth. In postindustrial economies, the future seems to entail the development of a media-saturated society and an information-intensive economy."[7] Chinese leaders have thus adopted a firm state policy to develop strong and powerful information technology, including modernization and globalization of communication network, as the single most important driving engine of China's nascent economic development and social advancement.

The world's economy relies heavily on computer automation and Internet to operate. The amount of financial, military and intelligence information, propriety business data, and personal communications transmitted by and stored on computers is beyond imagination, processing and transacting a huge volume of data. In China, as more and more people come to use CMC, first as a business tool, e.g. searching for business opportunities, and now as a personal instrumentality, e.g. discovering interests and finding communities, CMC has bred natural and inevitable dependency. More and more critical infrastructures – hospital service, air traffic control, military preparedness – are depending on CMC for efficient and effective operations.

November 4, 2000).

6 On February 27, 2002, Chinese Premier Zhu Rongi made the remarks at a lecture held by the State Steering Group of Science, Technology and Education in Beijing. The Vice-Director of China's Information Expert Consultative committee, Zhou Hongren was invited to speak on 'Global e-Government Administration and the Development of China's e-Government Administration' for the State Steering Group of Science, Technology and Education.

7 Milton Mueller and Zixing Tan, ***China in the Information Age – Telecommunications and the Dilemmas of Reform*** (The Washington Papers), (Praeger Publishers, 1997), p. 2

These computers and CMC are vulnerable to attack as subject of crime such as hacking, and all the information being processed via the Internet or other networks is also vulnerable to criminality such as corruption of data and spreading new kinds of computer viruses.[8] In other words, computers, particularly the Internet, facilitate criminality and have engendered a different form of crime.

The term computer crime has been used generally to refer to three categories, namely: computer crime in the strict sense, computer-related crime, and computer abuse. Donn B. Parker, the guru of computer security in USA, has defined of computer crime: "Computer crime may involve computers not only actively but also passively when usable evidence of the acts resides in computer storage. The victims and potential victims of computer crime include all organizations and people who use or are affected by computer and data communication systems, including people about whom data is stored and processed in computers. Anybody using the Internet is particularly vulnerable to computer crime."[9]

According to Professor Parker's definition, computer crime cases [10] may involve computers in one or more of the following roles as: 1. Object such as destruction of computers or computer data or programs contained in a computer; 2. Subject such as a financial fraud case that the financial data stored being changed; 3. Instrument such as using the computer actively in search of passwords and credit card numbers, or passively in the course of a continuing financial embezzlement; 4. Symbol such as using

---

8 For details on types of computer attacks and vulnerabilities, see David Icove, Karl Seger, and William VonStorch, ***Computer Crime: A Crimefighter's Handbook***, (O'Reilly & Associates, Inc., 1995), pp. 5-15 and pp. 17-21.

9 See Donn B. Parker, "Computer Crime", ***Encyclopedia of Computer Science, Fourth Edition (2000)***, (U.K.: Nature Publishing Group, 2000), pp. 349-353.

10 In some cases, the definition of computer crime may become a problem. For example, if a computer is stolen in a simple theft, it would not be classified as a computer crime. If knowledge of computer technology is necessary in the course of criminality, the theft would be considered a computer crime. Another categorization of computer crime is by types of information and information-processing loss: loss of information availability and utility – intrinsic to information such as changing it; integrity and authenticity of information – extrinsic to information such as changing access to it; and confidentiality and possession of information – external to information such as removing or copying the data. (See n12.)

nonexistent computers for intimidation or deception.[11]

This project investigates into and reports upon computer related crime and control in China. Particularly, it investigates into the nature and extent of computer related crime in China and reports upon the effectiveness of legal measures addressing computer related crime. This research project is a first attempt to study cyberspace governance and Internet regulations in China with indigenous PRC data and from a China perspective.

The report consists of the following eight sections.

I. Introduction – providing the background of this study and information technology in China.
II. Literature Review – reporting the existing research work done on the subject and the research gap identified.
III. Researching into China Cyberspace Governance – explaining some research difficulties, data sources and limitations.
IV. Internet in China – outlining IT development and emergence of computer crime in China; the origin and development of Internet in China; and analyzing the disparate growth in the use of Internet.
V. Nature, Prevalence and Distribution of Computer Crime.
VI. Cyberspace Governance in China – presenting China's policy towards cyberspace governance and Internet regulations; Felson's routine activity theory in crime control; China's comprehensive scheme in computer crime control and prevention; legislation and regulative measures in China; law enforcement; cybercrime prevention through education; management control; and technology control.
VII. Impact and Effectiveness of Comprehensive Control – assessing relative effectiveness in applying comprehensive scheme to control and prevent computer crime in China.
VIII. Conclusion – proposing various recommendations in improving cyberspace governance and Internet regulation foster law and order in cyberspace in China.

---

[11] Unless other specified, the terms including "computer crime", "computer-related crime", "computer abuse", and "Internet crime", are used interchangeably throughout this paper.

II. LITERATURE REVIEW

The study of cyberspace governance and Internet regulations in China, both in law and social science, is just beginning. Very little scholarly work has been published. Not much ground, much less controversial issues, have been covered. For example, as of March 20, 2002, an electronic search of Lexis-Nexis law database with the key words "China Internet" uncovered 31 articles,[12] of which only a handful (i.e. seven) are directly

---

12 Articles retrieved as of March 20, 2002 are as follows. #1. Eric R. Biel, THE IMPACT OF TECHNOLOGICAL CHANGE IN THE CANADA/U.S. CONTEXT: THE IMPACT OF TECHNOLOGICAL CHANGE ON DEVELOPING COUNTRIES, ***25 Can.-U.S. L.J. 257*** (1999); #2. Richard Cullen and Pinky D. W. Choy, ARTICLE: THE INTERNET IN CHINA, ***13 Colum. J. Asian L. 99*** (1999); #3. Henry M. Gladney, ARTICLE: DIGITAL INTELLECTUAL PROPERTY: CONTROVERSIAL AND INTERNATIONAL ASPECTS, ***24 Colum.-VLA J.L. & Arts 47*** (2000); #4. John H. Taylor, III, COMMENT: THE INTERNET IN CHINA: EMBARKING ON THE "INFORMATION SUPERHIGHWAY" WITH ONE HAND ON THE WHEEL AND THE OTHER HAND ON THE PLUG, ***15 Dick. J. Int'l L. 621*** (1997); #5. Ewan W. Rose, NOTE: WILL CHINA ALLOW ITSELF TO ENTER THE NEW ECONOMY?, ***11 Duke J. Comp. & Int'l L. 451*** (2001); #6. Lyrissa Barnett Lidsky, ARTICLE: SILENCING JOHN DOE: DEFAMATION & DISCOURSE IN CYBERSPACE, ***49 Duke L.J. 855*** (2000); #7. Stephan Wilske and Teresa Schiller, ARTICLE: INTERNATIONAL JURISDICTION IN CYBERSPACE: WHICH STATES MAY REGULATE THE INTERNET?, ***50 Fed. Comm. L.J. 117*** (1997); #8. Christopher M. Kelly, NOTE: "THE SPECTRE OF A 'WIRED' NATION": DENVER AREA EDUCATIONAL TELECOMMUNICATIONS CONSORTIUM V. FCC AND FIRST AMENDMENT ANALYSIS IN CYBERSPACE, ***10 Harv. J. Law & Tec 559*** (1997); #9. Chelsea P. Ferrette, E-COMMERCE AND INTERNATIONAL POLITICAL ECONOMICS: THE LEGAL AND POLITICAL RAMIFICATIONS OF THE INTERNET ON WORLD ECONOMIES, ***7 ILSA J Int'l & Comp L 15*** (2000); #10. Jack Linchuan Qiu, ARTICLE: VIRTUAL CENSORSHIP IN CHINA: KEEPING THE GATE BETWEEN THE CYBERSPACES, ***4 Int'l J. Comm. L. & Pol'y 1*** (2000); #11. Omar Saleem, ARTICLE: THE ESTABLISHMENT OF A U.S. FEDERAL DATA PROTECTION AGENCY TO DEFINE AND REGULATE INTERNET PRIVACY AND ITS IMPACT ON U.S.-CHINA RELATIONS: MARCO POLO WHERE ARE YOU?, ***19 J. Marshall J. Computer & Info. L. 169*** (2000); #12. Steven M. Hanley, COMMENT: INTERNATIONAL INTERNET REGULATION: A MULTINATIONAL

APPROACH, ***16 J. Marshall J. Computer & Info. L. 997*** (1998); #13. Stephen J. Choi, ARTICLE: GATEKEEPERS AND THE INTERNET: RETHINKING THE REGULATION OF SMALL BUSINESS CAPITAL FORMATION, ***2 J. Small & Emerging Bus. L. 27*** (1998); #14. Wei Luo, GENERAL ARTICLE: HOW TO FIND THE LAW OF THE PEOPLE'S REPUBIC OF CHINA: A RESEARCH GUIDE AND SELECTIVE ANNOTATED BIBLIOGRAPHY, ***88 Law Libr. J. 402*** (1996); #15. Rachael Abramson, ARTICLE: CATCHING FLIES WITH CHOPSTICKS: CHINA'S STRATEGIC LEAP INTO WIRELESS TELECOMMUNICATIONS, ***11 Minn. J. Global Trade 1*** (2002); #16. Brad L. Bacon, ARTICLE: The PEOPLE'S REPUBLIC OF CHINA AND THE WORLD TRADE ORGANIZATION: ANTICIPATING A UNITED STATES CONGRESSIONAL DILEMMA, ***9 Minn. J. Global Trade 369*** (2000); #17. Prof. Nadine Strossen, SHOULD CYBERSPACE BE A FREE SPEECH ZONE?: FILTERS, "FAMILY FRIENDLESS," And THE FIRST AMENDMENT INTRODUCTION:, ***5 N.Y.L. Sch. J. Hum. Rts. 1*** (1998); #18. John F. McGuire, NOTE: WHEN SPEECH IS HEARD AROUND THE WORLD: INTERNET CONTENT REGULATION IN THE UNITED STATES AND GERMANY, ***74 N.Y.U.L. Rev. 750*** (1999); #19. Scott E. Feir, COMMENT: REGULATIONS RESTRICTING INTERNET ACCESS: ATTEMPTED REPAIR OF RUPTURE IN CHINA'S GREAT WALL RESTRAINING THE FREE EXCHANGE OF IDEAS, ***6 Pac. Rim L. & Pol'y 361*** (1997); #20. Marc L. Caden & Stephanie E. Lucas, NOTE: ACCIDENTS ON THE INFORMATION SUPERHIGHWAY: ON-LINE LIABILITY AND REGULATION, ***2 Rich. J.L. & Tech. 3*** (1996); #21. Geraldine P. Rosales, NOTE AND COMMENT: MAINSTREAM LOUDOUN AND THE FUTURE OF INTERNET FILTERING FOR AMERICA'S PUBLIC LIBRARIES, ***26 Rutgers Computer & Tech. L.J. 357*** (2000); #22. Wendy Lei, STUDENT NOTE: ECONOMIC BOON OR REGULATORY BANE? THE EMERGENCE OF THE INTERNET IN MODERN CHINA, ***22 Rutgers L. Rec. 6*** (1997); #23. Kenton K. Yee, ARTICLE: LOCATION.LOCATION.LOCATION: INTERNET ADDRESSES AS EVOLVING PROPERTY, ***S. Cal. Interdis. L.J. 201*** (1997); #24. A. Tom Grunfeld, Ph.D., ARTICLE: HUMAN RIGHTS AND THE PEOPLE'S REPUBLIC OF CHINA, ***9 Touro Int'l L. Rev. 71*** (2001); #25. Kristina M. Reed, COMMENT: FROM THE GREAT FIREWALL OF CHINA TO THE BERLIN FIREWALL: THE COST OF CONTENT REGULATION ON INTERNET COMMERCE, ***13 Transnat'l Law. 451*** (2000); #26. Kristina M. Reed, COMMENT: FROM THE GREAT FIREWALL OF CHINA TO THE BERLIN FIREWALL: THE COST OF CONTENT REGULATION ON INTERNET COMMERCE, ***12 Transnat'l Law. 543*** (1999); #27. Nada Alees Geha , COMMENT: A JOURNEY INTO CYBERSPACE AND ITS EFFECT ON THE RIGHT TO DEVELOPMENT, ***8 Tul. J. Int'l & Comp. L. 391*** (2000); #28. Amy

relevant[13] to the present investigation, namely:

1. Richard Cullen and Pinky D. W. Choy, ARTICLE: THE INTERNET IN CHINA, 13 Colum. J. Asian L. 99 (1999);
2. Scott E. Feir, COMMENT: REGULATIONS RESTRICTING INTERNET ACCESS: ATTEMPTED REPAIR OF RUPTURE IN CHINA'S GREAT WALL RESTRAINING THE FREE EXCHANGE OF IDEAS, 6 Pac. Rim L. & Pol'y 361 (1997);
3. Wendy Lei, STUDENT NOTE: ECONOMIC BOON OR REGULATORY BANE? THE EMERGENCE OF THE INTERNET IN MODERN CHINA, 22 Rutgers L. Rec. 6 (1997);
4. Kristina M. Reed, COMMENT: FROM THE GREAT FIREWALL TO THE BERLIN FIREWALL: THE COST OF CONTENT REGULATION ON INTERNET COMMERCE, 13 Transnat'l Law. 451 (2000);
5. Kristina M. Reed, COMMENT: FROM THE GREAT FIREWALL TO THE BERLIN FIREWALL: THE COST OF CONTENT REGULATION ON INTERNET COMMERCE, 12 Transnat'l Law. 543 (1999);
6. S. David Cooper, ARTICLE: THE DOT.COMMUNIST REVOLUTION: WILL THE INTERNET BRING DEMOCRACY TO CHINA?, 18 UCLA PAC. BASIN L.J. 98 (2000);
7. Clara Liang, NOTE: RED LIGHT, GREEN LIGHT: HAS CHINA ACHIEVED ITS GOALS THROUGH THE 2000 INTERNET REGULATIONS?, 34 Vand. J. Transnat'l L. 1417 (2001).

Knoll, COMMENT: ANY WHICH WAY BUT LOOSE: NATIONS REGULATE THE INTERNET, ***4 Tul. J. Int'l & Comp. L. 275*** (1996); #29. S. David Cooper, ARTICLE: THE DOT.COMMUNIST REVOLUTION: WILL THE INTERNET BRING DEMOCRACY TO CHINA?, ***18 UCLA PAC. BASIN L.J. 98*** (2000); #30. Clara Liang, NOTE: RED LIGHT, GREEN LIGHT: HAS CHINA ACHIEVED ITS GOALS THROUGH THE 2000 INTERNET REGULATIONS?, ***34 Vand. J. Transnat'l L. 1417*** (2001); #31. John Lewis, ARTICLE: CARNIVORE -- THE FBI'S INTERNET SURVEILLANCE SYSTEM: IS IT A RAMPAGING E-MAILASAURUS REX DEVOURING YOUR CONSTITUTIONAL RIGHTS?, ***23 Whittier L. Rev. 317*** (2001).

13 When I say directly relevant, I mean the articles contribute to our understanding of cyberspace governance and Internet regulations in substantive and substantial ways. Most of the articles only referenced China tangentially as a backdrop to the discussion on hand.

A review on the source materials of these writings informs that there is rarely any reference to PRC data sources of the subject matter. This phenomenon is not hard to explain. There are difficulties in accessing local source materials from abroad,[14] particularly before the e-Government[15] initiative promoted by China authorities and on an emerging topic.[16] In studying the footnotes provided in these articles, it is observed that the research work on China Internet is still immature while very few of the reference materials are from law journals or academic research, more so for those articles written before 2000. A further literature search on the English language law journals reveals that there is even less research conducted in the study of computer related crime and control in China, with reference to local source materials and from an indigenous perspective.

As might be expected, the lack of quality research and properly informed literature hampers understanding of cyberspace governance in China by academicians, policy makers and practitioners alike. This research is an effort to address such perceived research deficiency and apparently existing data gap in China cyberspace governance and Internet control. This literature review is a comprehensive study of all English

---

14 The access problem afflicted internal as well as local scholars alike. For example, Jack Linchuan Qiu, a researcher living in Hong Kong from Wuhan, was not able to capitalize his language facility and social connectedness in producing a research based on local data and theory. See Jack Linchuan Qiu, "Virtual Censorship in China: Keeping the Gate between the Cyberspaces," **4** ***Int'l J. Comm. L. & Pol'y*** **1** (2001).

15 Recently (1999-2000) the China government has launched an open government campaign. As a result more and more government information, including law, policy, and cases of regulation on Internet and control is now readily available on the net. In public security, this policy initiative is called "Jingwu gongkai" (Opening up of police work). For example, 100% of all public security bureaus at the national and provincial level are now accessible by the net. In terms of Internet research, there is a section of China Police Report on Internet - "Warning: Internet Trap" http://www.china110.com/topic/49.shtml (Visited March 10, 2002). The corner is devoted to reporting on the latest development in internet crime ("Wang shang qingren, qwingrenjie luo wang" ("Lovers on the net, netted on the lover's day, April 4, 2001) and control ("Quanguo cuti "wang bar" lianwan jia" (Nation crackdown on 20,000 "net café", December 12, 2001).

16 In Cullen and Choy's case, the omission to use local source materials is more difficult to explain since Cullen once worked in Hong Kong and Choy was a law student in Hong Kong.

language law review/journal articles on China cyberspace governance and Internet regulations. It seeks to find out what kinds of research have been conducted in the field of cyberspace governance and Internet regulation in China that are considered necessary and useful in informing the direction, focus and approach of this research.

In embarking on a comprehensive review of the English legal literature in this emerging field, the first thing one notices is a lack of comprehensive, in-depth, and above all else theoretically informed and empirically denominated research on the subject matter. As Table 1 (below) shows, there are only a total of 7 articles published on the subject matter, the first study being conducted in 1997 and the last one in 2001. Most of them, 5 out of 7 publications, are in the form of research note and commentary.[17] In the rest of this section, I will provide a critical review of the law journal articles reported in Table 1, in order to address the more common literature review questions of: what has been done, what have been learnt, and finally what needs to be done and learnt, before I come to terms with the focus and approach of this investigation.

Table 1: Law Journal Articles on China Cyberspace Governance and Internet Control (1996 – 2002)

	2002	**2001**	**2000**	**1999**	**1998**	**1997**	**1996**	**Total**
Law Articles	0	1	2	2	0	2	0	7
As Research Note/Commentary	0	1	1	1	0	2	0	5

With this review, I will start by providing a summary account of each and every article: questions posted, data used, evidence adduced, analysis adopted, findings arrived at, observations made, and conclusion drawn. Then I will make observations about the relative contributions and limitations of each article. With the summarizing of all the articles, I will then be able to present an overview about the state of research into China cyber-governance and Internet research todate.

The articles inform that most researchers have a common interest in the study of whether

---

17 The two articles are: Richard Cullen and Pinky D. W. Choy, ARTICLE: THE INTERNET IN CHINA, ***13 Colum. J. Asian L. 99*** (1999); and S. David Cooper, ARTICLE: THE DOT.COMMUNIST REVOLUTION: WILL THE INTERNET BRING DEMOCRACY TO CHINA?, ***18 UCLA PAC. BASIN L.J. 98*** (2000). The other five studies are published in the form of a research note or commentary.

China will be able to effectively maintain authority and order by controlling the accessibility and flow of information in the Internet. In general, two opposite schools of thoughts are observed. One group of scholars, including S. David Cooper, Scott Feir and Wendy Lei, present their arguments that Internet control in China seems impossible and the regulatory efforts by Chinese authority ultimately will not be successful. On the contrary, some scholars such as Kristina Reed and Clara Liang, hold the view that China's attempt in various control measures is effectively regulating content access of the Internet in the global community.

In their study, Richard Cullen and Pinky D. W. Choy[18] attempt to explore how the China government mediates the tensions between Internet control and the use of Internet in modernization. They believe that the fundamental tenet of the Communist Party of China (CPC) is to control the media. Their article describes in details the historical development of Internet in China, roles and responsibilities of various governing bodies, and regulations implemented. The authors conclude that the government role of "technological modernizers" is in the ascendancy of "controllers" in China. Although both authors have been living in Hong Kong for years, they have omitted to use local source materials from indigenous perspectives for unknown reasons.

Scott E. Feir presents a study[19] on the likelihood that the Chinese authority will succeed in restraining the free flow of information in China. His article briefly describes the existing regulations in China, the objectives of these regulations, and the government structure in law enforcement. Feir also tries to provide information from technical perspective on how and what the Chinese authority could do in monitoring and controlling information flows in the Internet. Cases are cited on how the Chinese authority has handled incidents related to "state security", "state secret", "public order", and "criminal activity". As no cases could be cited directly related to Internet, the author tries to make analogy on how the Chinese authority will react and handle Internet related incidents similar to controlling other communication media. The author concludes that the attempt to restrict access to the Internet through a combination of regulations and

---

18 Richard Cullen and Pinky D. W. Choy, ARTICLE: THE INTERNET IN CHINA, ***13 Colum. J. Asian L. 99*** (1999).

19 Scott E. Feir, COMMENT: REGULATIONS RESTRICTING INTERNET ACCESS: ATTEMPTED REPAIR OF RUPTURE IN CHINA'S GREAT WALL RESTRAINING THE FREE EXCHANGE OF IDEAS, ***6 Pac. Rim L. & Pol'y 361*** (1997).

physical controls ultimately will not be successful.[20] Internet users in China will continue to seek and provide restricted sources of information with the advance in technology and the desire of people for communication and information.[21] This article was the first legal discussion on the subject, and often cited by other authors.

Wendy Lei[22] presents a similar view to Feir in her study on whether China will be successful to effectively maintain authority and order by controlling the accessibility and flow of information in the Internet. Her article refers substantially to news and reports from newspapers, periodicals and magazines as sources on events, facts and figures. It describes what the China government has done in controlling the accessibility and information flow in the Internet. It then elaborates in details how the control is done by four phases: the sources of information, physical access by user registration, physical monitoring of information flow, and severe punishment on cases found. The author further argues that the regulatory efforts will fail from the perspectives of technology, market incentives, and competition between government agencies. The author attempts to provide a long-term forecast on the development of Internet in China. The emergency of Internet is important to China as a forum of discussion and as a means of obtaining information from the West. The Internet remains as a potential threat to the Chinese authority but its decentralized nature is difficult to control. Various factors have profound impact to the Internet development in China, including economic growth, stability of the country, and economic incentive to join the WTO.

In his study, S. David Cooper[23] reviews the challenges faced by China in pursuing Internet technology and markets. He also investigates the possible effects brought by

---

20 In Feir's words, "The Chinese government, not wishing to dissuade foreign investment nor to allow its people unfettered access to information, is attempting to restrict access to the Internet through a combination of regulations and physical controls. This attempt, backed by the rule of an authoritarian government, is likely to meet with only partial success. See n.23.

21 The author's views appear to be typically confined to a foreigner's perspective in understanding China.

22 Wendy Lei, STUDENT NOTE: ECONOMIC BOON OR REGULATORY BANE? THE EMERGENCE OF THE INTERNET IN MODERN CHINA, ***22 Rutgers L. Rec. 6*** (1997).

23 S. David Cooper, THE DOT.COMMUNIST REVOLUTION: WILL THE INTERNET BRING DEMOCRACY TO CHINA?, ***18 UCLA PAC. BASIN L.J. 98*** (2000).

Internet on the future of communism in China. Cooper presents his finding that control of Internet in China seems impossible from both technology and regulation points of view. A brief status of democracy is accounted on Tibet, Hong Kong, Macau and Taiwan. He concludes that democracy in China is an inevitable result of more and more Internet usage and China's communism system will eventually fall in the future.

Kristina M. Reed has researched on Internet control in China and Germany, the two countries that have national firewalls to block illegal and undesired content in the Internet. Reed presents two papers[24] of her study on the differences between the two countries and the impact to their economic growth. A substantial amount of news and reports from newspapers, periodicals and magazines is cited and many websites are also used as reference. The articles compare China and Germany in the following areas:

a. Historical background of the right to free speech
b. Regulation on the Internet
c. The impact of these regulations on e-commerce

While it is difficult to block only illegal sites in the Internet, Reed is convinced that both countries are effectively regulating content access for the global community. This has profound impact to the business resulting in reduction of growth in e-commerce market in both countries. Reed holds a view quite opposite to that of Feir who believes that Internet control will be impossible.

China has issued a cluster of regulations on Internet in 2000. Clara Liang's article[25] attempts to find out whether China has achieved its goal with these regulations. Apart from describing the regulations in details, Liang tries to convince the readers that the China authorities are actually following the same strategies or "bootstrapping" what have been done in the traditional media in regulating the use of Internet. Liang considers China has successfully derived moderate benefits from the Internet industry while

---

24 Kristina M. Reed, COMMENT: FROM THE GREAT FIREWALL TO THE BERLIN FIREWALL: THE COST OF CONTENT REGULATION ON INTERNET COMMERCE, ***13 Transnat'l Law. 451*** (2000); Kristina M. Reed, COMMENT: FROM THE GREAT FIREWALL TO THE BERLIN FIREWALL: THE COST OF CONTENT REGULATION ON INTERNET COMMERCE, ***12 Transnat'l Law. 543*** (1999).

25 Clara Liang, NOTE: RED LIGHT, GREEN LIGHT: HAS CHINA ACHIEVED ITS GOALS THROUGH THE 2000 INTERNET REGULATIONS?, ***34 Vand. J. Transnat'l L. 1417*** (2001).

keeping political unrest in check. Like Kristina Reed, Liang holds the view that China has managed to control access of the Internet contents effectively. Liang further concludes that China has successfully achieved a win-win situation of regulating the Internet for modernization and in a controlled environment.

The above literature study suggests that the research work conducted so far in the field of cyberspace governance and Internet regulation in China has been centered around how China attempts to restrict free information flow and freedom of speech on Internet while the government is eager to gain substantial benefits from its economical development enabled by the new technology. All of them are descriptive study based on newspaper accounts with little original data gathering or independent empirical research and, still less critical analysis of data, empirical support of findings and enlightened debate over issues. In these articles, one does not find any independent investigation into the nature and prevalence of Internet abuse or computer attacks; or any investigation into how the law regulating China Internet is interpreted, applied, received or impacted; or any investigation into whether one or more of the regulating schemes being in fact effective in curbing Internet abuse. Most of the articles follow a similar pattern: a description of the growth of Internet in the world and China, a statement of the problem – attitude of Chinese leaders towards Internet, i.e. economic liberation versus political control; an outline of the regulatory framework; and a listing of the applicable laws. Subsequently most conclusions drawn by these authors on whether the Internet control is/will be effective in China tend to be descriptive comments and lack converging views.

Being the first legal writing in 1997 on the subject matter, Feir's article[26] is frequently cited in similar research studies. Albeit his literature is by no means authoritative in view of the small number of authors and limited research work available in an emerging field. There are supporters on his conclusion that China will unlikely to succeed in controlling free flow of information in the Internet and the technology is weakening the control of the Communist Party of China (CPC)[27] over the people. Liang[28] holds a different view

---

26 Scott E. Feir, COMMENT: REGULATIONS RESTRICTING INTERNET ACCESS: ATTEMPTED REPAIR OF RUPTURE IN CHINA'S GREAT WALL RESTRAINING THE FREE EXCHANGE OF IDEAS, ***6 Pac. Rim L. & Pol'y 361*** (1997).

27 Since China is a one-party State, the views hold by the Communist Party of China (CPC) are usually interpreted as equivalent to that of the Chinese government.

28 Clara Liang, NOTE: RED LIGHT, GREEN LIGHT: HAS CHINA ACHIEVED ITS

after a study on impacts of the Internet Regulations enacted in China since 2000. She concludes in her research that the China government has successfully managed to derive "moderate benefits from the Internet industry while keeping political unrest in check". Despite their different views, both authors fail to substantiate their research with empirical data. This limitation in research data is generally true in other articles under review. For example, the imprisonment of Lin Hai[29] and death sentences of Hao Jing-long and his brother[30] are two popular Internet crime cases referenced but they are not cited from local source.

To conclude, the state of research into China cyberspace governance and Internet regulation to date is immature; research coverage is limited in scope and mainly descriptive in nature; views are divergence and lacking authoritative literature hardly supported by empirical data from Chinese local source. Having identified the research gap, I now turn to report my study on the topic that is based upon literature in Chinese and local data accessible from all possible sources.

GOALS THROUGH THE 2000 INTERNET REGULATIONS?, ***34 Vand. J. Transnat'l L. 1417*** (2001).

29 "On January 20, 1998, Lin Hai, a software entrepreneur was tried for allegedly giving 30,000 Chinese e-mail addresses to "V.I.P. Reference," a United States-based on-line pro-democracy magazine. He was sentenced to two years imprisonment for "incitement to subvert the state."" See Richard Cullen and Pinky D. W. Choy, THE INTERNET IN CHINA, ***13 Colum. J. Asian L. 99*** (1999), n95.

30 "Hao Jing-long, a staff member of the Zhejiang branch of China Industrial and Commercial Bank, and his brother were found guilty of hacking into the bank's data-base from their home. They transferred funds amounting to 720,000 RMB to 16 accounts which had been opened in false names. The two brothers were sentenced to death." See Richard Cullen and Pinky D. W. Choy, THE INTERNET IN CHINA, ***13 Colum. J. Asian L. 99*** (1999), n100.

III. RESEARCHING INTO CHINA CYBERSPACE GOVERNANCE

Research Difficulties

Researching into cyberspace governance and Internet regulation[31] in China is not easy nor straightforward. This is particularly so before 1995 when research into and reporting about cyberspace governance is rare to non-existent. The situation improves substantially and progressively after 1995. However, the existing literatures show that there are more reporting on computer crimes and detailing of legislative measures than understanding the nature of the problem and impact of the regulations. More descriptive account of the historical development and current state of regulatory framework, than a philosophical discussion, theoretical development and policy analysis on why and how best to deal with computer related crimes are sorely missing. There are three major problems in the area of computer crime study in China, lacking a quality team of researchers in studying computer crime; lacking a sound system in filing computer crime cases in supporting data analysis; and lacking a specialized institution to conduct academic research in computer crime and cross-disciplines study in other areas such as electronics, computing science, criminology, sociology, and history, etc.[32]

Overall speaking, there is a lack of previous scientific investigations, i.e. theoretically driven and empirically based research,[33] on the subject of cyberspace governance and Internet control in China.[34] Computer related crime came to China as an emerging

---

31 Though cyberspace governance and internet regulation reference different intellectual domains and specify separate investigation projects, i.e. the former is concerned with the overall control framework – philosophy, policy, theory, and the later is focused on particularly regulatory measures – laws, rules, regulations, cyberspace governance and Internet regulation will be used interchangeably throughout the research to denote the main focus and demarcate the outer scope of this paper, i.e. how cyberspace is governed, controlled and regulated. As a scope statement, cyberspace governance and Internet regulation research necessary implicates the study of computer related crime problems.

32 For more detailed discussion on history and problems of cyberspace governance research in China, see Jiang Ping, ***Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)*** (Bejing: Commercial Press, 2000), pp. 37-45.

33 Theory and empirical data are important in forming the basis of a scientific study to enable a piece of research work being objective and systematic.

34 This is not ONLY a cyberspace issue, but most legal studies issue. Classical analysis of

techno-social-legal problem since late 20th century with the availability of computers to the Chinese people and accessibility of the Internet to the general public.[35] The first computer crime case in China was officially[36] reported[37] in 1986 and the Country was officially accessible to the Internet worldwide starting late 1994[38]. The short history of Internet development[39] and the few cases of computer crime reported[40] in China do not arouse much interest from scholars or practitioners to devote resources for a scientific study to research on the subject socially or legally. Long before cybercrime became a social problem, it has become a technical and political issue, as evident by the joining hand of China computer safety professional committee and Ministry of Public Security, Computer Management and Supervision Bureau etc. Driven by the scientific ideology of

---

the law is the heart of law journals.

35 For background data on computer availability in China, see Statistics of China Internet, China Internet Network Information Center (CNNIC), at http://www.cnnic.net.cn. For a discussion of accessibility issues, see Zixiang Tan, William Foster, and Seymour Goodman, "China's State-coordinated Internet Infrastructure", ***Communications of the ACM*** (1999).

36 There is no computer crime legislation in 1987. The crime was reported as regular theft.

37 The first case was uncovered in Shenzhen on 22-Jul-1986 when a Hong Kong merchant realized that a sum of RMB20,000 was missing from his bank account. Similar finding was reported in a different branch of the bank two months later. A computer operator of the bank, Chen succeeded in transferring the money to his designated account through unauthorized access to the database. See Yu Zhigang and Others, ***Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime)*** (Jilin: Jilin renmin chubenshe, 2001), p.1.

38 In 1994, China's first network (NCFC) was accepted to connect with the Internet, a move endorsed by the Sino-American Federation of Science and Technological Cooperation and the National Science Foundation of the United States. Thereafter China is officially recognized as a country with accessibility to the Internet, to the outside world with a full-function linkage.

39 For more details of China Internet development up to 1999, see report "Evolution of Internet in China" published by CNNIC, at http://www.cnnic.net.cn. (Visited on 27-Mar-2002). In case of any discrepancy between the Chinese report and its English translation, the local language version preempts.

40 Government statistics reported 700 cases in 1999 representing 5 times of that in 1998. See Jiang Ping,. ***Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)***, (Beijing: Commercial Press, 2000), p.153.

CPC and pragmatism of Chinese character in coping with the economic needs, resources priority has been given to research projects on setting safety standards and measures for computer security, data center protection, or E-Commerce development where the research outputs are more geared for the technological and economic advancement of the nation. The people who have been involved in related work/studies are just handful. For example, Jiang Ping is one of the few researchers from a law enforcement agency who specializes in monitoring computer security and fighting computer related crime for over 10 years. So far, Jiang's study is one of the very few local research found that has provided a scientific analysis and supported with empirical data.[41] I'll describe more on his work in the later section.

In terms of Internet crime research, there is a lack of systematic and comprehensive study based on valid and reliable first hand data, e.g. computer crime victimization survey. [42] Before 1995, there is no separate crime category to report, record, or classify a computer crime case for statistical or case analysis purposes.[43] Currently, computer crime is not reported separately in annual PRC police reports.[44] It is very difficult to single out cyber-crime specific cases among traditional crime records. Moreover, it is a general perception that criminal stories made available to the public are usually filtered by government agencies to serve the political needs of the State such as propaganda and socialist education. [45] Similar to other countries, there are always dark figures in cyberspace crime, i.e. undiscovered and/or unreported cases. For examples, in 1995, the FBI's National Computer Crimes Squad estimates that between 85 and 97 percent of computer intrusions in U.S. are not even detected. With sponsorship from the U.S.

---

41 It is regrettable that Jiang's article was not well received nor popularized in China, e.g. there are few references to and citation of her work). More troublesome, his work is not scientific as much as it is an attempt to provide for independent research on the problem.

42 China conducted its first victimization survey in the early 1990s. The survey does not cover computer crime.

43 See Ministry of Public Security internal criminal statistic compilation, ***Gongan Neiqin Gongzuo Shouce (Police Administrative Manual)*** (Beijing: Jingquan Jiaoyu Chubanshe, 1994). See also the relevant categories on statistics, ***Zhongguo gongan baike quanshu*** (***Chinese Public Security Encyclopedia***) (Changchun: Jilin chubanshe, 1989).

44 See ***Procuratorial Yearbook of China (annual)*** (***Zhongguo Jiancha Nianjian)***.

45 In readings of computer crimes reported by the Ministry of Public Security, it is not difficult to notice that the authorities are trying to send messages. Not all cases are reported.

Department of Defense, Richard Power conducted a test to attack a total of 8,932 computer systems participating in the study. The management of only 390 systems detected the attack; among them only 19 of the managers reported the attacks.[46] China faces similar problems of dark figures, even to a worse extent, in tracking statistics of computer crime. Attempting a cyber-crime typically requires sophisticated knowledge and technical know-how of the invisible offender who takes an illegal act in a virtual environment thus causing an unexpected damage/inconvenience to the victims. In most cases the victims are not even aware of the impact to them, or perhaps come to realize the loss after a prolong period. Many corporations, especially those in service sectors, such as finance industry, are reluctant to report a cyber-crime case with a fear of jeopardizing their corporate image and credibility to their customers.

The situation of data availability for Internet research has been improved since 1997 upon the promulgation of the Interim Regulations of the PRC on the Management of International Networking of Computer Information (Amended), and the Criminal Law of the PRC modified to include three articles in Chapter VI regarding computer crime. Article 285 states that "Whoever, in violation of State regulations, invades the computer information system in the fields of State affairs, national defence construction or sophisticated science and technology shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention." Article 286 states that "Whoever, in violation of State regulations, cancels, alters, increases or jams the functions of the computer information system, thereby making it impossible for the system to operate normally, if the consequences are serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention; if the consequences are especially serious, he shall be sentenced to fixed term imprisonment of not less than five years. Whoever, in violation of State regulations, cancels, alters or increases the data stored in or handled or transmitted by the computer information system or its application program, if the consequences are serious, shall be punished in accordance with the provisions on the preceding paragraph. Whoever intentionally creates or spreads destructive programs such as the computer viruses, thus affecting the normal operation of the computer system, if the consequences are serious, shall be punished in

---

46 David Icove, Karl Seger, and William VonStorch, ***Computer Crime: A Crimefighter's Handbook***, (O'Reilly & Associates, Inc., 1995), p.3. See also Jiang Ping,. ***Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)***, (Beijing: Commercial Press, 2000), pp. 105-107.

accordance with the provisions of the first paragraph." Article 287 states that "Whoever uses computers to commit the crimes such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of State secrets shall be convicted and punished in accordance with the relevant provision of this Law." In early 1999, the State Council announced the year of E-Government in building up computer-mediated channels for speedy and convenient communication between the people and government agencies through Internet[47]. With this open campaign launched since 1999-2000, more and more cyberspace related information, including law, policy, regulation, crime cases and control, is now readily available on the website of various government agencies.

---

47 Cheng Qi, "1999 Zhongguo Zhengfu Dashangwang (1999 – The Year of E-Government in China)", ***No. 10 Fazhi Yu Jingji (Legal System and Economy)***, 1999.

Literature in Chinese

Before the web has become a popular press and publishing medium, there are several Chinese journals in law, law and technology, and law and social science that contain research work related to cyberspace governance and Internet regulation in China. For a quick start, I've utilized the rich resources provided in the Universities Service Centre (USC) for China Studies[48] at The Chinese University of Hong Kong. There are several journals informing the early development of Internet research studies by Chinese scholars and practitioners[49] before the 20th century. In fact, most articles under review discuss on computer security, software and data protection, intellectual property right, and legal issues in E-Commerce. Occasionally there are isolated articles sharing the status and experience of computer crime and control in foreign countries. Some of the journals under review that contain relevant articles to this research are listed below in Table 2.

Table 2 - Chinese Law Journals with Relevant Articles up to 2000

Chinese Journal	Period	Publisher/Editorial
Keqi Yu Falu (Science Technology and Law)	1992 to 1996	Zhongguo Kexue Qizhu Faxuehui (China Science Technology and Law Institute)
Jingji Yu Fa (Economy and Law)	1997 to 2000	Jingji Yu Fa Zazhishe (Economy and Law Publisher)
Fazhi Yu Jingji (Legal System and Economy)	1998 to 1999	Quangxi Zhuangzu Zizhigu Fajiju (Legal System Bureau of Quangxi Zhuangzu Autonomous Region)
Xiandai Faxue (Modern Law Sciences)	1998	Xinan Zhangfa Xueyuan (Southwest University of Political Science and Law)
Falu Kexue (Law Science)	2000	Xibei Zhangfa Xueyuan (Northwest University of Politics and Law)
Zhongguo Lushi (Chinese Lawyer)	1999 to 2000	Zhonghua Quanquo Lushihui (China National Association of Lawyers)
Zhishi Chanquan (Intellectual Property)	1999	Zhishi Chanquan Zazhishe (Intellectual Property Publisher)

[48] "Universities Service Centre (USC) for China Studies is known as 'a mecca for China Studies' by many international China scholars. The centre was established in 1963 by Western scholars to serve the overseas professors and graduate students engaged in China studies. The Chinese University of Hong Kong incorporated USC in 1988, and has continued to offer gratis services to China researchers. Today, renown by its accessibility, USC possesses the most extensive collection on contemporary China." See homepage of USC at http://www.usc.cuhk.edu.hk.

[49] For those articles that are in printed format without electronic copies, hard copies are filed with author.

Falu Shiyong (Applying Law)	2000	Guojia Faquan Xueyuan (National Institute of Judges)
Xinfaqui Yuekan (New Regulations Monthly)	2000	Shanghaishi Jingjifa Yanjiuhui (Shanghai Research Institute on Law of Economy)

Most of the articles were written in 1999/2000. The first article touching on the subject was found in 1992 discussing the "Michelangelo" virus.[50] Huang Guomin[51], Wang Shizhou[52], Zhao Bingzhi and Yu Zhigang[53] are few of the pioneers in the initial studies of computer crime and control in China.

The above findings inform us that local research work on computer crime is very rare before the millennium 2000. Starting 2000, more research studies on computer crime are observed. To date, there is not yet a regular journal published by Chinese scholars that specializes on computer crime, cyberspace governance, or Internet regulation in China.[54]

---

50 Guo Liben, "You 'Michelangelo' Bingdu Suoxiangqi De" (Reflection on 'Michelangelo' Virus), ***No.2 Keqi Yu Falu*** (Science Technology and Law), 1992. Starting from the incident of 'Michelangelo' virus, Guo reviews the nature of computer virus in general, discusses available preventive measures, and finally proposes to amend the Criminal Law in fighting the spreading of computer virus.

51 Huang Guomin, "Shilun Jiasuanji Fanzui" (On Crime by Computer), ***No.3 Keqi Yu Falu*** (Science Technology and Law), 1995. The article discusses the nature of computer in general and classifies them into 3 categories: consciously causing damage to the computer and network; abusing the use of computer; and illegal use of computer in achieving one's personal objective.

52 Wang Shizhou, "Lun Diannao Fanzui" (On Crime by Computer), ***No.2 Keqi Yu Falu*** (Science Technology and Law), 1996. Wang proposes measures on prevention of computer crime, protection of information asset, and changes in the Criminal Law against computer crime.

53 Zhao Bingzhi and Yu Zhigang, "Lun Jisuanji Fanzui de Dingyi" (On Defining the Computer Crime), ***No.5 Xindai Faxue*** (Modern Law Sciences), 1998. The article reviews the emerging definition of computer crime and proposes a definition in alignment with the amended Criminal Law.

54 The Peking University Intellectual Property School and the Peking University Center for the Study of Rule of Law has jointly published the first volume of Internet Law Review comprising 14 topics related to Internet. However, the journal is not planned to be a regular publication as stated by the editor Zhang Ping. See Zhang Ping, "Xiezia Beida Jiangtan

Articles of these topics are found discretely under a small sub-topic of other broader academic disciplines. The Gongan Daixue Xuebao (Journal of the Chinese People Public Security University), has a column on computer crime under the heading of Fanzui Yanjiu (Crime Research). The bi-monthly journal, under editorial supervision of the Ministry of Public Security, "is considered one of the most authoritative, prestigious and influential journal in PRC policing community in China."[55] The level of coverage on computer crime in this authoritative journal typically reflects the scarcity of empirical data available in the field for this research.

Apart from the above journals, there is an abundance of Chinese books published on the subject. As mentioned in earlier section, the most prominent and scientific piece of work is by Jiang Ping[56]. Jiang has collected and analyzed 185 cases between 1986 and June, 1999 for his research study on computer related crime in China. His book, Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problem) is very instrumental for future studies of cyberspace governance and Internet regulations in China. The study is nominated a research item in 1999 (reference number 993281201) by the China Gongan, i.e. the Ministry of Public Security. Another book Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime), by Yu Zhigang and Others[57], also provides valuable reference in analyzing the crime cases from criminology and Criminal Law perspectives.

Internet resources certainly are key to any research work of cyberspace related subjects. In addition to the legal publishing agencies[58], such as the Bureau of Legislative Affairs of

---

Zhiwai" (Foreword: Writing Beyond the Forum in Peking University), ***Internet Law Review, Volume 1***, (Beijing: Law Press China, October, 2001), p. 2

55 For a better understanding on Chinese gongan (public security) and research literature, see Kam C. Wong, "Police Reform in China in the 1990s", ***British Journal of Criminology*** (2002). As far as I know, this is the only methodological article on PRC police research.

56 Jiang has collected and analyzed 185 cases between 1986 and Jun-1999 in his research study on computer related crime in China. See Jiang Ping, ***Jisuanji Fanzui Wenti Yanjiu*** (Research into Computer Crime Problems), (Beijing: Commercial Press, 2000).

57 Yu Zhigang and Others, ***Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi*** (Analyzing the Nature of Internet Crime), (Jilin People's Press, 2001).

58 For a comprehensive research guide on Chinese Law and legal sources in North America, see Wei Luo, "How to Find the Law of the People's Republic of China: A Research Guide and

the State Council and the Legal Affairs Committee of the Standing Committee of the National People's Congress, the various government websites and agencies' electronic newsletters are crucial in obtaining timely and official documents on government policy, regulation, and crime case reported in the local language. Mandatory websites relevant to this research include the Ministry of Information Industry[59] (MII), the Ministry of Public Security[60] (MPS), the China Police Daily Online[61], and the China Police Report[62]. MII provides official information such as policy change and regulation enactment related to the information industry covering the cyberspace arena while MPS is assuming the role of cyberspace police. The official websites of MPS and police units of various provinces report to the public on selected computer crime cases after scrutiny. There is a section in the China Police Report, Jingti : wangluo xianjing (Warning : Internet Trap), with an index page located at <http://www.china110.com/topic/49.shtml>, that is of great assets to Internet crime research. This corner is dedicated to reporting on the latest development in Internet crime[63] and control[64] back to late 2000. Local news agencies, such as the People's Daily[65] and Xinhua News Agency[66], are also very helpful in reporting online news on cyberspace policy, Internet regulation and computer crime stories. Online information services provided by established and prestige universities, such as Beijing University and Qinghua University, are useful in contributing to Internet research. For example, the two websites managed by the Peking University Center for Legal Information, chinalawinfo.com and lawinfochina.com are of much value, particularly so if you do not read Chinese or if you need bi-lingual versions of a document. I've

---

Selective Annoted Bibliography", ***88 Law Libr. J. 402*** (1996)

59 ***The Ministry of Information Industry, PRC*** at http://www.mii.gov.cn.

60 ***The Ministry of Public Security, PRC*** at http://www.mps.gov.cn.

61 ***Renmin Gongan Bao Dianziban (China Police Daily Online)*** at http://www.cpd.com.cn.

62 ***Zhongguo Jingwu Baodao (China Police Report)*** at http://www.china110.com.

63 "Wangshang tanqing Jianmian Qiangjie (Falling in love on Web, robbery on dating)", 27-Mar-2002, ***Zhongguo Jingwu Baodao (China Police Report)*** at http://www.china110.com/topic/49/shtml (Visited 3-Apr-2002)

64 "Quanguo Qudi 'Wangba' Liangwan Jia (Nation crackdown on 20,000 'Net Café')", 12-Dec-2000, ***Zhongguo Jingwu Baodao (China Police Report)*** at http://www.china110.com/topic/49/shtml (Visited on 10-Mar-2002)

65 ***Renmin Wang (People's Daily Online)*** at http://www.peopledaily.com.cn.

66 ***Xinhua Wang (Xinhua News Agency Online)*** at http://www.xinhuanet.com.

appended a list of Internet resources for this research to share with interested readers.

Data Sources

The data used in this article come mainly from the Zhongguo Gongan (Ministry of Public Security), Renmin Gongan Bao Dianziban (China Police Daily Online) and Zhongguo Jingwu Baodao (China Police Report). The MPS website is officially open to public since 17-Aug-2001. These other two online bulletins of the China Police present Internet news and Internet crime cases. For this research, I've viewed all Internet news and crime cases reported on these websites, up to early April, 2002. For example, China Police Report under the dedicated corner on Internet crime and control, Jingti : wangluo xianjing (Warning : Internet Trap) has reported 44 articles between December 2000 and March 2002.[67] Earlier cases and crime statistics of this research come from Jiang Ping, Jisuanji Fanzui Wenti Yanjiu (Computer Crime Research), Commercial Press (2000), and Yu Zhigang and Others, Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime), Jilin People's Press (2001). Internet law and regulation published before September, 2000 are adopted from Jisuanji Ji Wangluo Falu Fagui (Computer and Internet Laws and Regulations), Falu Zhubanshe (2000) that is approved by the Law Committee of PRC National People's Congress. Reference on more current regulations and accounts on recent Internet news are primarily cited from the People's Daily Online, Xinhua News Agency Online and China Daily.

---

[67] There are 44 scripts posted on the China Police Report between 12-Dec-2000 and 27-Mar-2002, 1 record in 2000, 23 records in 2001 and 20 records in 2002 at http://www.china110.com/topic/49.shtml (Visited on 3-Apr-2002). It is obvious that not all of the crime cases are reported. See examples in n66 and n67.

IV. INTERNET IN CHINA

IT Development in China and Emergence of Computer Crime

Before we start our investigation into computer crime situation in China, let us first understand the recent development of information technology (IT) and importance of Internet in China, with it the emergency of computer criminality as a social problem.

Since 1990s, China's information technology (IT) industry[68] *has rapidly become one of the three main resources pillars - material, energy and information - in the development of the national economy. As envisioned by the PRC government and as observed by Wu Jichuan,*[69] *Minister of Information Industry*[70] *"The information industry is expected to grow at annual rate of some 20 percent in the next five years."*[71] *In time the IT will become "a strategic industry and a new*

---

68 The information technology (IT) sector of China is one of the largest in the world and its growth rate remains higher than the rest of the world's major markets. Despite much overlap, the IT sector in China is basically divided into five sectors, namely hardware, software, components (especially semiconductors), telecom equipment, and telecom services.

69 Before 1998, multiple government agencies were involved in the managing various sectors of the IT industry causing much confusions and inefficiency. To rectify the situation, the Chinese Government has merged the five agencies, namely Ministry of Post & Telecommunications (MPT), Ministry of Electronics Industry (MEI), State Radio Regulatory Commission (SRRC), State Council Informatization Promotion Office (SCIPO), State Administration of Radio, and Film & Television (SARFT) Network Department, into the Ministry of Information Industry (MII) to manage the IT sector more effectively.

70 The Ministry of Information Industry (MII) was established in March 1998.

71 Wu Jichuan, Minister of MII, made the remarks at the opening ceremony of the 2000 International Forum on the Information Industry, jointly sponsored by the Ministry of Information Industry and Xinhua News Agency on 23-Aug-2000. See "China Attaches Strategic Importance to IT Industry", ***People's Daily Online*** at http://english.peopledaily.com.cn/200008/23/eng20000823_48843.shtml. (Visited on 24-Apr-2002).

area for the growth of China's economy in the 21st century."

The potentiality and important of the IT industry is not lost on the top national and political leadership. In December 2001, at the first meeting of the national leading group[72] on informationalization[73], Chinese Premier Zhu Rongji has called for "greater efforts and better coordination to push forward China's information industry in a market-oriented way …" Premier Zhu and Minister Wu's comments reflects current IY policy in China as espoused earlier by Jiang Zemin, Chinese President and CPC General Secretary. In a preface to the work of "China's Informationization: Exploration and Practice", entitled "Speed Up China's Information Construction", Jiang has called for attaching great importance to the development of the information industry in China and consider it as indispensable to the four modernizations. More specifically, "through information construction the whole Chinese nation should be enabled to achieve a qualitative raise in their knowledge of science and culture".[74]

Looking ahead, by 2005, China's information industry is anticipated to grow over 20 percent, on a scale two times greater than 2000, to produce over 7 percent of GDP according to the country's plans. The National Information Industry Working Conference held in February 2001 reveals the government's expectation on the industry's contributions to the national economy and their five major tasks in 2001-2005 of which three tasks are highlighted here. "First, headway will have to be made on the "bottleneck" of bandwidth so as to build flexible, efficient and safe information infrastructures with outsize capacity and advanced technology. The postal industry should strengthen electronic information and financial services on top of traditional

---

72 The leading group was formed in accordance with a decision by the CPC Central Committee to strengthen leadership over the development of the country's information technology.

73 See "Premier Zhu Calls for More Efforts to Boost IT Industry", ***People's Daily Online*** at http://english.peopledaily.com.cn/200112/28/eng20011228_87593.shtml. (Visited on 24-Apr-2002). The national leading group on informationalization was formed in August 2001 headed by Premier Zhu. Other vice-heads of the group include Hu Jintao, Li Langing, Ding Guangen and Wu Bangguo.

74 See "President Urges Faster Development of Information Technology", ***People's Daily Online*** at http://english.peopledaily.com.cn/200112/27/eng20011227_87579.shtml. (Visited on 24-Apr-2002).

business scales. … Third, efforts will be made on the application of IT technologies … to press forward information-centered construction. Fourth, governmental functions are to be enhanced to form an efficient, well-supported industry management system operating under law and, to create a favorable environment in regard of regulations and market competitions for the development of IT industry. …".[75] The first task in building flexible, efficient and safe information infrastructures addresses direct to the exponential growth in the use of Internet in recent years. The Internet is viewed instrumental to contribute significantly to China's transformation in the years after the country has joined the World Trade Organization (WTO)[76], particularly in the areas of education and economy development. A senior economist in Beijing University, Zhou Qiren pointed out that "China was at a turning point and changing from a supply economy to a demand economy and applications based on the broadband network will be a good way to stimulate people's consumption."[77]

As observed earlier, while the Internet development has boosted economic growth, speeded up social progress, and brought much convenience to the Chinese people in their daily life, Internet has also provided conditions and power for producing and disseminating various kinds of network-related criminal behavior and harmful information as perceived by the Chinese government. A commentary published on the front page of the People's Daily on 12 July, 2001 has summarized precisely the worries faced by the Chinese leaders and their strong wish in fighting this "smokeless war" with all possible measures. "Using legal means to guarantee and promote the healthy development of information network is an important new subject. On the one hand, we should … complete information networking legislation, strengthen enforcement of law and administration of justice, legally attack networking criminal offences and construct a good order featuring the rule of law. … On the other hand, we should … firmly establish

---

75 See "China's Information Industry by 2005", ***People's Daily Online*** at http://english.peopledaily.com.cn/200102/19/eng20010219_62770.html.

76 China becomes an official member of the World Trade Organization (WTO) effective December 2001.

77 See "Internet to Contribute More to China's Transformation", ***People's Daily Online*** at http://english.peopledaily.com.cn/200111/27/eng20011127_85455.html. (Visited on 24-Apr-2002). See also "Connecting China Education Community to the Global Internet - The China Education and Research Network Project (April 20, 1995)" at http://www.isoc.org/HMP/PAPER/077/html/paper.html. (Visited on 24-Apr-2002).

strategic awareness, security awareness and lawful awareness of information network among the people of the whole country, vigorously promote socialist moral standard, create a sound social foundation for the orderly development of information network and promote the healthy development of China's information network."[78]

In the following discussion, I'll account on few major events[79] to illustrate how Internet became a reality to Chinese people in catching up with the world and study the recent development through reported statistics on Internet usage over the past few years. I'll analyze the problems of Internet perceived by the Chinese government and the reasons for the leaders' eagerness to control and regulate.

Origin and Development of Internet in China

In September 1987, China's first e-mail "Crossing the Great Wall to Join the World", by Professor Qian Tianbai, was sent through Chinese Academic Network (CANET), a joint project by the Beijing Municipal Computer Application Research Institute and Karlsruhe University of former West Germany. This marks the beginning of Internet history in China. With a primary objective in boosting the country's economy and technology advancement, the Chinese government has been very supportive on Internet related research. During the period between 1988 and 1993, majority of the network-related activities, in terms of project size and deliverables, took place in academic and research institutes. In December, 1988, Qinghua University campus network linked to University of British Columbia, Canada with e-mail application. In September 1989, a College Network (CASNET) project was launched to build a high speed network inter-connected with Beijing University (PUNET), Qinghua University (TUNET) and the Chinese Academy of Sciences in establishment of a super-computing center. The project, completed in 1992, was a pilot network of education and scientific research (NCFC) for the Zhongguancun area connecting 30 research institutions later. In October 1990, China's Internet top domain name was officially registered as "CN" in DDN-NIC, a

---

78 See "Using Legal Means to Guarantee and Promote Sound Development of Information Network", People's Daily Online at http://english.peopledaily.com.cn/200107/12/eng20010712_74810.html. (Visited on 24-Apr-2002).

79 For a more detail exposition of historical events, see "Evolution of Internet in China", ***China Internet Network Information Center (CNNIC)*** at http://www.cnnic.net.cn/evolution.shtml (Visited on 27-Feb-2002).

network center of ARPANET managed by the U.S. Department of Defense for distributing Internet domain names and IP addresses worldwide. Thereafter, ".CN" is used for China e-mail communication worldwide.

The first direct link from China to the Internet was established in 1993 by the Institute of High-Energy Physics (IHEP) which is part of the Chinese Academy of Sciences (CAS).[80] IHEP connected to the Stanford Linear Accelerator Center (SLAC) of Stanford University via a 64K leased satellite circuit from AT&T. Meanwhile, as the CASNET grew, its unit National Computing and Network Facility Center (NCFC) was designated as the network center, designated China's top domain server, and connected to the Internet at 64K. The Beijing University of Chemical Technology (BUCT) became the third institution in September 1994 to have Internet connectivity via a 64K MCI satellite circuit connected to Consortium of Asian Research and Education Network (CAREN) and John von Neumann Center Network – Princeton University (JVNCnet) which was disconnected in 1997 and switched to CERNET. CERNET, the Chinese Education and Research Network is the largest Chinese network connected to the Internet. It was started in 1993, funded by government and managed by the Chinese State Education Commission[81]. CERNET is charted to connect all Chinese universities and institutes and all K12 schools. In 1994, China's network (NCFC) was formally accepted to connect with the Internet, a move endorsed by the Sino-American Federation of Science and Technological Cooperation and the National Science Foundation of the United States. Thereafter China is officially recognized as a country with accessibility to the Internet worldwide, to the outside world with a full-function linkage.

In March 1993, Deputy Premier Zhu Rongji proposed the Golden Bridge Project to

---

80 See William Yurcik and Zixiang Tan, "The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China" (1996), ***University of Pittsburgh and Syracuse University***, at http://www.tprc.org/abstract/tan.txt. According to CNNIC, this link was limited to access to American energy network only.

81 See William Yurcik and Zixiang Tan, "The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China" (1996), ***University of Pittsburgh and Syracuse University***, at http://www.tprc.org/abstract/tan.txt. According to CNNIC, CERNET work started in 1994. There are few events dated differently by these two sources partly due to a different interpretation on the start date of an Internet project. The historical dates cited should be read with care.

establish the National Public Economic Information Processing Network. In August of the same year, Premier Li Peng approved the funding of USD 3 millions in supporting the initial construction phase of the Golden Bridge Project. Since then, several more Golden Projects[82] have been introduced gradually and government agencies become key users of the Internet contributing significantly to its development. With the infrastructure in place, China launched a campaign in 1999-2000 for open government policy and E-administration, or E-government on the web.[83]

Between 1994 and 1995, there were many activities going on cultivating an Internet environment and creating new features on web at different sectors. For examples, the country's first set of web pages were introduced in May 1994 by the Institute of High-Energy Physics Research Institute posted on CASNET. China Telecom installed the first two 64K dedicated circuits between U.S. and China, U.S.-Beijing and U.S.-Shanghai, leading to the establishment of CHINANET (China's Internet). The first international conference of an Internet community, Asia-Pacific Networking Group Annual Meeting, was held in China hosted by NCFC, CAS, Peking University and Tsinghua University. In 1995, the first Chinese e-journal CHISACM (Chueng Kong Scholars) was published by the Ministry of Education (State Educational Committee) on CERNET. The Chinese Science and Technology Network (CSTNet) was built to link domestic learning institutions in 24 major cities with the existing college network (CASNET) connected with 30 research institutions in Beijing and the Internet. The first Internet-based bulletin board system (BBS), Shuimu Qinghua was in operations on the China Education and Research Network (CERNET).

In parallel to the vast activities in developing Internet usage and building up the necessary infrastructure, the year of 1996 marks the beginning of China's conscientious

---

82 Some of the Golden Projects are : Golden Agriculture – industrial production information network; Golden Bridge – public economic information processing network; Golden Card – electronic monetary and modern payment system; Golden Customs – foreign trade information sources; Golden Enterprises – management and service information system; Golden Intellectual – education and research computer network; Golden Policy – economic micro-policy making support system; Golden Shield – national and local police agencies network; and Golden Tax – electronic taxation system.

83 Cheng Qi, "1999 Zhongguo Zhengfu Dashangwang (1999 – The Year of E-Government in China)", ***No. 10 Fazhi Yu Jingji (Legal System and Economy)***, 1999.

efforts in an attempt to regulate the Internet and govern the cyberspace using legal means. Apparently, an alarm was triggered in late December 1995 when Guangen Ding, head of the CCP propaganda department found Playboy's web site and several Chinese dissident homepages and protest newsletters.[84] On January 1, 1996, the Xinhua News Agency reported that the government called for a crackdown on the Internet to rid the country of unwanted pornography and detrimental information. The survey statistics presented below will help us understand better the recent trends of Internet development and the potential problems or risks anticipated by the country leaders.

Disparate Growth in the Use of Internet

Over the past few years, the tremendous growth in numbers of Internet users since 1997 is far beyond imagination of the world including IT experts, businessmen, scholars and the Chinese leaders. According to the latest survey report released in January 2002[85] by the China Internet Network Information Center[86] (CNNIC)[87], there was a total of 33.7

---

84 "Surfing Censor." ***Far Eastern Economic Review***, February 8, 1996 cited by William Yurcik and Zixiang Tan, The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China", ***University of Pittsburgh and Syracuse University*** (1996), at http://www.tprc.org/abstracts/tan.txt. (n38).

85 "The Semiannual Survey Report on the Development of China's Internet (January 2002)" published by the China Internet Network Information Center (CNNIC) in January 2002 at http://www.cnnic.net.cn, (Visited on 27-Feb-2002). The prior CNNIC published survey reports were ("Survey Report on Internet Development In China") in November 1997, July 1998, January 1999 and July 1999, January 2000, July 2000, January 2001 and July 2001, January 2002. "Semiannual Survey Report on the Development of China's Internet" (1997 – 2002), ***CNNIC*** at http://www.cnnic.net.cn/develst/repindex-e.shtml (Visited on 27-Feb-2002).

86 China Internet Network Information Center (CNNIC for short) was founded on Jun. 3rd 1997. It is a nonprofit-making organization managed and administered by the Computers Network Information Center of Chinese Academy of Science and led by Ministry of Information Industry, and administratively it is under the leading of Chinese Academy of Science. CNNIC performs the following tasks: Registration Service, i.e. providing domain names registration, IP addresses distribution, autonomous system codes (AS codes for short) distribution, etc; Catalogues Database Service, i.e. setting up national catalogues database and provide information to network consumers, e.g. on IP addresses, domain names, AS codes, etc.; Information Service: compiling statistical data of Internet development in China and provide information on policies and regulations of Internet network in China;

million of Internet users as of Dec 31, 2001 compared to 620 thousands users in October 1997, representing an increase of over 5,300 times in five years.[88] Since CNNIC is an authorized agency by Chinese officials, some parties may challenge the credibility of the survey reports. [89] Albeit, people are in agreement of the rapid growth and the number of

---

Attestation Service of Net Station Visitors Flow, i.e. proposing standard of attestation to record and validate net station visitors flow; Attestation Training: providing Internet technology & application training to the public, e.g. by setting up consumer IT courses for the public. Finally, CNNIC also undertakes national scientific research into matters and issues related to and provides technological consultation service on Internet to the society. See "A Brief Introduction of CNNIC", ***CNNIC***, at http://www.cnnic.net.cn/e-about.shtml (Visited on 27-Feb-2002).

87 In 1997, the State Council's Informatization Office and the China Internet Network Information Center (CNNIC) Working Committee determined that the CNNIC, in cooperation with the four major networks units in China, would carry out surveys on Internet development in China. Statistics on Internet development in China, including the total number of hosts and users, user geographic distribution, traffic pattern, and domain name registration etc. were gathered, reported and analyzed. The data were gathered to assist government agencies and commercial enterprises in making their policy and business decisions. See China Internet Network Information Center (CNNIC) at http://www.cnnic.net.cn/develst/e-index.shtml, (Visited on 27-Feb-2002).

88 The CNNIC surveys and reports remains to be the most authoritative data source upon which PRC government IT police is abided and China bound foreign IT scholars used. See "Survey Report On Internet Development In China", ***CNNIC***, at http://www.cnnic.net.cn, (Visited on 27-Feb-2002).

89 The research methodology and data collection process was not detailed in great length by CNNIC. For example, one finds this as proper description of methodology: "Following the international convention, the statistical work adopts some methods including automatically seeking computers on Internet and online survey, etc. These advanced methods ensure a wide bound of sampling and accurate result. It is the first survey in China Internet and provides accurate report to society." See "Statistical Report of the Development of China Internet (1997.10)", CNNIC at http://www.cnnic.net.cn/develst/9710/e-9710.shtml. Two methods were adopted to collect Internet users data. A multiple methods were used, e.g. automatic online searching, online survey and sampling survey. The sampling survey was used to gather data on Chinese Internet users, i.e. their characteristics and their behaviors in using the Internet. The online survey collects information on Internet usage, users'

Internet users in China representing the largest among nations in the Asia Pacific region. According to the Report, China has 12.54 million computers linked to the Internet with a bandwidth of 7,679.5M. Table 3 provides a summary of the annual growth in the number of Internet user, computer host, ".CN"domain name, "WWW" website, as well as the total bandwidth from year 1997 to 2001. A comparison of year 2001 figures over the same period in 2000 indicates an increase of 49.8% in Internet users, 40.6% increase in computers linked to the Internet, and 174.4% increase in total bandwidth. The number is still increasing rapidly and the growth rate is estimated to be exponential.

Table 3 –CNNIC Statistics on the Development of China's Internet (1997 to 2001)

Year	**2001**	**2000**	**1999**	**1998**	**1997** [90]
Internet User	33,700,000	22,500,000	8,900,000	2,100,000	620,000
Computer Host	12,540,000	8,920,000	3,500,000	747,000	299,000
".CN" Domain Name	127,319	122,099	48,695	18,396	4,066
"WWW" Website	277,100	265,405	15,153	5,300	1,500
Total Bandwidth (M)	7,597.5	2,799	351	143.2	25.4

(Source: CNNIC)

The following growth patterns and development trends of China Internet are observed from the statistics summarized in Table 4 - Profile of Internet Users in China (1997 – 2001).

1. The total number of Internet users marks a quantum leap from a mere 620 thousand in 1997 to 33.7 million in 2001, representing an average growth of 170% per annum. A reducing cost in personal computers, lower rate in accessing the Internet, and a rich content of websites available are major reasons leading to the increase of users. Internet access becoming so easy and popular to the mass public causes a concern to the communist leaders on this open media. More westernized thoughts and culture are available, especially to the educated, from websites overseas. This presents a

---

practices and their views toward some hot issues. The online surveys were posed to many famous domestic Websites and supported by numerous well-known Chinese ISPs and ICPs. In January 2002 online survey, there were 75,383 responses, with 64,627 being valid ones. As to sampling survey, telephone interviews were used. 53,797 samples are available (under the confidence coefficient of 95%, the absolute error of the provincial result is less than 3%) CNNIC http://www.cnnic.net.cn/develst/rep200201-e.shtml (Visited April 22, 2002).

[90] The first survey conducted by CNNIC is as of 31-Oct-1997. Thereafter, surveys are conducted semiannually closing at 30-Jun and 31-Dec of each year with the corresponding report published in July of the same year and January of the following year respectively.

challenge to the one-party ruling position of CPC.

2. Most of the Internet users are youngsters of age 30 and below. The number remains relatively stable at around 70% compared with all users throughout this period. There is a clear tendency that Internet users are becoming younger. The number of users below age 18 surged from only 2.4% in 1999 to 15.3% in 2001. This presents one of the major challenges to the Chinese leaders as the teenagers are typically energetic, with much spare time, curious, fast learners and inexperienced. They are easily led to try on new activity on Internet without knowing that they have broken the law. Juvenile crime statistics indicate that offenders are getting younger in recent years. Between 1997 and 2000, juvenile delinquency of age below 17 represents 5%, 11%, 12% and 12% respectively of total crimes in the year. One of the major contributing factors is due to ignorance in legal knowledge and implication of violations.[91] A study of Internet crimes in Hexi area of Tianjian between January and July, 2001 indicates that 75% of the offenders are below the age of 18.[92] The CPC strongly believes that failure in setting and directing the behavior of this age group will lead to serious social and political problems. Besides, the number of female users increases gradually from 12.3% in 1997 to 40% in 2001. A possible reason is that more female citizens have education opportunity and they are required to use computers at work. This is an emerging area deserves attention from policy makers in China in designing a controlled framework to fight against Internet crime.

3. The education level statistics indicate that the trend is moving gradually towards junior and high school level (67% in 2001) from college graduate level (50% in 1998). Together with the movement in age group described above, it indicates that most of the Internet users are young students with ability to learn and master the technology quickly and at ease.

---

91 For detailed statistics, see Liu Tianfeng, "1991-2000 Woguo Qingshaonian Fanzui De Tedian Yuanyin Yu Yufang Duice (The Characteristics, Causes and Preventive Measures of Juvenile Crime in China Between 1991 and 2000)", ***Qingshaonian Fanzui Yanjiu (Juvenile Crime Research) No. 2, 2002***, pp. 26-32.

92 See study by Rong Huizhen, "Diannao Wangluo – Wei Chengnian Ren Shishi Fanzui De Xin Meijia (Computer Networks – New Media for Juvenile Crime)", ***Qingshaonian Fanzui Wenti, (Juvenile Crime Issues) No. 2, 2002***, pp. 12-15.

Table 4 – Profile of Internet Users in China (1997 – 2001)

Year	2001	2000	1999	1998	1997 [93]
Internet User (Thousand)	33,700	22,500	8,900	2,100	620
1. Gender Ratio:					
Male	60%	69.6%	79%	86%	87.7%
Female	40%	30.4%	21%	14%	12.3%
2. Age Group:					
Below 18	15.3%	14.9%	2.4%	)	)
Age 18 to 24 [94]	36.2%	41.2%	42.8%	) 51.4%	) 41.9%
Age 25 to 30 [95]	16.3%	18.8%	32.8%	27.1%	29%
Age 31 to 35	12.1%	8.9%	10.2%	11.3%	13.2%
Age 36 to 40	8.2%	7.1%	5.7%	4.9%	4.3%
Age 41 to 50	7.6%	5.7%	4.5%	4%	6.8%
Above 50	4.3%	3.4%	1.6%	1.3%	4.8%
3. Education Level[96]**:**					
High School or Below	10.2%	6.4%	3%	6.9%	n/a
Junior College	56.9%	52.4%	45%	34.2%	n/a
College Graduate	30.4%	38.8%	45%	49.6%	n/a
Master & Above	2.5%	2.3%	7%	9.3%	n/a

(Source: CNNIC)

5. The eastern region, southern region and northern region remain to be the top three in terms of geographical distribution of the Internet users during the period.[97] A closer comparison of the figures indicates a trend of Internet popularization from large cities to rural areas gradually over the past five years. The number of Internet users in Beijing, used to representing over one-third of the user population in 1997,

---

93 The first survey conducted by CNNIC is as of 31-Oct-1997. Thereafter, surveys are conducted semiannually closing at 30-Jun and 31-Dec of each year with the corresponding report published in July of the same year and January of the following year respectively.

94 A combined percentage of the age groups from below 15 to 25 for surveys conducted in 1998 and 1997.

95 Statistics represent the age group from 25 to 30 for surveys conducted in 1998 and 1997.

96 Education Level statistics for 1998 are as of 30-Jun. The grouping of year-end figures is not applicable.

97 These regions cover large cities such as Beijing, Shanghai, Guangzhou and Shenzhen. Development in various areas including economics, technology and research are more advanced compared to other parts of China.

dropped significantly to 9.8% only in 2001.[98] Internet development in places like Jilin, Heilongjiang, Jiangsu and Zhejiang are catching up very rapidly. It is obvious that Internet users are gradually spreading across the nation to a more evenly distribution. Tables 5 summarizes the geographical distribution of Internet users between 2001 and 1997. In later discussion, we'll observe that Internet crime and control activity are dispersed in various locations of China.

Table 5 – A Comparison of Geographical Distribution of Internet Users (1997 – 2001)

Geography	2001	2000	1999	1998	1997
Guangdong	10.4%	9.69%	12.94%	20.93%	8.3%
Beijing	9.8%	12.39%	21.24%	23.93%	36%
Shanghai	9.2%	8.97%	11.21%	4.34%	8%
Jiangsu	8%	5.43%	5.91%	5.31%	5.9%
Zhejian	6.6%	6.62%	4.51%	4.63%	3.7%
Sichuan	5.2%	5.03%	3%	3.54%	2.4%
Shangdong	4.3%	5.33%	5.19%	3.65%	4%
Hubei	4.3%	3.52%	3.32%	3.28%	6%
Liaoning	3.8%	4.66%	4.27%	3.64%	2.9%
Fujian	3.6%	3.59%	2.69%	3.07%	2.8%
Hunan	3.4%	3.97%	3.44%	1.69%	1.8%
Henan	3.1%	2.33%	2.11%	2.14%	2.8%
Heilongjian	2.8%	2.46%	1.66%	2.09%	1.4%
Hebei	2.8%	2.47%	2.59%	1.65%	2.5%
Tianjian	2.7%	2.53%	2.68%	1.68%	1.6%
Guangxi	2.6%	2.02%	1.34%	1.96%	1.3%
Anhui	2.5%	2.43%	0.97%	1.4%	2%
Jilin	1.8%	2.41%	1.5%	1.06%	0.9%
Jiangxi	1.8%	2.07%	1.14%	1.66%	0.7%
Chongqing	1.6%	2.03%	1.9%	1.48%	0.7%
Yunnan	1.5%	1.46%	0.63%	0.44%	0.8%
Shaanxi	1.5%	1.47%	1.96%	2.4%	1.2%
Xinjiang	1.3%	1.51%	0.47%	0.65%	0.1%
Gansu	1.3%	1.13%	0.57%	0.58%	0.5%
Shanxi	1.2%	1.34%	1.04%	1.03%	0.6%
Inner Mongolia	1.2%	1.21%	0.5%	0.39%	0.3%
Guizhou	0.6%	0.8%	0.46%	0.49%	0.4%
Hainan	0.5%	0.31%	0.49%	0.52%	0.3%
Ningxia	0.3%	0.48%	0.16%	0.25%	0%
Qinghai	0.2%	0.31%	0.08%	0.1%	0.1%
Tibet	0.1%	0.03%	0.03%	0.02%	0%

(Source: CNNIC)

[98] This is a natural phenomenon as most Internet users at the early stage were on research and located in Beijing. As Internet evolves, more usage is developed in other locations.

4. Table 6 below summarizes key changes of Internet users' behavior from 1998 to 2001 across the country. An analysis of the users' access expenditure indicates that increasing portion of Internet users, 73.7% in 2001, are spending their own expenses on Internet for personal purposes, either for knowledge seeking or leisure, instead of for work. People have more opportunities to access variety of information that used to be under tight control and scrutiny by the government. For example, it is reported in Beijing that nearly 50 percent of all teenage cyber-surfers in 2001 browse the Internet for study purposes, while the other half indulge themselves in online games, chatrooms and even porn websites.[99] Other studies also indicate that 76% of the student surfers spend substantial time chatting on web such as ICQ and bulletin board; 55% indulge in playing online games; 46% visit pornographic websites, and less than 20% of them search for information.[100] The educated are more easily informed with western culture and ideas that may conflict against the CPC ideology. Such a change in the flow of information presents a threat to Chinese leaders.
5. E-commerce is acceptable to more people, from 8.79% in 1998 to 31.6% in 2001. Despite there is an increasing trend of people's willingness to purchase online, security remains to be the most serious concern of potential buyers using the Internet as a purchasing channel. If business entities and individual consumers do not find the Internet secured and their rights being protected by law, they will refuse electronic transactions and consequently E-commerce will slow down. The Chinese government is making efforts in legislation to filling the gap.

Table 6 – Changing of the Internet Users' Behaviors (1998 – 2001)

INTERNET USERS' BEHAVIOR	2001	2000	1999	1998
1. Internet Access Expenditure				
At company expense	10.7%	14.15%	21%	26%
At personal expense	73.7%	63.37%	59%	45%
Both	15.6%	22.48%	20%	29%
2. Most Serious Concerns of Online Business				
Security is uncertain	31.0%	31.20%	36.54%	n/a
Product quality, post-sales service and	30.2%	32.03%	27.64%	n/a

99 "Half Beijing's Teenage Surfers Addicted to Recreational Websites: Officials", ***People's Daily Online*** at http://english.peopledaily.com.cn/200102/11/eng20010211_62072.html. (Visited on April 23, 2002).

100 "80% Teenagers Surf Web for Funs and Chatting", ***Xinhua News Agency (April 23, 2002)*** at http://news.xinhuanet.com/it/2002-04/23/content_370193.htm. (Visited on April 23, 2002).

credibility of the manufacturer are uncertain				
Obstructed delivery channel	13.9%	9.86%	9.26%	n/a
Payment is inconvenient	11.8%	12.59%	17.68%	n/a
Unattractive price	6.3%	7.39%	7.78%	n/a
Information is unreliable	6.3%	5.91%	N/A	n/a
Others	0.5%	1.02%	1.10%	n/a
3. Willingness to Purchase Online				
Yes	31.6%	31.67%	8.79%	n/a
No	68.4%	68.33%	91.21%	n/a

(Source: CNNIC)

Summary

We have observed from above the exponential growth, spread and penetration of Internet in China with data from CNNIC and since 1997. We particular note the concerns raised by such patterns of growth and spread to the PRC political leadership, i.e. political instability to the educated, moral hazard to the youth, and insecurity to commerce. We now turn and focus on how the computer and Internet has been used for criminal purposes, both as a tool and object.

V. NATURE, PREVALENCE AND DISTRIBUTION OF COMPUTER CRIME

The introduction of computer and spread of Internet has boosted economic growth, speeded up social progress, and changed the lifestyle of the Chinese people in untold ways. However, technological advancement has also brought along new social ills and political concerns. Computer and Internet introduce various kinds of computer-mediated criminality and network-related social/political deviance into China. In this section, I will be describing the nature, prevalence and distribution of computer crime, as revealed by China data sources and as understood by the PRC scholars and policy makers.

Computer crime came to China 15 years ago. The first computer related crime in China was officially reported in 1986. The crime was reported as a regular theft since there was no computer crime legislation during that time.[101] The case was uncovered in Shenzhen on July 22, 1986 when a Hong Kong merchant realized that a deposit of RMB20,000 (equivalent to USD2,400) was missing from his bank account.[102] A similar crime was reported at a different branch of the bank two months later. A computer operator of the bank, Chen succeeded in transferring the bank's money to his designated account through unauthorized access to the database.[103] In March, 1988, a minicomputer operator Tse and his gang managed to transfer a sum of RMB870,000 from the Agricultural Bank in Szechuan for their personal use while working on the bank's computers. Between late 1989 and June 1990, another computer operator Fong, a bank employee in Zhejian, was successful in withdrawing RMB1.61 million on cash from the bank deposits accounts by

---

101 There is still an on going and vibrant debate as to whether computer crimes are unique thus deserving of separate legislation or whether computer crimes are generic crimes properly regulated by traditional criminal law. See John Perry Barlow, *A Declaration of the Independence of Cyberspace*, (Davos, Switzerland, 1996); and David R. Johnson and David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, ***48 Stanford Law Review 1367*** (1996).

102 During that period, the average income of a worker was around RMB 200-300, or even less. In relative terms, computer crime resulted in substantial amount of loss to victims and harm to society.

103 Wei Min, "Diannao Shijie De Youling (Phantom of the Computer World)", ***Jingcha Tiandi (The Police Horizon), No. 50-51, 1994***. See also Yu Zhigang and Others, ***Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi*** (Analyzing the Nature of Internet Crime) (Jilin: Jilin Renmin Chubanshe, 2001), p.1.

abusing his access privilege in the course of his duty.[104] So far, the cases recorded were related to individual banking systems.[105]

According to the Supervision Bureau for Public Information Security (Zhongguo Gongan Gonggong Xinxi Wangluo Anquan Jianchaju) of the Ministry of Public Security, China has recorded an increasing number of cybercrime from roughly a hundred cases in 1998 to 4,500 cases in 2001.[106] A yearly breakdown of the figures are summarized in Table 7 below.

Table 7 – Statistics of Cybercrime in China (1998-2001)

---

104 Wei Min, "Diannao Shijie De Youling (Phantom of the Computer World)", ***Jingcha Tiandi (The Police Horizon), No. 50-51, 1994***.

105 In historical context, no one has any money except the bank. More significantly, no one is using computer except the government, particularly the bank.

106 Li Heng, "New Faces of Cybercrimes", ***Renmin Wang (People's Daily Online)*** (April 11,2002), at http://english.peopledaily.com.cn/200204/11/eng20020411_93883.shtml, (Visited on April 12, 2002).

Year	2001	2000	1999 [107]	1998	Total
No. of Cybercrime Cases Under Investigation	4,500	2,700	400	100+	7700+
Annual Growth Rate	67%	575%	300%	--	--

(Source: MPS)

The cybercrime statistics were announced on April 11, 2002 in a working conference of the Supervision Bureau for Public Information Security held in Beijing. In the same event, cybercrime in 2001 was classified into five major categories by an Internet information security official, namely:

1. Using computer to make, copy and spread pornographic materials. Some pornographic CD's and literature are sold on the net for making money. This category accounts for over 50 percent, 2,000 cases odd, of all computer related crime under investigation in 2001.
2. Committing economic crime via the Internet, such as theft, blackmail, illegal pyramid sales activity. These criminal activities are difficult to detect. No further statistics are revealed on this category.

---

107 The number of cybercrime in 1999 (400 cases) quoted here differs from the statistics (700 cases) reported in a research program jointly sponsored by the Zhongguo Renmin Gongan Daixue (Chinese People Public Security University) and Zhongguo Gongan Gonggong Xinxi Wangluo Anquan Jianchaju (Supervision Bureau for Information Security, Ministry of Public Security) published in August 2001. One possible reason is the confusion in the definition and categorization of computer crime in police reporting . In 1999, overall crime statistics were reported under 6 categories where computer crime was not a separate reporting item of the MPS. However, the discrepancy is negligible in comparison to the drastic increase to 2,700 cases in 2000. For police report categorization, see MPS Internal Criminal Statistic Compilation, ***Gongan Neiqin Gongzuo Shouce (Police Administrative Manual)***, (Beijing: Jingquan Jiaoyu Chubanshe, 1994), p. 409. See also ***Zhongguo Gongan Baike Quanshu (Chinese Public Security Encyclopedia)***, (Changchun: Jilin Chubanshe, 1989), pp. 524-525. For more descriptions on the current status of cybercrime in China, see Li Wenyan and Others, ***Jisuanji Fanzui Yanjiu*** (Computer Crime Research) (Beijing: Zhongguo Fangzheng Chubanshe, 2001), pp. 41-44. See also Jiang Ping, ***Jisuanji Fanzui Wenti Yanjiu*** (Research into Computer Crime Problems) (Beijing: Commercial Press, 2000), pp. 152-153.

3. Sharp increase in computer virus and hacker attacks jeopardizing information system and network security including network of some governments and institutes. It is reported that 600 cases have been uncovered in 2001, representing a rise of 58% over the previous year.
4. Infringement upon citizens' personal rights and democratic right, such as personal attack and libel through the Internet. In 2001, 186 cases investigated were criminal offenses, representing a rise of more than three times over previous year.
5. More and bigger cases using Internet to jeopardize national security such as Falungong and national splittist spreading messages in attacking CPC and Chinese government.

The above official statistics do not provide a complete picture of the current status of Internet crime in China. However, it informs us that, from the perspective of the police authority and with limited data, pornography is considered the top crime problem, followed by economic crime and national security breaches. Together, they contribute to 38% of the Internet crime. The official media of the police, the China Police Report, has designed its section, Jingti: Wangluo Xianjing (Warning : Internet Trap), to counteract the rising trend in Internet criminality. A detail examination of the Internet crime stories posted in this corner from January 2001 to March 2002 shows 44 computer crime cases reported. Obviously not all computer cases are made known to the public. Still, there is a lack of official data for an adequate research of computer crime in China. Having said that, we are able to reference a few research conducted before 2000, among them Jiang Ping's study is one of the most comprehensive one in China.

Jiang[108] had collected 185 typical cases of computer related crimes between 1986 and

---

108 Jiang Ping, now one of the very few computer crime and control experts in China, pioneered the first 'scientific" study of computer crime in China. The Ph.D. project, now in book form, provides us with a systematically gathered data set on computer crime, anywhere in China in that point of time and even now. The Jiang's data, valuable though it obviously is in providing us with a rare glimpse into the nature, prevalence and distribution of computer crimes in China, however suffers from a number of methodological problems, which detracts from its potential scientific use. First, the data, collected in 1996-1999 became dated. Second, the cases were collected from newspapers, hardly a reliable source of information. Particularly, computer crimes are first reported to the police before public release. The police report crime only when it serves their purpose, e.g. educational reasons.

June 1999 of which 183 cases had recorded a known environment in committing the crime[109]. His analysis on the 183 cases is listed in the Table 8 below. The figures show that 169 cases, representing over 90% of the Jiang's total study, were computer crime committed over the network.

Table 8 – Jiang's Analysis of the 183 Cases in Computer Crime (1989 and 1999)

Commission Environment	Standalone Computer	Intranet	Extranet	Internet
No. of Crime	14	123	8	38
Percentage of 183 Cases	7.65%	67.21%	4.37%	20.77%

(Source: Jiang Ping, *Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)*)

In his research into computer crime problems, Jiang has grouped the 185 crime cases into four major categories, namely pornography on web, computer virus, financial frauds using credit card, and hacking of the information network. Some of the sample cases described by Jiang are listed as follows[110].

Table 9: Samples Cases of Computer Crime and Classification

Classification	Brief Descriptions of the Computer Crime Case
Pornography on Web	1. On 2 March 1995, the Public Security of Tianjin investigated the first pornographic crime committed by Li who used computer to replicate, sell and propagate obscene software to the consumers. 2. On 25 March 1995, the Public Security of Tianjin arrested a gang of 12 people who sourced obscene software from Beijing and Sichuan and sold to 27 provinces and cities across the nation. 3. In June 1995, the Public Security of Henan Province launched a campaign against pornography and detained 1,012 copies of obscene optical disks and 3,298 copies of obscene software. There were 35 people arrested and punished. In a city, 24 out of 80 computer firms were involved with issues in pornography and drugs. 4. In July 1995, the Public Security of Nanjing arrested Gao, a major supplier of

---

Third, the newspapers do not offer rich and particular details for the proper classification of the cases. Fourth, the limited number of 185 cases collected, over a long period and within a large population, is not adequate to show an emerging pattern, much less support any theoretical framework. Jiang's data should be cited with caveat and used carefully.

109 Jiang Ping, ***Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)*** (Beijing: Commercial Press, 2000), p.79.

110 See Jiang Ping, ***Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)*** (Beijing: Commercial Press, 2000), pp.138-149.

	computer pornographics to Nanjing students of high schools, colleges and universities. 5. In April 1996, a company in Zhangsu replicated pornographic optical disks and leased them to consumers in making a profit. 6. In May 1997, a computer company in Nanjing provided pornographic software in servicing their computer games to customers. 7. On 25 Feb, 1998, the Public Security of Beijing investigated an internet site that had downloaded 70+ obscene photos and 14 e-magazines.
Computer Virus	8. In 1992, a high school student modified the virus "1575" to produce a more powerful virus. The student was referred to the school authority for re-education in absence of an appropriate law and regulation. 9. In Nov. 1996, a self-virus "Tel 2815" in Zhangsu destroyed the data in electricity loading of a power supply plant. It also contaminated a personnel software of an electricity plant destroying data in wages and personnel records. 10. In 1999, China computers were attacked by viruses Maleesa and CIH propagated from outside networks. 11. In 2000, China computers were attacked by the virus "I Love You" propagated from outside networks.
Financial Frauds using Credit Card	12. In July 1995, Li and Wen from HeilongZhang used their credit card to overdraw over RMB10,000, with each transaction below RMB500, in various locations including Jinang, Tsingtao, Shanghai, Hangzhou, Ningbo, etc. 13. In Dec. 1998, the credit card section of a bank noticed that there were abnormal transactions processed for 3 closed accounts and reported the case to the Public Security. After investigation, it was discovered that Sun, a program developer of the bank succeeded to plant a decryption program in the computer main frame to by-pass the password verification. Then, Sun produced a fake card for himself to draw cash from the closed or active accounts through ATM machines or remote access. Sun managed to draw a cash total of over RMB100,000 using this sophisticated computer skills. 14. In 1996, an employee in a bank, Zhu changed the transaction date in the computer record for her boyfriend Chen so that it appeared that he was using his credit card before the spending limit was over. Both had deceived a total of RMB87,000 using a credit card with RMB200 deposit only.
Hacking Information Network	15. In Oct. 1998, Zhou and his brother were arrested for hacking into the information network of a bank in Guangxi and drawing money illegally from the bank. Zhou was a system administrator of the bank. 16. In Feb. 1998, an information service provider (ISP) in Guangzhou lost access control twice for a 4-hours duration each in managing the network. Out of curiosity and show-off, Lu and Yuan intruded the network changing the password of the system server, thus took a complete control of the entire network. 17. In Sep.1998, a library system in a province was attacked by hackers. The homepage was unlawfully altered and the hyperlinks to other sites were also re-directed randomly. Such an intrusion had forced the library website to close down for 6 days.

(Source: Jiang Ping, *Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)*)

Despite a criticism on the small sampling size of Jiang's empirical data, the above sample cases do provide us a sense of the nature of cybercrime in China up to June 1999. Jiang further summarized his findings[111] from the 185 cases as follows.

1. Most of the victims were reported in the finance sector. 54.05% of the cybercrime cases is related to the financial systems. Business enterprises fall into the second position that has a share of 32.97%.[112] This slightly differs from the criminal trend in 2001 when there is a leap jump of individual Internet users for personal purposes. More cases are uncovered and reported by MPS with more focus on the subject.
2. Majority of the principal offenders are educated youngsters with an occupation as computer operator (59.85%), system administrator (31.39%), or program developer (3.65%). The remaining balance of 5.11% is identified as students. Most of the accomplices are students (52.38%) or computer operators (38.10%). While most cases were reported in financial sector, the offenders were primarily insiders who had access to the computer network and corporate information to enable them making the offense.
3. Majority of the principal offenders are university graduates (40.42%). College students and post-graduate students contribute to 19.15% and 10.64% respectively. Only 29.79% of the total have completed high school education level or below. This appears logical as the criminality requires a sophisticated knowledge in computing and mastering of technical know-how.
4. Only 117 cases have the gender information where 91.45% of the principal offenders are male and 8.55% are female. However, it is observed from the news clippings today that female offenders have obviously increased substantially. Part of the reasons being a larger population of female Internet users, increased from 12.3% in 1997 to 40% in 2001.

---

111 See Jiang Ping, ***Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)*** (Beijing: Commercial Press, 2000), pp.150-152.

112 There are sociological, technological, and structural reasons why financial crime remains to be in the financial sector. First, socially, China is still a less developed country with many more people living at subsistent level. This provide many "motivated" offender. (Felson). Second, technologically, computer offers an easy to steal and secretive way to hide. Third, structurally, financial loss in public institutions (banking) cannot be hidden.

Computer Crime in Context of the Criminal Law in China

Many legal scholars and professionals in China have taken a different perspective in analyzing the nature of computer crime. For examples, Yu Zhigang, PhD of Zhongguo Jingfa Daxue (University of Political Science and Law) and Li Wenguang, an official of the Supreme Peoples' Court, have adopted the Criminal Law (1997) as a framework in the analysis of cybercrime, a framework very commonly used. They have presented the crime cases and legal discussions in their book[113] according to the structure of the Part Two, Specific Provisions, of the Criminal Law (1997).

Criminal Law Chapter	Descriptions	Sample Case of Computer Crime
I	Crimes of Endangering National Security	Chen was a Taiwanese who worked for his uncle as factory manager in an eastern coastal region of China. After rejection of his application to open a branch by the local authority in 1999, he downloaded illegal materials from Internet on hostile attacks to China, dismemberment of Taiwan, Inner Mongolia and Tibet, plot to subvert the government and overthrow the socialist system. He built his personal web page with such materials for free access by the public and went further to send these materials via email to mass media inside and outside China. He was later caught and prosecuted for committing crime endangering state security. (p. 97)
II	Crimes of Endangering Public Security	Liu was a worker in a train station. He hated his management due to disagreement in job evaluation and housing allocation. Instead of working in the station, he went to Internet bar chatting via Internet for most of his time in a day. One day, he met with a guy during chatting in the Internet who also expressed his discontent towards the station management. Both subsequently planned for a plot on train accident with details on time, location, and escape route agreed. Fortunately, the plot was uncovered in the Internet by another user who reported the case to public security authority. Both Liu and the guy was caught and prosecuted for committing crime endangering public security. (p. 137)
III	Crimes of Disrupting the Order of the Socialist Market Economy	Huanyu was a company manufacturing and selling racket and shuttlecock for badminton with a majority market share in a city. Lisheng was a newly formed company also engaged in manufacturing and selling of similar products with its own brandname. The competition between these companies in the market was fierce but Lisheng was able to capture a large share of market from Huanyu. In order to regain the market share, Huanyu disseminated false information in the Internet accusing that the quality and reliability of Lisheng's products were bad. Though Huanyu was subsequently improved in market share, it was caught and prosecuted by public security authority. (p. 196)
IV	Crimes of Infringing Upon Citizen's Right of the Person and Democratic Rights	Due to late attendance and bad discipline records, Zhu lost his bonus of 1,000 yuan in May 1998. He decided to take revenge by accusing his manager committing corruption and sent email to Public Security Bureau, Procuratorate, and Anti-corruption Bureau. He made up a story saying that the manager received

113 Yu Zhigang and Others, ***Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime)*** (Jilin: Jilin Renmin Chubanshe, 2001)

		100,000 yuan as bribe in the construction of factory building. As a result, the manager was ordered to suspend his duty for investigation. Zhu later was prosecuted and charged with crime of calumny. (p. 292)
V	Crimes of Property Violation	Yang was a staff of a stated-owned enterprise, which has successfully completed a research on a new product and planned for market launch in 1998. All critical information about the research and the new product was stored in the computer system of the company. In order to blackmail the enterprise for money, Yang planned to stole the information via Internet. He connected the company's computer system to the Internet and successfully make access to it via remote connect from his personal computer at home. (p. 365)
VI	Crimes of Obstructing the Administration of Public Order	Both He and Yang are unemployed in a city of Henan. They built their own webpages with an expectation of generating revenue from advertisement. In order to raise the hit rate, they downloaded a large number of pornographic materials and pictures onto their webpages from free websites overseas. (p. 406)
VII	Crimes of Impairing the Interests of National Defense	In 1996, a research officer of a Computer Research Institute in Guangzhou was found guilty of copying a highly confidential material from the computer of a national security system. He worked as a spy for a foreign government and accessed illegally to the security system with his expertise and skills in computer and network. (p. 416)
VIII	Crimes of Embezzlement and Bribery	Wang was a finance officer in a bank and held the password in accessing the computer system as required by his job. In November 1996, he illegally transferred a sum of RMB200,000 from the bank to an account opened by him via remote connect in the Internet with his personal computer at home. (p. 450)
IX	Crimes of Dereliction of Duty	Chang worked in the government of a city responsible for managing document filing. Chang had a good friend who planned to reproduce a bibliography of a leader in a foreign country. The leader had stayed in the city for quite some time in the past and a file was kept in the government filing system. Chang rejected his friend's request to access the file as it was classified confidential. One day, Chang discovered that there was hacking in the computer system on the documents. He later found that the hacker was actually his friend. Not knowing what to do, he did not take action to protect the system from hacking. As a result, the file was copied and reproduced in the bibliography published by his friend. Chang was charged guilty of dereliction of duty. (p. 480)
X	Crimes of Servicemen's Transgression of Duties	nil

(Source: Yu Zhigang) [114]

[114] Yu Zhigang and Others, ***Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime)*** (Jilin: Jilin Renmin Chubanshe, 2001)

VI. CYBERSPACE GOVERNANCE IN CHINA

China Policy Towards Cyberspace Governance and Internet Regulations

To the Chinese government and CCP leaders, the Internet is to be used primarily for the facilitation of economic reform, social development and cultural revival. As a matter of state policy endorsed by the Fifth Session of the Fifteenth CCP Central Committee meeting, the net is to be tightly controlled and strictly regulated to forestall against any inappropriate and non-approved use of the Internet.[115] On July 12, 2001, the CPC Central Committee held a special meeting at Zhongnanhai to discuss policy issues pertaining to cyberspace governance and Internet control.[116] At the meeting, President Jiang Zeming outlined the policy postures of NPC: active promotion of the net with due regard to containing its side effects and addressing its problems and shortcomings, e.g. spread of pornography.[117] The priorities on hand are: (1) perfect regulation and control of Internet

---

115 Jiang Zeming: Use law to protect and promote the healthy development of the internet. ("Jiang Zeming: yunyong falu shouduian baozhang chujing xingxi wangluo jiankan fazhang") China Police Daily Online. July 12, 2001. http://www.cpd.com.cn/xxlr.asp?menulb=019%D4%DA%CF%DF%D0%C2%CE%C5&id=2465

116 The legal system – policy meeting was attended by CPC Political Bureau members: Jiang Zemin, Li Peng, Zhu Rongji, Hu Jintao, Li Ruihuan, and Wei Jianxing. The meeting was chaired by Cheng Chengxi, a researcher in the Law School of the Chinese Social Science Academy (CSSA). Cheng instructed and discussed with the political bureau leadership on three aspects of cyberspace governance and control, i.e. the importance of Internet development and the corresponding need for regulation and control; cyberspace governance and Internet regulation in foreign counties; and Internet legal system establishment situation in China.

117 See "Wangluo saohuang fuhuan falu zijian" (Purging pornographic materials from the need, calling upon the sword of the law), ***China Police Daily Online*** (February 8, 2001), at http://www.cpd.com.cn/xxlr.asp?menulb=039%C8%CB%C3%F1%B9%AB%B0%B2%B1%A8&id=12058 (31 years old Yang Linhua used the internet to set up "Chinese call girls" web where he earned 35,000 in six months.) In order to promote health, ethical and moral use of Internet, the CPC organized a host of activities through the China Communist Youth League (Gongqingtuan or gongchanzhuyi qingniantuan), e.g. issuing the "National youth civilized (use of) Internet Pact" (Quanguo qingxiaonian wangluo wenming gongyue). See also "Qingshanian yaoliao wangluo xingwei daode guifan" (Internet young people have ethical conduct norms), ***China Police daily Online*** (November 30, 2001), at

through legislation; (2) promote civilized and cultural (wenming) use of Internet[118]; (3) enhance and participate in international cooperation in Internet control; (4) actively promote training and education of party leaders and government offices to computer use and Internet. So far, Jiang's statement in this policy meeting is the most important and representative of the China's official line towards cyberspace governance.

Judging from the above events and policy initiative emulating from the CPC and PRC government since then, political leaders and government officials in China is well aware of the potentiality for good and evil of the Internet in China's reform process.

On one hand, Internet technology is a power tool to spur China's economy into new height, if not changed direction, with ever faster speed, greater efficiency, and cost-effectiveness. According to Zeng Peiyan, the minister-in-charge of the State Development Planning Commission, one of the major targets for national economic and social development in 2002 is to attain an economic growth rate around 7 percent. IT is going help China to achieve that goal, by maintaining a competitive edge in the global economy; especially given a slowdown in the more matured industry. Thus, China government will make strong efforts in integrating information technology into the national economy and society. For instances, E-government will be introduced, a policy framework for e-commerce will be formulated, e-commerce certification systems development, and "no time should be lost in developing information security systems".[119]
On a pragmatic front, slow growing economy will easily lead to social and political instability.

On the other hand, Internet changes the availability and substance of information in the community and to the people. In the past, the CPC and PRC government have dominated over all mass communication channels and a total control over public information distribution in China. With the advent of Internet, the CPC and PRC government find it

---

http://www.cpd.com.cn/xxlr.asp?menulb=039%C8%CB%C3%F1%B9%AB%B0%B2%B1%A8&id=8295.

118 Akin to development of ethical culture with the Internet users and community.

119 Zeng Peiyan, "Report on the National Economic and Social Development Plan, the Fifth Session of the Ninth National People's Congress, PRC, March 6, 2002", ***Xinhua News Agency Online*** (March 17, 2002), at http://news.xinhuanet.com/english/2002-03/17/content_320000.htm (Visited on March 18, 2002).

increasingly difficult, if not impossible, to control people's access to information, e.g. by way of CMC.[120] Internet has totally transformed the means, contents and patterns of communication in China. More diversified opinions on the web, some of those may be contradictory to the CPC's views and socialist ideology, are disseminated easily and quickly through this open media. It presents a challenge, or even a threat to a certain extent, to the monolithic and centralized government. From a political point of view, obviously there is a strong reason for China to adopt active measures in regulating the uncontrolled information made available in the cyberspace.

In a government work report delivered by Premier Zhu at the Ninth National People's Congress, the overall mission in maintaining national security and social stability is clearly stated. "It is of vital importance to ensure national security and social stability in the new circumstances. We must take strict precautions against and firmly crack down on, according to law, sabotage by hostile forces both inside and outside China, and we must crack down on criminal activities perpetrated by forces of terrorism, religious extremism and ethnic separatism. We must continue to fight Falungong and other cults. … Under the principle of combining action with prevention …, we must implement measures for the all-round improvement of social order, … establish a prevention and control system for public security …".[121]

Felson's Routine Activity Theory and Comprehensive Control in China

In attempting to control cybercrime and regulate Internet, China adopts a scheme of comprehensive control (zonghe zhili) - a crime control and prevention model developed by contemporary Chinese leaders under an influence of the 'opportunity model' or 'routine activity model' by Marcus Felson and his associates (Cohen and Felson 1979; Cohen, Felson, and Land 1980; Felson 1983; Felson 1987; Felson 1992);[122] heritage of

---

120 June 4 and Falungong are two great examples. In both cases, in spite of PRC government expressed intent and avowed efforts, news about student uprising and messages of FLG spread like wild-fire.

121 Premier Zhu Rongi, "Government Work Report, the Fifth Session of the Ninth National People's Congress, PRC, March 5, 2002", ***Xinhua News Agency Online*** (March 16, 2002), at http://news.xinhuanet.com/english/2002-03/16/content_319108.htm (Visited on March 18, 2002).

122 China is leaning towards Felson in two aspects. First, some scholars have come up with a China-Felson Theory. Second, the principles underscoring the Felson and PRC approach

ancient Chinese philosophy and culture in moral and ethics; Marxian sociology and ideology in overall social responsibility and social reform; and CPC's pragmatic experience in applying their political doctrines and socialist market economy to the country's unique situations (guo qing) as well. Felson argues that "predatory crime incidents depend on the physical convergence of these three elements: a likely offender, a suitable target, and the absence of capable guardians".[123] Felson's routine activity theory is immensely popular among researchers and police agencies.[124]

Comprehensive control in China is an integrated scheme of crime control with prevention as the core. Other crime control measures are built around prevention with education as a key component, followed by co-operations from local communities. The scheme has similarities of "Problem Oriented" policing that treats crime as integrated social and economical problem, more so than only a legal one to be reacted to by police and punished with law. The policy of comprehensive approach for crime control and prevention in China could be traced in a document that was published 10 years ago, the *Decision of the Standing Committee of the National People's Congress Regarding Comprehensive Control in Social Order and Security*, issued by the NPC Standing Committee on March 2, 1991, for the purpose of creating a safe and orderly environment facilitating execution of the 10-year development plan on state economy.[125] It provides comprehensive control guidelines for maintaining social order, public safety and country stability; ensuring a smooth progress of social reform and openness, and socialist modernization and construction. On September 5, 2001, the Central Committee of the CPC and the State Council reiterated the importance of this policy and called for greater efforts in improving public security through the approach of comprehensive control.[126]

---

are basically similar.

123 Marcus Felson, ***Crime and Everyday Life – Insight and Implications for Society*** (Pine Forge Press, 1994), p. 30. See also Ronald V. Clarke and Marcus Felson, "Introduction: Criminology, Routine Activity, and Rational Choice", ***Routine Activity and Rational Choice, Advances in Criminological Theory, Volume 5*** (Transaction Publishers, 1993), pp. 1-14.

124 See Li Wenyan and Others, ***Jisuanji Fanzui Yanjiu (Computer Crime Research)*** (Beijing: Zhongguo Fangzheng Chubanshe, 2001), pp. 5-6.

125 Since then, there is a national conference in 2001 to report the state and accomplishments of comprehensive control in 10 years since 1991.

126 See "Opinion on Further Improving Social Order Through a Comprehensive Approach",

There are key messages highlighted in the document that reflect the influence of Felson's routine activity theory.

1. "To vigorously develop crime prevention networks at the grassroots level in parallel to law enforcement with harsh punishment while keeping crime prevention in a primary role. Education in moral and legislation to the youth is emphasized." – This statement aims at reducing the number of motivated offenders in view of the high percentage of Internet users being teenagers.
2. "To strengthen the crime prevention infrastructure and extend comprehensive control to different hierarchies, from cities, rural areas, to street-levels." – This statement aims to reduce the crime opportunity through environmental design.
3. "To reinforce a total scheme of comprehensive control in communities, coordinate efforts in crime fighting, crime prevention, and crime control by local authorities with appropriate provision in rules and regulations." – This statement aims to cultivate a group behavior in crime prevention, and possibly enable the presence of guardians, more and easily available such as operating a safe Internet bar in neighborhood.
4. "To hold responsible bodies strictly accountable to ensure effectiveness of comprehensive control in maintaining social order and public security." – This statement aims to ensure a controlled Internet in operation under the radar, reduced crime level but within tolerance of the Chinese leaders in terms of information contents and information flow.

The above directives inform that Chinese leaders are very serious in deploying a comprehensive scheme to regulate the Internet as they realize a growing trend of Internet crime and malevolent contents on the web threatening the innocent youth, CPC socialist ideology, state security and social order. In terms of applying comprehensive control to cybercrime, emphasis is put on educating the youngsters civilized use of Internet, providing legal awareness training, and providing guardianship. Recently, a teleconference was jointly held by eight government agencies, including the Ministry of Public Security, Ministry of Education, Ministry of Information Industry, and Ministry of State Security, etc. A nation-wide program was under plan to regulate and control the Internet, keeping it clean from malevolent information. The importance of a comprehensive approach for this special program was reiterated. Meeting participants

---

People's Daily Online (November 19, 2001), at http://www.people.com.cn/GB/shizheng/16/20011119/607800.html. (Visited on April 30, 2002).

are urged for quick and serious implementation.[127]

Internet-related crimes in China are currently dealt with in accordance with administrative regulations on computer security and information network safety, and provisions in the criminal law. In the following section, I'll discuss on how China government builds up a comprehensive crime control and prevention program in cyberspace with various means: legislation for legal framework, education for prevention, management control for deterrence, and technology for structural control.

Legislation

The Criminal Law[128], revised and enacted on October 1, 1997, contains no clear definitions of Internet crimes. In this revision, there are only three provisions, Articles 285 to 287, specifically relevant to computer related crime under Chapter VI. They are:

Article 285 Whoever, in violation of State regulations, invades the computer information system in the fields of State affairs, national defence construction or sophisticated science and technology shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention.

Article 286 Whoever, in violation of State regulations, cancels, alters, increases or jams the functions of the computer information system, thereby making it impossible for the system to operate normally, if the consequences are serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention; if the

---

127 Participants of the teleconference include officials from the Ministry of Public Security, Ministry of Education, Ministry of State Security, Ministry of Information Industry, Ministry of Culture, State Administration for Industry and Commerce, Information Office of the State Council, State Bureau of Secrecy. See "Eight Ministries Joint Conference on Special Program to Keep the Internet Clean from Malevolent Information", ***Xinhua News Agency Online*** (May 1, 2002), at http://news.xinhuanet.com/nescenter/2002-05/01/content_379468.htm. (Visited on May 4, 2002)

128 The *Criminal Law* of the PRC (Adopted at the Second Session of the Fifth National People's Congress on July 1, 1979, revised at the Fifth Session of the Eighth NPC on March 14, 1997, promulgated by Order No. 83 of the President of the PRC on March 14, 1997, and shall enter into force as of October 1, 1997). See ***Zhonghua Renmin Gongheguo Fadian (Laws of the People's Republic of China, Chinese-English Edition)*** (Jilin: Jilin Renmin Chubanshe, 2000).

consequences are especially serious, he shall be sentenced to fixed term imprisonment of not less than five years. Whoever, in violation of State regulations, cancels, alters or increases the data stored in or handled or transmitted by the computer information system or its application program, if the consequences are serious, shall be punished in accordance with the provisions on the preceding paragraph. Whoever intentionally creates or spreads destructive programs such as the computer viruses, thus affecting the normal operation of the computer system, if the consequences are serious, shall be punished in accordance with the provisions of the first paragraph.

Articles 287 Whoever uses computers to commit the crimes such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of State secrets shall be convicted and punished in accordance with the relevant provision of this Law.

It is obvious to note that the above three Articles provide legal basis to punish only those who invade the computer systems connected with State affairs, national defence, advanced technology and computer information. The *Criminal Law* has no article protecting the rights of individual surfers or financial and commercial networks. Similar to other traditional crimes, like theft and defamation, illegal acts performed over the web in private sectors have to be judged and prosecuted in accordance with existing legislations without an appropriate reference to the specific characteristics of Internet crime.

Regulative Measures

Before and after the *Criminal Law* is revised in 1997, lawmakers have established other administrative regulations in response to the dynamic development of cybercrime specifically. For example, the Ministry of Public Security issued a notice, on April 5, 1995 calling for an action to curb criminal activities in using computers to duplicate, spread and sell pornographic materials. In general, the administrative regulations on computer security and information network safety are grouped in three major categories: network monitoring and control, network information system security, and domain name registration. Together with the *Criminal Law*, these regulations provide a framework for the China government to control the information flow of the Internet, keep track the Internet users, lay responsibilities on Internet service providers in the control process, empower Internet policing and law enforcement, and provide legislations for punishing criminals. In the forthcoming discussion, I'll introduce some of the regulations for network monitoring and control, network information system security, domain name

registration, and protection of intellectual property and facilitation of E-commerce.

1. **Regulations on computer network monitoring and control.** The legal foundation of China Internet is stated in China's State Council Order 195, "*Provisional Regulations of the PRC for the Administration of International Networking of Computer Information Networks*", issued by the State Council on February 1, 1996 and amended on May 20, 1997. Apparently, an alarm was set in late December 1995 when Guangen Ding, head of the CCP propaganda department found Playboy's web site and several Chinese dissident homepages and protest newsletters.[129] On January 1, 1996, the Xinhua News Agency reported that the government called for a crackdown on the Internet to raid the country of unwanted pornography and detrimental information. It follows that all Internet users are required to register with the Ministry of Public Security (MPS) within 30 days, and report subsequent changes if they cancel their accounts or switch accounts to a different information service provider (ISP). The year of 1996 marks China's conscientious efforts in an attempt to regulate the Internet and govern the cyberspace using legal means while the Internet Content Regulation issued in 2000 seals another landmark regulating the IT industry. The new regulation requires Internet content providers (ICPs) to keep 60-day records of user activities online for necessary inspections by related government administrations, including user's log-on time, Internet account, web address and other information. "The ICPs are prohibited from providing information related to anti-government, obscenity and anti-social stability, and intruders will be punished according to the actual situations," states the ruling.[130]

   In brief, this category of regulations control the information flow, track Internet users, and cast monitoring responsibilities on Internet service providers. Some of the other major regulations under this category include:

   - *Measures for the Administration of the Entering and Exiting Channels for*

---

129 "Surfing Censor", ***Far Eastern Economic Review***, February 8, 1996 cited by William Yurcik and Zixiang Tan, The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China", ***University of Pittsburgh and Syracuse University*** (1996), at http://www.tprc.org/abstracts/tan.txt. n38.

130 "IT Sector Hails New Regulations", China Daily (10/15/2000) at http://search.chinadaily.com.cn/isearch/i_textinfo.exe?dbname=cndy_printedition&listid=12441&selectword=IT%20SECTOR%20HAILS%20NEW%20REGULATIONS

International Networking of Computer Information Networks (Issued by the Ministry of Post and Telecommunications on April 9, 1996);

- *Interim Provisions on the Interconnection of Designated Networks with Public Networks* (Issued by the Ministry of Post and Communications on July 24, 1996);
- *Interim Measures for the Administration of Quality Certification for Entering the Network of the Communications Equipment Imported for Official Use* (Issued by the Ministry of Post and Communications on January 14, 1997);
- *Implementing Measures for the Provisional Regulations of the PRC for the Administration of International Networking of Computer Information Networks* (Issued by the Information Task Force of the State Council on February 13, 1998);

2. **Regulations on network information system security.** The *"Safety and Protection Regulations for Computer Information System*", announced on February 18, 1994, was the first official regulation on computer security dictating individual organizations to create their own procedures to implement computer protection, such as access controls and administrative controls. It was issued even before Internet access was feasibly available to most Chinese people. In 2000, a host of key regulations gearing for state security on web and Internet security become available, for examples: the "*Regulations on State Secrets Administration for International Networking of Computer Information Systems*", (issued by the State Bureau of Secrecy and enforced on January 1, 2000), and the "*Decision of the Standing Committee of the National People's Congress Concerning Maintaining Internet Security*", (adopted on December 28, 2000).

   The State Secret Regulations were promulgated to ensure security for state secrets and strengthen secrets administration for international networking of computer information systems. They were promulgated on the basis of the *Law of the People's Republic of China on the Preservation of State Secrets* and relevant laws and regulations. *The Internet Security Decision* lists numerous acts that may be committed involving computer systems and the Internet and provides that if such acts "constitute a crime" criminal liability will be investigated and dealt with in accordance with the relevant provisions in the *Criminal Law*. For example, one of the acts listed is using the Internet to incite racial hatred. If such an act is committed and if the act constitutes a crime, criminal liability will be investigated and dealt with in accordance with the *Criminal Law*. If the Internet is used to commit an illegal act that

contravenes public order administration but does not constitute a crime, the public security authorities will impose penalties in accordance with the *Regulations on Public Order Administration Penalties*. If an act does not constitute a crime but other laws or administrative regulations are violated, the relevant administrative authorities will impose administrative penalties in accordance with the law. If a party uses the Internet to infringe the lawful rights and interests of others and the acts constitute infringement of a civil nature, that party shall bear civil liability. In April 3, 2001, the *Measures for Managing Business Operations in Providing Internet Services* was jointly issued by the Ministry of Information Industry, Ministry of Public Security, Ministry of Culture, and General Administration of Industry and Commerce, to prohibit the service providers and Internet users from any illegal behavior jeopardizing computer network security and information security.

In brief, this category of regulations is very instrumental in addressing a wide spectrum of issues related to system security, from state secrets, encryption, hackers, to computer viruses attacking an information system. These legal tools also allow tracking of Internet users in case any criminal activity is detected and it also addresses system security issues such as computer viruses and hacking. Some of the other major regulations are:

- *Regulations of the PRC for the Safety and Protection of Computer Information System* (Issued by the State Council on February 18, 1994);
- *Notice of the Ministry of Public Security on the Recordation of Computer Information Networks Connected with International Networking* (Issued by the Ministry of Public Security on January 29, 1996);
- *Notice on Strengthening the Administration of the Information Security in the International Networking of Information Networks* (Issued by the Ministry of Public Security on July 1, 1996);
- *Measures for the Protection of Security and Administration of International Connection of Computer Information Networks* (Issued by the Ministry of Public Security on December 16, 1997);
- *Interim Provisions on the Administration of Protection of Secrecy for the Computer Information Networks* (Issued by the State Secrecy Bureau on February 26, 1998);
- *Interim Provisions on the Safety Protection Work for the Computer Information Networks of Financial Institutions* (Issued by the Ministry of Public Security and the People's Bank of China on August 31, 1998);

- *Measures for the Prevention and Control of Computer Viruses* (Issued by the Ministry of Public Security on April 26, 2000);

3. **Regulations on registration of domain name.** Throughout the 1970s and 1980s, the network expanded as technology became more sophisticated. In 1984, the Domain Name System (DNS) was introduced, giving the world domain suffixes, such as .edu, .com, .gov and .org, and a series of country codes. This system made the Internet much more manageable. Without it, users had to remember the Internet Protocol (IP) address - a long series of numbers - of every Internet site they wanted to visit instead of a string of words.[131] CNNIC is the only authorized body to provide services related to the registration of domain names in China. In an effort to hammer out a sound environment for Chinese character domain names, the Ministry of Information Industry (MII) released a new regulation in late 2000 regulating the Chinese domain name registration. Without approval from the Telecom Administrative Bureau of the MII approval, no organizations or individuals can become involved in the businesses related to domain name registration, related services or agent registration.[132] This category of regulations serves as an important mechanism for censorship of Internet website operators: to restrict creation of new websites and keep track who are the information content providers of a website. Other major regulations under this category include:

- *Provisional Administrative Measures on Registration of China Internet Domain Names* (Issued by the State Council Information Leading Group on May 30, 1997);
- *Implementing Measures on Registration of China Internet Domain Names* (Issued by the State Council Information Leading Group on June 3, 1997).

4. **Protection of intellectual property and facilitation of E-commerce.** China has joined the major international conventions to protect intellectual property rights and has enacted a vast array of laws and regulations in this area. There is a host of regulations pertaining to computer software copyright, intellectual property right on

---

131 See "Refreshing Your Understanding of the Internet", ***China Daily*** (April 23, 2002), at http://www1.chinadaily.com.cn/bw/2002-04-23/68055.html. (Visited on April 30, 2002).

132 "Websites to Play the Name Game", ***China Daily*** (November 12, 2000), at http://search.chinadaily.com.cn/isearch/i_textinfo.exe?dbname=cndy_printedition&listid=13638&selectword=DOMAIN%20NAME.

Internet, and processing commercial transactions via Internet. Regulations on these areas are anticipated to grow substantially within the coming 2-3 years in compliance with the World Trade Organization (WTO) agreements and to cope with the international business environment.[133] Some examples of the regulations under this category are:

- *Regulations for the Protection of Computer Software* (Issued by the State Council on June 4, 1991);
- *Measures for Registration of Computer Software Copyright* (Issued by the Ministry of Machinery and Electronics Industry on April 6, 1992);
- *Notice on the Administration of Computer Software Copyright* (Issued by the State Copyright Bureau on October 19, 1994);
- *(e-publication* (Issued by … on December 30, 1997);
- Provisional Measures for the Administration of Software Products (Issued by the Ministry of Electronic Industry on March 4, 1998);
- The *PRC Contract Law* (Enacted by the National People's Congress on March 15, 1999). It recognizes the legality of contracts concluded through Internet or Intranet in the form of "data messages";
- *Regulations on Commercial Encryption* (Issued by the State Council on October 7, 1999) - most of its overreaching provisions, though, were effectively rescinded in March 2000;
- *Circular on Relevant Issues Concerning Online Business of Audiovisual Products* (Issued by the Ministry of Culture on March 24, 2000);
- *Interim Regulations for the Online Securities Brokerage Sector* (Issued by the CSRC in April 2000);
- *Procedures for the Examination and Approval of Securities Companies for*

---

133 For example, Shanghai has tightened regulations on Internet activities, especially in the realms of on-line shopping and e-biz, to create a more benign environment for those wishing to do business on-line.

The city is now requiring all firms involved in e-commerce, e-biz, on-line auctions and cyber-advertising to register and get a business licence from the Shanghai Municipal Industry and Commerce Commission.

The regulation became effective on September 1, 2000. "City Tackles Lawless Net", ***China Daily*** 09/04/2000) at http://search.chinadaily.com.cn/isearch/i_textinfo.exe?dbname=cndy_printedition&listid=10757&selectword=CITY%20TACKLES%20LAWLESS%20NET.

Engaging in Online Brokerage Activities (Issued by the CSRC in May 2000).

Law Enforcement

The Supervision Bureau for Public Information Security of the Ministry of Public Security was formed in September 1998. It is a specialized unit assuming the role of cyberspace police in China.[134] Today, the Ministry of Public Security in each of the 26 provinces, autonomous regions, and municipalities directly under the Central Government has set up a corresponding Supervision Bureau for Public Information Security, to combat cybercrime in China. For example, Shanghai, one of the largest and most progressive municipality in the nation established its own "Internet police" (wangluo jingcha) – Shanghai Internet Communication Safety Supervision Office (Shanghai Gonganju xingxi wangluo anquan jianchachu) - in June of 2001. The structure and function of the Shanghai "Internet police" mirror that of the MPS and other provinces. Its major functions are: guide, coordinate, inspect and supervise computer and internet safety of Party and government organs, financial and critical infrastructure and communication points; investigate and deal with according to law those intrude into and damage computer-information system, and study and form polices in the prevention of computer crime.[135] Since the establishment of the supervision bureau, a total of 6,889 cybercrime cases have been cleared between 1998 and 2001[136], roughly representing a clearance rate of 89% versus the total of 7,700 reported cases. The example of Internet bars raid is a very good illustration on the actions taken by the MPS to fight against the increasing crime in Internet bars.

---

134 One of the very first Internet police was at Shenyang. The Shenyang Municipality Public Security set up a "net police" office in the police force, then, Bureau Communication's Office, over ten years ago. The new "Internet police" is built upon this foundation – Shenyang Municipality Public Security Bureau Internet Safety Supervision Office. (Shenyangshi gonganju wangluo anquan jiangcha chu).

135 "Internet Police First Appears in Shanghai" ("Wangluo jingcha" zai Shanghai liangxiang") ***China Police Daily Online***, June 30, 2001, at http://www.cpd.com.cn/xxlr.asp?menulb=019%D4%DA%CF%DF%D0%C2%CE%C5&id=2053

136 See " Wangluo Jingcha Shenshou Bufan (Highly Competent Cyberpolice)", ***China Police Daily Online*** at http://www.cpd.com.cn, 11-Apr-2002. (Visited on 12-Apr-2002)

In view of a growing trend in criminality, the Chinese government, particularly the MPS, puts substantial efforts in regulating and controlling Internet bars and other electronic amusement shops alike. Many teenagers visit Internet bars, or Internet cafés to escape from their parents and teachers so as to enjoy surfing recreational websites freely without supervision. Since 1999, there are increasing criminal activities reported that involve Internet bars, e.g. pornography[137], gambling[138], fraud, and infringement of copyright. Recently, the term "electronic heroine" is newly coined in depicting the adverse impacts brought by Internet in an uncontrolled environment such as Internet bars. Many parents and teachers are in a worry that teenagers are easily caught in a net by illegal Internet bars jeopardizing their physical health as well as intellectual growth. For example, a 17-old student died of heart failure in an Internet bar indulging in playing computer games for long hours daily and continually for months.[139] The monitoring and regulating efforts on Internet bars will continue as more negative stories are reported. Back in late 2000, over 20,000 Internet bars and 12,000 computer games shops were suspended in a

---

137 For example, in April 2001, Yang Linhua and his wife set up "Chinese call girls" website where he posted lots of pornographic materials attracting subscription and advertising. They earned RMB35,000 in six months. The couple was arrested and prosecuted in January 2002 by Shenyang police. See "Purging Pornographic Materials from the Net, Calling upon the Sword of the Law" ("Wangluo saohuang fuhuan falu zijian"), ***China Police Daily Online*** (February 8, 2001) at http://www.cpd.com.cn/xxlr.asp?menulb=039%C8%CB%C3%F1%B9%AB%B0%B2%B1%A8&id=12058

138 Net gambling is a growing concern to PRC police. PRC noted the growth of net-gambling company is a worldwide phenomenon. In 1996 there were only 15 net gambling company worldwide. By 1997, there were 50. One company, the Yibo Wangluo Gongsi started in Nov. 1997 has a gross revenue growth by 5000% in just one year. By the year 2000 the company was grossing US$ 15,000,000 and doing business in 20 languages offering gambling in 16 sport events. In April of 2001, Liaoning province public security break up the nation's first net-gambling ring. (Source-Jiancha Ribao). See "Gambling on the Net, the Black Current of the WWW" (Wangshang dubo, wangluo shijia de hechao), ***China Police Report***, at http://www.china110.com/police/plzxjw/jfts/item/2001_11/574939.shtml. (Visited Feb. 20, 2002).

139 "High School Student Died Abruptly When Playing Computer Online Game", ***Xinhua News Agency*** (April 23, 2002) at http://news.xinhuanet.com/it/2002-04/22/content_367495.htm. (Visited on April 23, 2002).

campaign to regulate the Internet services market[140], and these commercial shops have to be operated under a valid license. The *Measures for Managing Business Operations in Providing Internet Services*, issued in 2001, prohibits an Internet bars to allow any teenagers of the age below 18 entering the shops without accompany of a guardian. It also restricts the shops' opening hours for teenagers: between 8 a.m. and 9 p.m. of national legislative holidays. A three-month campaign was held again between April and June, 2001 to curb Internet bars that had violated the law or allowed irregularities in their shops. More than 56,800 Internet bars or cafés were inspected across the country with 2,000 Internet cafés forced to shut down and 6,000 units suspended for making changes before operations.[141]

Cybercrime Prevention Through Education

Chinese leaders believe that it is important to promote ethics of the Internet and awareness of computer crime among young surfers as an effective means of cybercrime prevention. Apart from cracking down on Internet crime, it is crucial to enhance the use of a "healthy Internet" amongst the younger generation. According to the Vice-Premier Li Lanqing, "Supervision over culture-oriented and entertainment business needs to be strengthened to provide a healthy social atmosphere for young people." Law enforcement bodies are urged to standardize the operation of Internet services, electronic games centers and entertainment clubs in addition to regulating of book and audio-video products markets. Entertainment places, including the Internet bars are under strict supervision to prevent gambling, prostitution, drugs trafficking and other crimes.[142]

In order to promote healthy, ethical and moral use of Internet, the CPC organized a host of activities through the China Communist Youth League (Gongqingtuan or Gongchanzhuyi qingniantuan), e.g. issuing the "National Youth Civilized (use of) Internet Pact" (Quanguo qingshaonian wangluo wenming gongyue).[143] In the meantime, there are

---

140 "Quanguo quti 'wangba' lian wan jia" (Nation Suspended 20,000 'Internet Bars'), ***China Police Report*** (Dec. 12, 2000), at http://www.china110.com/police/policezt/item/2000_12/575498.shtml. (Visited Feb. 20, 2002)

141 "China Cleans Internet Cafés", ***Peopl's Daily Online*** (July 20, 2001) at http://english.peopledaily.com.cn/200107/20/eng20010720_75430.html. (Visited on April 23, 2002).

142 "Cultural Market to be Better Regulated", ***China Daily*** (August 17, 2001).

143 "Young People Have Ethical Norms on Internet Conduct" (Qingshaonian yaoliao wangluo xingwei daode guifan), ***China Police Daily Online*** (November 30, 2001), at

many seminars organized for parents and teachers in understanding the youth's Internet behavior and communication skills with the young surfers. Some studies indicate that the youth pick up 90 percent of their learning, including social knowledge, rules of the game, life philosophy, and concept of value, through mass communication media. In the Internet age, how to communicate with the youth becomes an emerging topic. One of the views from suggests that the traditions of Chinese culture should be preserved and integrated with the Internet culture openly. The youth should be induced with a stronger sense of social responsibility in coexistence with their rights. An evaluation scheme on social matters should be reinforced as well.[144]

Management Control

Chinese government has a fair understanding on the importance of effective network management in Internet environment. In a symposium on Internet Security and Management, Yang Zhenquan vice-director of the Information Office of the State Council commented that Internet security and management has become a general concern of people today following an Internet boom throughout the world. More efforts should be made to guarantee the security of the Internet in China. "No security and effective management, there will be no healthy development of the Internet to speak of, not to say the legal rights and overall interests of websites and social public to be undermined, that's a consensus view reached by the International community." [145] Effective management in Internet crime prevention covers a wide spectrum of areas, including personnel security, physical security, and operations security. The biggest threat to computer security is people. In fact, local studies indicate that most detected computer crime are committed by employees of the victim organizations. Developing a personnel security program, including employee selection process and staff training, in an organization contributes to prevention in computer crime. In addition to personnel

---

http://www.cpd.com.cn/xxlr.asp?menulb=039%C8%CB%C3%F1%B9%AB%B0%B2%B1%A8&id=8295. (Visited on April 30, 2002).

144 "Education New Topic: How to Communicate with the Youth in Internet Age", ***China Police Daily Online*** (April 15, 2002), at http://www.cpd.com.cn/xxlr.asp?menulb=039%C8%CB%C3%F1%B9%AB%B0%B2%B1%A8&id=15387. (Visited on April 30, 2002).

145 "No Security, No Healthy Development of Internet: Official", ***People's Daily Online*** (November 3, 2000) at http://english.peopledaily.com.cn/200011/03/eng20001103_54290.html. (Visited on April 30, 2002).

security, physical security is vital in restricting people from unauthorized access into a computer facility. Through operations security measures, Chinese government is putting efforts in promoting awareness of possible crime among potential victims and discouraging a criminal from actually committing a computer crime. However, Chinese leaders are aware of their deficiency in security management and strive to improve the effectiveness.

Technology Control

By nature, Internet is an artifact of advanced technology and sophisticated human intelligence. Information system design weaknesses and program flaws are attractive to hackers, with or without malice. Fighting computer crime is warfare in a virtual space requiring technical know-how and cross-border co-operation. Such a battle requires a strong understanding of information technology. China is in a disadvantage position – China is in a catching mode with most IT products and technical skills being imported; system weaknesses sometimes pre-exist depending on types of IT product or vendor; and Internet infrastructure builds on open technology that creates extra difficulty in control. As counter-measures, China adopts international security standards to establish national standards in information technology and communication networks.[146]

Preventing and combating hackers is an area that MPS allocates substantial resources in protecting computer network safety and information system security. For deterrence purpose, China imposes severe punishment on criminal hackers of serious nature, such as disrupting the order of the socialist market economy and embezzlement. For examples: In 1999, Zhao Zhe in Shanghai was sentenced to 3-year imprisonment and a RMB10,000 fine for breaking into the computer system and manipulating prices on the Shanghai Securities Exchange causing a direct loss of RMB2.95 million.[147] In June 2000, a 36-

---

146 For example, China has established 13 national standards and 6 military standards in information security technology as of 1997. See Jiang Ping, ***Jisuanji Fanzui Wenti Yanjiu*** (Research into Computer Crime Problems) (Bejing: Commercial Press, 2000), pp. 266-268.

147 "Zhao Zhe, a staff member at a securities company, broke into the computer of the Shanghai Securities Department of the Sanya Zhongya Trust Investment Company and changed five transaction records, causing the turnover of two stocks to increase drastically, and bringing about a direct loss of 2.95 million yuan. This is the first case of a hacker attempting to influence prices of securities on the Shanghai bourse." See "Computer Hacker Sentenced to Three Years in Prison", ***People's Daily Online*** (November 15, 1999), at

year old hacker in Hangzhou, Fang Yong was sentenced to death for embezzling over RMB one million from a bank account. The punishment of this case is recorded the most severe that a Chinese judicial organization has given to a hacker.[148] In April 2002, Luo Yun-bin, a hacker to a telecom system in Jiujian of Zhejian was on trial and pleaded guilty. The case is reported being the first one in attacking an information system and the second one being prosecuted for destroying computer system in the country. The term of punishment will be announced by court shortly.[149] Not all uncovered hackers are prosecuted successfully, though. For example, Zhejian public security cracked one of its first computer crime (hacker) case in 2001. The case is reported being the second computer crime in China. The hacker Zheng Guwei got hold of other people's computer code and started to trade securities with the accounts for funs and excitement. When he was arrested on April 25, 2001, Zheng had generated a total loss of over RMB39,000 from four victims. Zheng was charged with criminal damages but the Wenling procuratorate found the charge inappropriate and released Zheng on May 30, 2001. Zheng finally settled with the victims and agreed to pay them RMB55,000 to compensate their loss.[150]

---

http://english.peopledaily.com.cn/199911/15/eng19991115T104.html. (Visited on April 12, 2002).

148 "As an accountant in Ningbo branch of the Bank of Communications of China, Fang Yong embezzled about 1.66 million yuan (about US$200,000) of public money, by counterfeiting bank paper, and taking money from people's account from May to August 1990. He fled to Canada in 1990 and was expelled by the Canadian government last year [1999] and sent back to China for trial." See "Chinese Hacker Sentenced to Death for Embezzlement", ***People's Daily Online*** (June 13, 2000), at http://english.peopledaily.com.cn/200020/13/eng20000613_42866.html. (Visited on April 12, 2002).

149 Luo Yunbin, a graduate in Information and Electronic Engineering of Zhejian University, worked as a system technician in Unicom and Telecom Bureau of Taizhou city. He was charged for illegal access into the billing database of the Telecom Bureau in Internet and deletion of critical data on customer billing on September 13, 2001. The system was resumed normal on September 16 with reported financial loss of 100,000 yuan. See "Country's First Case of 'Hacker' in Disrupting Telecom System On Court Today", ***People's Daily Online*** (April 23, 2002), at http://www.peopledaily.com.cn/GB/it/49/150/20020423/715970.html. (Visited on May 2, 2002).

150 Zheng Guwei, a medical technology college graduate, participated in the stock market

In terms of technological details in fighting hackers, very little information is released, probably because hacking details are not formally reported or the information is classified confidential. Instead we are informed of other non-technological approaches in resolving the problem. For example, there was a hacking plan organized by five organizations to attack overseas websites on May 1 this year. The plan was finally called-off[151] after lobbying efforts by the Internet Society of China and the China National Computer Emergency Response Team/Coordination Center (CNCERT/CC). CNCERT under the MPS is also responsible for monitoring and preventing any virus attack on computer systems and information networks, providing assistance in recovery solutions, and tracking the source of such criminality. When CIH virus broke out around April 26, 2001, statistics indicated that there were 5,000 telephone calls received by anti-virus producers and emergency centers from various sectors including computer, finance, post, government departments, education and science research. According to a survey by the China National Security Office and the Ministry of Public Security, a total of 73 percent computer users in the survey have encountered the virus and 59 percent have been infected for three times or more.[152]

---

trading (Zhejian province Wenling stock trading unit) with his own savings since March 1998. In 2001, during the Chinese New Year, Zheng visited the Wenling stock trading unit and observed a young lady helping an old lady to input her code. He remembered the code and started to trade for the old lady for fun. From March to April 24, 2001, Zheng traded for the old lady 11 times, with a loss of 21,100, i.e. from 30,000 to 10,000. Challenged by the experience, Zheng started to break into three other accounts. On March12, 2001 one of the account holder (Ye) discovered that he could not enter his own account. On March 15, 2001, Ye's wife discovered that someone has been trading with their account with substantial loss. The case was reported to the Sanmen County police. Because the case was first of its kind in the province, it received much attention from the public security. Computer technical experts of the Wenling public security worked with Wenling stock trading experts on the case. Zheng was soon arrested on April 25, 2001. See "Zhejian Number One Hacker Is Arrested" (Zhejian touhao gushi heke luowang), ***China Police Report***, at http://www.china110.com/police/plnews/gdjs/zhej/item/2001_11/574555.shtml. (Visited Feb. 20, 2002).

151 "May 1 Hacker Warfare Plan Called Off ", ***People's Daily Online*** (May 8, 2002), at http://www.peopledaily.com.cn/GB/it/20020508/723638.html. (Visited on May 9, 2002).

152 "'Red Code II' Lands in China, Dutch Hackers Claim Bug Intriguer", ***People's Daily***

Even though little could be done in coping with technological changes in Internet, China remains to have a strong motivation to impose Internet censorship in controlling information flow and limiting information access for political reasons. Some scholars have made a study on a censorship strategy in using combinations of new technologies, such as intranets and firewalls to create controlled Internet environments in China.[153] "If China is attempting to build a national intranet to take advantage of established network connectivity while limiting access to information forbidden by Chinese Internet regulations, it would become the largest intranet in the world if successfully implemented."[154] The result is yet to be seen.

Summary

In this section, we have seen how China government attempts to control cybercrime from four aspects: legislative, education, management, and technology, with an objective to prevent (fang), combat (da), and regulate and control (zhi). The approach in cyberspace control and Internet regulation in China is an extended arm mirroring the comprehensive scheme in controlling other criminal activities. In the coming section, I'll discuss the impacts and limitations of such a comprehensive control approach in cyberspace governance and Internet regulation in China.

Online (August 8, 2001), at http://english.peopledaily.com.cn/200108/08/eng20010808_76837.html. (Visited on April 12, 2002).

[153] William Yurcik and Zixiang Tan, The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China", ***University of Pittsburgh and Syracuse University*** (1996), at http://www.tprc.org/abstracts/tan.txt.

[154] L.T. Greenburg and S.E. Goodman, "Is Big Brother Hanging By His Bootstraps?", ***Communication of the ACM***, July 1996/Vol. 39, No. 7, pp. 11-15.

VII. IMPACT AND EFFECTIVENESS OF COMPREHENSIVE CONTROL

Comprehensive approach has been a common and consistent strategy of the CPC in governing China. The effectiveness of such a comprehensive scheme in cyberspace governance varies depending on the control objective in a particular area. In preventing young people from exposure to vice, the comprehensive approach is successful to a large extent. The adolescent issues on Internet-related vice are similar to that of other countries. In fighting against vice on Internet, Chinese government mirrors the same approach in combating other traditional crimes, such as pornography and gambling, except the crime takes place through different media. The battlefield is now shifted to a virtual space and the instruments deployed are of advanced technology. The campaign in promoting the "National Youth Civilized Use of the Internet Pact" for a moral and civilized use of the Internet by the youngsters is a visionary long-term strategy. With the presence of a political and socialist structure, unlike U.S., China is able to induce this concept relatively easier through mass education and top-down approach. The campaign events, organized by the China Communist Youth League with various local communities, are very typical and effective tactics deployed by the authorities to conduct awareness training, to have active participation and to obtain commitment of the youth in fighting against Internet crime.[155] The criticism on this educational approach curbing creative thinking of the youth is a separate discussion. Interestingly, some U.S. officials support the idea and have also suggested the youngsters to learn "cyber-ethics"[156]. The U.S. Department of Justice arranges programs, like the Cybercitizen Partnership[157], to teach

---

155 See "Chinese Youngsters Vow to Clean Up Net", ***People's Daily Online*** (November 29, 2001), at http://english.peopledaily.com.cn/200111/29/eng20011129_85583.shtml. (Visited on April 30, 2002).

156 See "Teen Hackers Told to Learn 'Cyber-ethics', Obey Law", ***China Daily*** (April 21, 2000), http://search.chinadaily.com.cn/isearch/i_textinfo.exe?dbname=cndy_printedition&listid=4890&selectword=CYBER; (Visited April 30, 2002). "WASHINGTON: The top US law enforcer has a message for teen hackers: The law is watching you. -- Speaking after Canada announced on Wednesday the arrest of a 15-year-old in connection with attacks on CNN's Web site in February, US Attorney-General Janet Reno made a call for children to learn "cyber-ethics.""

157 See "Remarks of Attorney General John Ashcroft, First Annual Computer Privacy,

young people the right ways to use the Internet, and there is a web page designated for cyber ethics information.[158] On-going actions taken by the Ministry of Public Security in China, such as Internet bars raid and restricted opening hours for youths, have a deterrence effect. The introduction of safe Internet bars is another proactive measure to safeguard the youth and reduce their exposure to crime opportunity. In this aspect, we can see a comprehensive scheme applied entirely by the Chinese government with Felson's theory attempting to remove motivated offender, reduce crime opportunity and provide guardianship to the youth in prevention of Internet crime. There are much more work to be done as noted in the teleconference jointly held by eight government agencies in early May and a special control program is being planned to clean up the Internet.[159]

In preventing educated people from being informed of online news and opinions disapproved by the Chinese government, such as western democracy, human rights debate and falungong, the comprehensive scheme adopted is similar to what China has been doing in controlling other communication media. China keeps the radar on 24-hour a day throughout the year, monitoring very closely and tightly. Action will be taken immediately if any sensitive information on the web is detected. For examples,[160] in December of 1999, China Democracy Party founder Wang Youcai was sentenced to 11 years in prison for subversion. Two of his crimes were sending e-mail to exiled Chinese dissidents in the United States and accepting overseas funds to buy a computer. VIP Reference, an electronic magazine based in Washington, breach Chinese system of censorship over the Internet by way of e-mailed into China. The group distributes the

---

Police & Security Institute (May 22, 2001)", ***Computer Crime and Intellectual Property Section (CCIPS)*** of the Criminal Division of the U.S. Department of Justice, at http://cybercrime.gov/AGCPPSI.htm.

158 See "General Information – Cyber Ethics", ***Computer Crime and Intellectual Property Section (CCIPS)*** of the Criminal Division of the U.S. Department of Justice, at http://cybercrime.gov/.

159 See "Eight Ministries Joint Conference on Special Program to Keep the Internet Clean from Malevolent Information", ***Xinhua News Agency*** (May 1, 2002), at http://news.xinhuanet.com/newscenter/2002-05/01/content_379468.htm. (Visited on May 4, 2002)

160 See Farley, Maggies, "Electronic guerrillas breach blocks set up by the government to keep citizens from seeing unorthodox news and opinions on the Internet," ***LA Times*** 1999 at http://www.gis.net/~cht/dissidents.html

pro-democracy magazine throughout China with shotgun blasts of e-mail to about 250,000 addresses compiled from commercial and public lists.[161] Unlike vice websites that contain pornography and gambling contents, this kind of ad hoc information dissemination is so unpredictable but organized that there is hardly any preventive action that the Chinese government may take in a proactive manner. Moreover, technology keeps changing so rapidly that it is impossible to filter all suspicious websites. Thus, cases of disapproved news and opinions, like falungong, are handled individually as they emerge. Of course, China imposes severe punishment for deterrence effect. Overall speaking, the effectiveness of the comprehensive scheme in preventing disapproved contents on the Internet is not obvious except the CPC continues to work hard in educating the people on political doctrines and patriotism. As long as China still benefits economically from the Internet, it is unlikely and technologically impossible that the Chinese government would curb all external websites that keep changing and increasing. China will keep watching and leave this problem area status quo, co-existing with other Internet development, in a controlled manner within a tolerance limit acceptable to the CPC. This area remains the most threatening and tricky to the Chinese leaders and the ruling position of the CPC in a long run.

In building up a secure Internet environment for E-commerce and preventing the network from attacks, the effectiveness of comprehensive scheme is not obvious. From the earlier discussion on Internet legislation and administrative regulation, a comprehensive legal framework appears to be missing for Internet-related activities including network security and E-commerce. In terms of technological measures, China is not equipped well today although Chinese leaders are working very hard to have more local people trained up. The comprehensive scheme seems working better for educating the youth on civilized use of Internet, but not so effective in this aspect. More conscious efforts in making legislation for Internet are deem necessary.

---

161 Lin Hai, a 30 years-old Shanghai software entrepreneur was named China's first "cyber-dissident", was charged and convicted of providing 30,000 banes to VIP References on December 4, 1999.

VIII. CONCLUSION

The Internet technology is so powerful that China's economy cannot prosper without it. On the other hand, Internet changes the flow of information and contents of information available in the community. As such, Chinese leaders strongly believe that cyberspace must be governed and policed through a comprehensive scheme. Through combined efforts in legislation, education, management and technological measures, China attempts to develop a unique model in cyberspace governance and regulate Internet in China.

Internet development has been so rapid and dynamic since 2000 that the existing legal framework in China is outdated and no longer sufficient to serve the changes. The Internet related regulations put forth so far tend to be piecemeal and on a reactive mode. Following accession into the World Trade Organization (WTO), E-commerce related legislation, such as digital signature and encryption, appears to be one of the most urgently needed among all.

From technological perspective, China needs to speed up research and development on critical IT products, such as encryption, firewall, and router, to overcome weaknesses in importing these security and communication technology. As long as China has to rely heavily on imported technology, China will not be able to evade from computer attacks, thus in turn assure a complete control in network security.

Human resources is key to cyberspace governance. China needs to put substantial investment to train up more professionals, ethical and quality people in management control of various dimensions such as system operations, information security management, process management and computer audit.

Internet is extra-territorial that has no border by nature. Cybercrime in a virtual world very often needs to be tackled by joint efforts from various countries. International co-operation is critical for Internet crime prevention and control in defining standards, information exchange, and law enforcement.

Through Internet, Chinese people are able to achieve a quality improvement in their living, knowledge and culture. Cyberspace governance in China is just a means of

assurance in achieving the goal and it is still a long way. In President Jiang Zemen's words, "On the one hand, we should … complete information networking legislation, strengthen enforcement of law and administration of justice, legally attack networking criminal offences and construct a good order featuring the rule of law. … On the other hand, we should … firmly establish strategic awareness, security awareness and lawful awareness of information network among the people of the whole country, vigorously promote socialist moral standard, create a sound social foundation for the orderly development of information network and promote the healthy development of China's information network."[162]

---

162 See "Using Legal Means to Guarantee and Promote Sound Development of Information Network", People's Daily Online at http://english.peopledaily.com.cn/200107/12/eng20010712_74810.html. (Visited on 24-Apr-2002).

References

1. Books in English

Clarke, Ronald V. and Marcus Felson. "Introduction: Criminology, Routine Activity, and Rational Choice", ***Routine Activity and Rational Choice, Advances in Criminological Theory, Volume 5*** (Transaction Publishers, 1993)

Erbschloe, Michael. ***Information Warfare: How to Survive Cyber Attacks***, (Osborne/McGraw-Hill, 2001)

Felson, Marcus. ***Crime and Everyday Life – Insight and Implications for Society*** (Pine Forge Press, 1994)

Icove, David, Karl Seger and William VonStorch. ***Computer Crime: A Crimefighter's Handbook***, (O'Reilly & Associates, Inc., 1995)

Mueller, Milton and Zixiang Tan. ***China in the Information Age: Telecommunications and the Dilemmas of Reform***, (Praeger Publisher, Westport Connecticut, 1997)

Pfleeger, Charles P. ***Security in Computing***, (Prentice-Hall Inc., 1989)

Ralston, Anthony, Edwin D. Reilly and David Hemmendinger. ***Encyclopedia of Computer Science, Fourth Edition (2000)***, (U.K.: Nature Publishing Group, 2000)

2. Books in Chinese

Jiang, Ping. ***Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)*** (Bejing: Commercial Press, 2000)

Li, Wenyan and Others. ***Jisuanji Fanzui Yanjiu (Computer Crime Research)*** (Beijing: Zhongguo Fangzheng Chubanshe, 2001)

Yu, Zhigang and Others. ***Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime)*** (Jilin: Jilin Renmin Chubanshe, 2001)

Gongan Neiqin Gongzuo Shouce (Police Administrative Manual) (Beijing: Jingquan Jiaoyu Chubanshe, 1994)

Jisuanji ji Wangluo Falu Fagui (Computer and Internet Laws and Regulations) (Beijing: Falu Zhubanshe, 2000)

Zhongguo Gongan Baike Quanshu (***Chinese Public Security Encyclopedia***) (Changchun: Jilin chubanshe, 1989)

Zhonghua Renmin Gongheguo Fadian (Laws of the People's Republic of China, Chinese-English Edition) (Jilin: Jilin Renmin Chubanshe, 2000)

3. Articles in English

Abramson, Rachael. "Catching Files with Chopsticks: China Strategic Leap into Wireless Telecommunication", ***Minnesota Journal of Global Trade***, Winter 2002.

Barlow, John Perry, *A Declaration of the Independence of Cyberspace*, Davos, Switzerland (1996)

Bell, Tom W., *The Common Law in Cyberspace*, 97 Mich. L. Rev. 1746 (1999)

Bruce Sterling, ***The Hacker Crackdown: Law and Disorder on the Electronic Frontier*** http://lonestar.texas.net/~dub/sterling.html

Cooper, S. David. "The dot. Communist Revolution: Will the Internet bring Democracy to China?", ***UCLA Pacific Basin Law Journal,*** Fall 2000.

Cullen, Richard and Pinky D. W. Choy. "The Internet in China", ***Columbia Journal of Asian Law***, Spring 1999.

Dorothy E. Denning, "Concerning Hackers Who Break into Computer Systems", http://www.cosc.georgetown.edu/%7Edenning/hackers/Hackers-NCSC.txt

Feir, Scott E. "Regulations Restricting Internet Access: Attempted Repair of Rupture in China's Great Wall Restraining the Free Exchange of Ideas", ***Pacific Rim Law & Policy Journal***, March 1997.

Goldsmith, Jack L., *Against Cyberanarchy*, 65 U. Chi. L. Rev. 1199 (1998)

Johnson, David R. and Post, David G., *Law and Borders: The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367 (1996)

Kennedy, Gabriela. "China rushes to catch up with the Internet", ***International Financial Law Review***, London, Jul 2000.

Liang, Clara. "Red Light, Green Light: Has China Achieved Its Goals Through the 2000 Internet Regulations?" ***Vanderbilt Journal of Transactional Law***, November 2001.

Lei, Wendy. "Economic Boon or Regulatory Bane? The Emergence of The Internet in Modern Chin", ***Rutgers Law Record***, October 13, 1997.

Lessig, Lawrence, *The Zones of Cyberspace*, 48 Stanford Law Review 1403 (1996)

Lessig, Lawrence, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harvard Law

Liang, Clara. "Red Light, Green Light: Has China Achieved Its Goals Through the 2000 Internet Regulations?" ***Vanderbilt Journal of Transactional Law***, November 2001.

Luo, Wei, "How to Find the Law of the People's Republic of China : A Research Guide and Selective Annotated Bibliography", ***Law Library Journal***, Summer 1996.

Post, David, G., *Internet: Of Black Holes and Decentralized Law-Making in Cyberspace*, ***2 Vand. J. Ent. L. & Prac. 70 (2000) Review 501*** (1999)

Post, David G., *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace*, ***52 Stan. L. Rev. 1439*** (2000)

Qiu, Jack Linchuan. "Virtual Censorship in China: Keeping the Gate between the Cyberspaces", ***International Journal of Communications Law and Policy***, Winter 1999/2000.

Reed, Kristina M. "From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce", ***The Transnational Lawyer***, Fall

1999.

Reed, Kristina M. "From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce", ***The Transnational Lawyer***, Fall 2000.

Rheingold, Howard, *The Virtual Community: Homesteading on the Electronic Frontier*, 1993

Ronald B. Standler, "Computer Crime"
http://www.rbs2.com/ccrime.htm

Saleem, Omar. "The Establishment of a U.S. Federal Data Protection Agency to Define and Regulate Internet Privacy and Its Impact on U.S.-China Relations : Marco Polo Where Are You?", ***The John Marshalll Journal of Computer & Information Law***, Fall 2000.

Smith, Bradford L. "The Third Industrial Revolution: Policymaking for the Internet", ***Columbia Science and Technology Law Review***, 2001.

Tan, Zixiang (Alex). "Regulating China's Internet: Convergence toward a coherent regulatory regime", ***Telecommunications Policy***; Kidlington Apr/May 1999.

Tan, Zixiang (Alex). Foster, William, Goodman, Seymour. "China's state-coordinated Internet Infrastructure", ***Association for Computing Machinery, Communications of the ACM***, New York, Jun 1999.

Taylor, John H. III. "Fourteenth International Symposium on Economic Crime Corruption: The Enemy Within: Excerpts from the Symposium Held at Jesus College Cambridge, September 8-13, 1996: Comment: The Internet in China: Embarking on the "Information Superhighway" With One Hand on the Wheel and the Other Hand on the Plug", ***Dickinson Journal of International Law***, *Spring* 1997.

Wang, Jiang-yu. "The Internet and E-Commerce in China : Regulations, Judicial Views, and Government Policies", ***The Computer & Internet Lawyer***, January 2001.

Wong, Kam C. "Police Reform in China in the 1990s", ***British Journal of Criminology*** (2002)

4. Articles in Chinese

Cai Zhonghan, "Guoji Hulianwang de Fazhan ji Falu Yinsu Fenxi" (Development of Internet and Analysis of Legal Factors), ***No.3 Keqi Yu Fa Lu (Science Technology and Law),*** 1996

Guo Liben, "You 'Michelangelo' Bingdu Suoxiangqi De" (Reflection on 'Michelangelo' Virus), ***No.2 Keqi Yu Falu (Science Technology and Law)***, 1992.

Huang Guomin, "Shilun Jiasuanji Fanzui" (On Crime by Computer), ***No.3 Keqi Yu Falu (Science Technology and Law)***, 1995.

Jin Cheng, "Wangluo dui Qingshaonian Fanzui de Yingxiang ji Fangzhi Duice Yanjiu" (Study of the Impact of Internet on Teenager Crime and its Prevention Strategies), ***No 3 Gonggan Daxue Xuebao (Journal of Chinese People's Public Security University),*** 2001

Li Shuangqi, "Wangluo Fazui Zhencha" (Investigation of Internet Crime), ***No 3 Gonggan Daxue Xuebao (Journal of Chinese People's Public Security University),*** 2001

Li Wenyan and Yu Zhigang, "Guanyu Gongganjuquan Yingdui Jisuanji Zuifan de Xitong Sikao" (The Systematic Thinking of the Countermeasures Held by Police in Striking the Computer Crime), ***No.6 Gonggan Daxue Xuebao (Journal of Chinese People's Public Security University),*** 2001

Lin Chao, "Guanyu Gonggan Jiquan 'Wang Shang' Zuozhan de Sikao (The Thinking of Fighting in the Internet Held by the Police), ***No.1 Fanzui Yanjiu (Study of Criminal Crimes)***, 2000.

Liu Tianfeng, "1991-2000 Woguo Qingshaonian Fanzui De Tedian Yuanyin Yu Yufang Duice (The Characteristics, Causes and Preventive Measures of Juvenile Crime in China Between 1991 and 2000)", ***Qingshaonian Fanzui Yanjiu (Juvenile Crime***

Research) No. 2, 2002.

Rong Huizhen, "Diannao Wangluo – Wei Chengnian Ren Shishi Fanzui De Xin Meijia (Computer Networks – New Media for Juvenile Crime)", ***Qingshaonian Fanzui Wenti, (Juvenile Crime Issues) No. 2, 2002***.

Shi Ying, "Lun Jisuanji Fanzui" (Review on Computer Crime), ***No.7 Jingji yu Fa (Economy and Law),*** 2000

Shi Ying and Hao Minglei, "Jisuanji Fanzui de Changjian Shouduan" (Common Measures in Computer Crime), ***No.11 Jingji yu Fa (Economy and Law),*** 2000

Wang Shizhou, "Lun Diannao Fanzui" (On Crime by Computer), ***No.2 Keqi Yu Falu (Science Technology and Law)***, 1996.

Wang Xunfei, "Wangluo Xinxi Anquan de Ruogan Falu Wenti" (Some Legal Issues on Information Security of Internet), ***No.4 Keqi Yu Fa Lu (Science Technology and Law),*** 1996

Wei Hongxin, "Wangluo yu Qingshaonian Shehuihua" (Internet and the Socialization of the Minors), ***No 3 Gonggan Daxue Xuebao (Journal of Chinese People's Public Security University),*** 2001

Yang Hongtai, "Fangfan Jisuanji Fanzui de Falu Sikao" (The Legal Thinking in the Prevention of Computer Crime), ***No.3 Fanzui Yanjiu (Study of Criminal Crimes)*** 2000

Yang Zhongmin, "Jisuanji Fanzui Anjian Quanxia Chutan" (Preliminary study on the Division of Responsibility of Government Bodies in Computer Crime), ***No.1 Gonggan Daxue Xuebao (Journal of Chinese People's Public Security University),*** 2002

Zhang Jiaying, "Wangluo Fanzui yu Wangluo Anquan" (Internet Crime and Internet Security), ***No.2 Fanzui Yanjiu (Study of Criminal Crimes)*** 2001

Zhao Bingzhi and Yu Zhigang, "Lun Jisuanji Fanzui de Dingyi" (On Defining the Computer Crime), ***No.5 Xindai Faxue (Modern Law Sciences)***, 1998.

5. Websites in English

China Daily, http://www.chinadaily.com.cn

China Gateway, International Trade Administration, U.S. Department of Commerce**,** http://www.mac.doc.gov/china/chinagateway.html

China.org.cn (Zhongguo Wang), http://www.china.com.cn/english/index.htm

The China Internet Network Information Center (***CNNIC***), http://www.cnnic.net.cn/e-index.shtml

Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, http://cybercrime.gov/

LawInfoChina.com, (Peking University Center for Legal Information), http://www.chnlaw.com/

The Ministry of Foreign Trade And Economic Cooperation, PRC, http://www.moftec.gov.cn/moftec_en/index.html

People's Daily Online (English), http://english.peopledaily.com.cn

Universities Service Centre (USC) for China Studies, http://www.usc.cuhk.edu.hk

6. Websites in Chinese

Beida Falu Wangluo (Peking University Center for Legal Information), http://chinalawinfo.com/

The China Internet Network Information Center (***CNNIC***), http://www.cnnic.net.cn.

China Legal Daily, http://www.legaldaily.com.cn

The Ministry of Foreign Trade And Economic Cooperation, PRC, http://www.moftec.gov.cn/moftec_cn/

The Ministry of Information Industry, PRC, http://www.mii.gov.cn.

The Ministry of Public Security, PRC, http://www.mps.gov.cn.

Renmin Gongan Bao Dianziban (China Police Daily Online) at http://www.cpd.com.cn.

Renmin Wang (People's Daily Online), http://www.peopledaily.com.cn

Universities Service Centre (USC) for China Studies, http://www.usc.cuhk.edu.hk

Wangluo Wenmin Gongcheng (Internet Moral and Civilization Project), http://imcp.ccnt.com.cn/

Xinhua News Agency Online, http://www.xinhua.com.cn

Zhongguo Jingwu Baodao (China Police Report) at http://www.china110.com