Cyberspace Governance in China

Kam C. Wong, Xavier University
Dr. Kam C Wong

January 15, 2011

7 pm

132,503

All rights reserved
PART I: OVERVIEW

PART II: CYBERSPACE GOVERNANCE IN THE PEOPLE’S REPUBLIC OF CHINA

Chapter One: Introduction
Chapter Two: Researching into China Cyberspace Governance
Chapter Three: Internet in China
Chapter Four: Nature, Prevalence and Distribution of Computer Crime
Chapter Five: Cyberspace Governance in China
Chapter Six: Cyberspace Governance with Chinese Characteristics
Chapter Seven: Conclusion

PART III: CYBERSPACE GOVERNANCE IN HONG KONG

Chapter One: Introduction
Chapter Two: Researching into Hong Kong Cyberspace Governance
Chapter Three: Information Technology Usage and Penetration in Hong Kong
Chapter Four: The Discovery of Cyber Risk, Computer Crime and Electronic Privacy

Chapter Six: Cyberspace Governance in Hong Kong

Chapter Seven: Conclusion

APPENDIX I

The Internet Timetable of China Series CNNIC: 1987 to 2008

APPENDIX II:

The National Medium- and Long-Term Program for Science and Technology Development (2006-2020)
PART I

Overview
OVERVIEW

Computer processing and Internet communication has changed the way we learn, work, play and associate with each other. In the case of China (People’s Republic of China (PRC) and Hong Kong), the introduction of computer and spread of Internet has boosted economic growth, speeded up social progress, transformed the political landscape and changed the lifestyle of the Chinese people in untold ways. ¹ As a recent (2007) Editorial in Beijing Review attested:

“The Internet has come to shape the way people work and live in China, and this revolution has its positive as well as negative aspects. On the positive side, many profit-seeking Web sites have emerged to serve the vast Chinese Internet users, including sites specializing in advertisements, games, mobile phone value-added services, and fee-charging membership services. China's current boom in consumer spending has been fueled in part by Internet use. However, for all the freedoms and convenience of use the Internet offers, there are negative aspects. The lack of privacy and the vulnerability of private information is a major problem. Moreover, the Internet boom highlights the digital divide in China between rural and urban areas in terms of access and resources.” ²

During the economic reform, Internet has delivered people from rags to riches. With people in the street, the Internet offers an open forum to communicate with insulated officials and talk back at non-responsive government. Internet has also been used to conduct “public supervision” and deliver “e-justice”. In a recent public affairs forum (2007) in The PRC participants debated whether netizens have the right to take the law into their own hands in pursuing Internet justice, such as “human fresh search”. Some favor the use of Internet for public supervision. Others caution against the errors and terror of summary e-justice.

Lastly, many people use the cyberspace as a private retreat. In 2010, PRC Internet served 420 millions netizens, mostly of them under 25. They see the Internet less as a political or business tool but as a personal site for self-expression and social network to build customized community. For the young people, some use the Internet to make friends, build network, and pass time. Many others use it to actualize their fantasy, as in the case of “wanghun” (web marriage). In 2004, there were 100,000 web marriages and by 2007, there were a million.

Alternatively, the Internet can turn itself into a “public space” for people to hang out and exchange ideas. In so doing, the web blogs foster civil engagement and build

---

4 Yang Gengshen, Ji Huitao and Han Xue, “Do Netizens Have the Right to Take the Law Into Their Own Hands?” Beijing Review, Vol. 50 (25): 46-7 (June 21 2007)
civil society. Internet turns out to be a tool and a space for all person, purpose and season.

As alluded to above, 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 the case of PRC, according to the latest survey (July 2010) reported by the China Internet Network Information Center (CNNIC), there is an exponential rise of computer ownership and Internet usage in China to the tune of 420 millions. Computer crime has also leaped frog proportionally. The growth in computer/Internet and associated criminality has taken the PRC political leadership and government policy makers by surprise. In reaction, the PRC government has taken draconian steps and adopted a comprehensive control scheme to arrest the growth of computer crime, such as building a firewall to stop objectionable materials entering the cyberspace and enlisting mom

---

9 While computer crime in China, as in elsewhere, are selectively reported and poorly recorded, resulting in incomplete records and invalid data, there are sufficient preliminary indication that computer crimes are growing faster than computer utilization. See 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 Jan. 12, 2011). Thus observed, computer crime in China is growing disproportionately, instead of proportionately, relative to the growth in computer utilization.
against porn to clean up the information highway. However, the control measures fall far short of being a coherent regulatory framework, nor are they effective in taming the cyberspace.

Coming to the role, impact and control of Internet in Chinese political economy, Johan Lagerkvist is much impressed with CCP’s effectiveness in harnessing and controlling the Internet in advancing China’s economic (globalization of trade), political (strategic use of nationalism) and social agenda (Internet supervision of government).10

Lagerkvist observed that technological sophisticated netizens are increasingly able to use Internet to mobilize public opinion (Liu Yong case) and influence public policy (SARS epidemic of 2003). At the same time, political savvy leadership has routinely used the Internet to drum up support for national popular support for the regime (the Diaoyudao/Senkaku border dispute). 11

This research project is a study of cyberspace governance and Internet regulations in China (PRC and Hong Kong) with indigenous China perspective and data. The study of cyberspace governance and Internet regulations in China, both in law and social science, is just beginning.12

12 Milton L. Mueller, Ruling the Root: Internet Governance and the Taming of Cyberspace (Cambridge, Mass.: MIT Press, 2002). (“In Ruling the Root, Milton Mueller uses the theoretical framework of institutional economics to analyze the global policy and governance problems created by the assignment of Internet domain names and addresses.”); Zixue Tai, The Internet in China: Cyberspace and Civil Society (CRC PRESS, 2006) (The Internet in China examines the cultural and political
The book begins with an investigation into the latest development of Internet in China (Part II). This is followed by an exploration of the nature, prevalence and distribution of computer crime. The last part of the book finishes with a comprehensive description and thorough analyzing of existing PRC cyberspace regulatory regime. Finally, various recommendations in improving cyberspace governance and Internet regulation are proposed.

In respect to Hong Kong, it is at the frontier of the information age. As a premier “Cyber-port” in the Asia-Pacific region, Hong Kong reaps many of the intended benefits as well as suffers from a number of unanticipated consequences that comes with going cyber. On the positive side, computer mediated communication (CMC) brought people closer together in a virtual world. At the negative end, computers and Internet facilitates traditional criminality and introduces new ones. In order to safeguard the e-commerce environment and maintain cyberspace order, the Hong Kong government has studied and experimented with different ways to control and govern the cyberspace. This research project is an attempt to study cyberspace governance and computer crime control in Hong Kong.

The Hong Kong report (Part III) begins with an investigation into computer usage and Internet penetration in Hong Kong. This is followed by investigation into the “discovery” of cybercrime as a cognizable phenomenon in Hong Kong. The report then explores the nature, prevalence and distribution of computer crime in Hong Kong. All these contextual explorations set the stage for a comprehensive review and critical ramifications of the Internet for Chinese society. The Chinese government has enthusiastically promoted the rapid growth of the Internet while at the same time has as zealously sought to control the virtual environment. Individuals have responded with impassioned campaigns against official control of information.)
analysis of Hong Kong government’s computer crime control and cyberspace governance regiment. The report closes with a number of recommendations in improving Hong Kong cyberspace governance.
II

CYBERSPACE GOVERNANCE IN THE PEOPLE’S REPUBLIC OF CHINA
Chapter One

Introduction

Overview - characteristics

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 and cultural barriers. Compare with traditional communication, e.g., mail, phone or fax, CMC is much faster, cheaper, and effortless. People can share a large amount of information instantaneously. With the synergetic integration of computer and telecommunication technologies the Internet radically transforms the traditional information infrastructure; allowing people to communicate with each other anywhere, anytime and in many ways. In this way Internet becomes a catalyst of social, political, economic, cultural, scientific and government reform and development. The catalytic impact of Internet has domino effects and rippling consequences. It radiates from a variety of centers and penetrates diffuse layers of the

14 Ook Lee, “Understanding cyberspace behavior with the critical social theory,” Journal of Academy of Business and Economics Vol. 5(1); 131 -7 (2005).
generating unexpected consequences and registering far reaching impact. The impact and influence of Internet are quite beyond what has been contemplated. They still escape full accounting on hindsight. As one perceptive scholar 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”. Finally, The Internet and cyberspace is still morphing, very much a history in the making; defying control and staring down the law regime along the way.

As a medium, Internet is appealing because it is free, accessible and anonymous. People can come and go, as they like. People can say what they want as they please. People can become who they want to be, as they desire. For some the Internet allows them to act out their fantasy. For others it allows them to live in another world. For everyone else Internet makes possible the changing of personal relationship (at will) and transformation of socio-political structure (with few costs).

As such, Internet is particularly appealing to the young who are impatient with the old (tradition) and fascinated with the new (ideas).

18 “Internet penetration and impact” Pew Internet and America Life a Internet Project. (April 2006) 


21 Internet access and use is subject to economic, geographic, cultural, technological and legal barriers.

Internet has become a catalyst of reform with virtually every aspects of our society. The catalytic impact of Internet reaches into every corners of the Chinese society. No place is safe. None is spared. The impact and influence of Internet on Chinese life and society is immense and immeasurable. It has yet to realized it full potential.

With China, CMC has increased productivity, boosted economic growth, expedited social progress, radicalized political development, changed discourse pattern, and re-arranged lifestyle, all with grave impact and lasting consequences. In 2005 a CASS Internet Survey concluded that:

“[T]he political impact of the Internet is more significant than it is in other countries. The impact can be seen not only in the relationship between government and citizens but also among people who share similar political interests. Thus, we can predict that as Internet becomes more popular in China, the impact on politics will be stronger.”

27 Guo Liang, “Surveying Internet Usage and Impact in Five Chinese Cities,” Research
Specifically, Internet has empowered the netizens and liberated the society, without necessarily changing the authoritarian disposition of leaders or autocratic nature of the regime.\textsuperscript{28} As such, Party officials with a reform mind and Chinese activists of all persuasions also embrace it.\textsuperscript{29}

According to Professor Li Xiguang, Professor/Director, Center for International Communications Studies, Tsinghua University: “The Internet means different things to different people in different societies. To some, it provides an opportunity to make money; to others, it means freedom from press controls. For still others, the Internet is a public forum in which citizens of a closed society can discuss politics.”\textsuperscript{30}


\textsuperscript{29} Guobin Yang, \textit{The Power of the Internet in China: Citizen Activism Online} (N.Y.: Columbia University Press, 2009). (“Online activism is a response to the grievances, injustices, and anxieties caused by the structural transformation of Chinese society. State power constrains the forms and issues of contention, but instead of preventing contention, it forces activists to be more creative. Culture, understood as symbolic forms and practices, informs and constitutes online contention through both traditional and innovate rituals and genres. Market-driven business interests favor contention despite the dangers of manipulation. Civil society organizations strategically use the Internet to promote social change. And finally, transnationalization expands the scale and radicalizes the forms of online activism. All this adds up to a complex picture of online activism as a central locus of social conflict and social transformation in contemporary China.”)

\textsuperscript{30} Li Xiguang, “The Internet's Impact on China's Press,” Professor/Director, Center for International Communications Studies, Tsinghua University, China. Keynote speech at Asia-Pacific Journalists Meeting, 2001 RTHK
To the user, Internet’s function is neither this (depositor of knowledge) or that (transmitter of values) but what one wants it to be.\footnote{Christian Sandvig, “The Internet at play: Child users of public Internet connections,” \textit{Journal of Computer-Mediated Communication}, Vol. 11(4), (2006) http://jcmc.indiana.edu/vol11/issue4/sandvig.html} Some use it as a commercial tool, others use it as a recreational platform.

For the society, the utility of Internet is determined by historical, social and cultural context. For example, to the Americans Internet liberates as it democratize the people. For the Chinese, Internet is best used for reform and modernization of a nation.\footnote{Yongming Zhou , \textit{Historicizing Online Politics Telegraphy, the Internet, and Political Participation in China} (CA: Stanford University Press, 2006), p. 4.}

\footnote{Ibid. Yongming Zhou , p. 238.} In the ultimate analysis, the content, meaning and impact of Internet message is less intended – as determined by the sender as much as it is understood – received by the readers.

In all, Internet offers up unlimited opportunities for rich and poor, dreamers or adventurers, drifters or loafers, for work as well as play, make money or kill time, with little constrains and few consequences. Yang describes the Internet in China thus:

“The web inhabits a world with dynamic fields other than states and business corporations. Academia is turning to the web for educational purposes; journalists are experimenting with online journalism; aspiring authors have found new channels for publishing their works. These social groups, and many others, are now linked to their counterparts around the world and these ties have spawned their own internal dynamics. As has often happened in the history of modern societies, weaker parties tend to
enter coalitions to resist or negotiate with dominant political and economic actors. In the final analysis, then, the condition and fate of the Chinese virtual public sphere depends as much on its internal dynamics of private pleasures and public concerns as on the changing political, social, and technological environment.”

Alternatively, the Internet can turn itself into a “public space” for people to hang out and exchange ideas. In so doing, the web blogs foster civil engagement and build civil society. Finally, for the radicals, the Internet offers a forum to challenging the Party and government with minimum risks.

Impact of Internet

Ten Contributions of Internet to China

According to a well informed Chinese blogger, Internet brought about ten discernible changes to China in the last 40 years. First, people have and are able to change their outlook and worldview through interacting with others on the web. Second, people developed a strong sense of self in the process of articulating and defending their ideas on the web. Third, Internet helps to form collective identity in various virtual communities or during grass roots movement. Fourth, Internet fosters public discussion

34 Yang Guobin, “Mingling Politics with Play: The Virtual Chinese Public Sphere,” IIA Newsletter | # 3 3 | March 2003, p. 7
http://www.iias.nl/iiasn/33/IC_Mingling%20Politics.pdf
36 Zixue Tai, The Internet in China: Cyberspace and Civil Society (Routledge, 2006)
and debate on current events or controversial issues, keeping people informed and engaged as active citizens. Fifth, Internet improves government legitimacy and efficiency. Government and governance cannot do away with Internet. Sixth, Internet revolutionized communication, from vertical and central to horizontal and diffused. Seventh, Internet changes the way people relate to and communicate with each other. Eighth, Internet changes commercial practices and trade relationship. Ninth, Internet changes entertainment. Tenth, Internet changes public consciousness.37

**People in the street**

With the average people in the street the Internet offers an open forum to share ideas between people, talk back “to” the government and exchange information around the world.

**Business and industry**

During the economic reform, Internet has delivered people from rags to riches. Wu Xisang, a former computer programmer, became a multi-millionaire in China overnight by capitalizing on his knowledge and skills with the computer. Wu started his first of many Internet companies after graduating from college in 1995. He is now on his fifth start-up. The fact that he sold his first four companies for huge profits earned him the nickname “taoxian chengxuyan” or "the programmer who keeps cashing out."38

---

According the White Paper on “The Internet in China” (2010) the contribution of IT to economic development includes:

“The Internet has become an engine promoting the economic development of China. IT including the Internet and its industry has made significant contributions to the rapid growth of the Chinese economy. In the past 16 years the average growth rate of the added value of Chinese IT industry grew at over 26.6% annually, with its proportion in the national economy increasing from less than 1% to 10%. The combination of the Internet and the real economy, the reform and enhancement of traditional industry through IT …In 2008 Internet-related industries generated a turnover of 650 billion yuan, with sales of Internet-related equipment reaching 500 billion yuan-worth, accounting for 1/60 of China's GDP, and 1/10 of its global trade. Its software operations had a turnover of 19.84 billion yuan, up 26% over 2007.

E-commerce is undergoing rapid development. The e-commerce of large enterprises has expanded from online information release, purchase and sales to integrated online web design, manufacture and management between upstream and downstream enterprises…Online retailing is expanding quickly, and its market is being gradually regulated. According to a sample survey, over 50% of big enterprises have established e-commerce system, over 30% of small and medium-sized companies find their product suppliers through the Internet, 24% of them are engaged in marketing via the Internet, and there are over 100 million online buyers in China. In 2009 the trade volume of e-commerce in China surpassed 3.6
trillion yuan-worth. Specialized e-commerce services are taking shape. The supporting systems such as digital authentication, e-payment and logistics are being gradually formed.”

In the past five years, the average annual increase rate of online advertisement has maintained a level of 30%, with its turnover reaching 20 billion yuan in 2009. The online gaming industry in China had a turnover of 25.8 billion yuan in 2009, an increase of 39.5% over 2008, ranking top in the world. Online literature, music, radio and television in China have all witnessed rapid development….“39

E-government

The Chinese government championed the use of Internet to communicate with the people, to increase transparency of government and promote accountability of officials.40

On February 13, 2009, before the annual NPC and CPPCC sessions, Xinhuanet.com opened a column entitled "Premier, Please Listen to Me." The column leads with the following, "Whatever you want to say to our Premier, and anything you are concerned about and want our Premier to know, you may express here." In 2005, on occasion of the NPC and CPPCC sessions, Premier Wen again said, "I have browsed the pages of Xinhuanet.com. The netizens raised several hundred questions for me to answer. Their suggestions and opinions are worthwhile for me and our government to consider

earnestly." 41

In May 2009, the National Audit Office released an investigation “sport check report which showed Henan, Gansu, Shanxi, Heilongjiang, Jiangsu, Hunan, Fujian and Shaanxi provinces, the Inner Mongolia autonomous region and Chongqing municipality misused 2.69 billion yuan ($394 million) from an agriculture fund two years ago. The Internet users posed many comments on the net approving of NAO report”, which was welcomed by the government with open arms.42

According to the White Paper on “Internet in China” (2010):

“The Internet serves to publicize government information. In the mid-1990s the Government Online Project was launched. By the end of 2009 China had established more than 45,000 government portals. Seventy-five central and state organs, 32 provincial governments and 333 prefectural governments and over 80% county-level governments had set up their websites, providing various online services to facilitate people's work and life. The building of e-government has substantially improved the work efficiency and transparency of government information. Article 15 of the Regulations of the People's Republic of China on the Disclosure of Government Information, which was promulgated and put into force in 2008, stipulates, "Government agencies should take the initiative to disclose government information and should be disclosed by means of government gazettes, government websites and press conferences, as well

as through newspapers and magazines, radio, television and other methods that make it convenient for the public to be informed." The central government requires governments at all levels to establish corresponding mechanisms and give prompt explanations to issues of public concern. …The role of the Internet in satisfying people's right to know has become increasingly prominent.”

Politics

For the disaffected, the Internet allows them to air their discontent, ferment dissent and organize protest. Falun Gong (FLG) was able to use Internet to promote its cause, in distributing FLG - Li Hongzhi messages, mobilizing the grassroots followers, organizing a world-wide campaign, and challenging the Chinese government. A jailed dissident in China described the Internet as “God’s present to China”:“With the censorship here, my essays can only be published overseas…To avoid the articles being intercepted, I often went (to) a foreign friend who owned a fax machine… The Internet has made it easier to obtain information, contact the outside world and submit articles to overseas media. It is like a super-engine that makes my writing spring out of a well.

______________________________

The internet is an information channel that the Chinese dictators cannot fully censor, allowing people to speak and communicate, and it offers a platform for spontaneous organisation…Open letters signed by individuals or groups are an important way for civilians to resist dictatorship and fight for freedom. …Back then it took a lot of time and resources to organise an open letter…In an era without the internet, it was impossible to collect the signatures of several hundred people, and it was also impossible to disseminate the news rapidly all over the world. At the time, the influence of and the participation in letter-writing campaigns were all quite limited. We worked for many days, and in the end we would only get a few dozen people to sign. The letter-signing movements in this new era have made a quantum leap…The ease, openness and freedom of the internet has caused public opinion to become very lively in recent years. The Government can control the press and television, but it cannot control the internet. The scandals that are censored in the traditional media are disseminated through the internet. The Government now has to release information and officials may have to publicly apologise.”

**Internet supervision**

The Chinese government, especially under Hu-Wen administration is committed to efficient, effective and clean government, with the help of public opinion supervision. Internet supervision is one of the strategies to make government work transparent and officials accountable. In the latest White Paper on: “China's Efforts to Combat Corruption and Build a Clean Government”, the State Council made the following
observations of public opinion and Internet supervision on clean government.

“IV. Power Restraint and Supervisory System

“The Constitution endows citizens with the rights to criticize, advise, appeal, lodge lawsuit against or impeach state organs and state functionaries ... China lays great store by supervision from public opinion. The right to interview and right to supervise through public opinion of news media, including newspapers, television and radio, are protected by law. ... In recent years, with the rapid development and popularity of the Internet, supervision through the Internet has become a new form of supervision by public opinion that spreads quickly, produces great influence and features a wider range of participation. China highly values the positive role played by the Internet in enhancing supervision, conscientiously strengthens the collection, research, judgment and management of information regarding combating corruption and advocating integrity from the Internet. It is making efforts to enact laws and regulations on report websites and improve the acceptance mechanism and clue application and feedback system of the report websites in order to offer a convenient and unimpeded channel for the public to exercise their right of supervision through the Internet. Meanwhile, efforts are being made to strengthen the management, guidance and standardization of

supervision by public opinion so as to ensure that supervision by public opinion operates along the orbit prescribed by the law…”

On Dec. 4, 2009, in a yearend review of notable media related events, Internet public opinion supervision emerged as one of the most important media story. To many people in China Internet public opinion supervision is democracy in action.\textsuperscript{48} To the socially aggrieved, economically oppressed and legally wronged, Internet provides for “public supervision” of officials\textsuperscript{49} and “virtual justice” by netizens.\textsuperscript{50}

For example, in Nov. 2009, a netizen accidental came upon a set of government documents show official travel expenditures. He decided to circulate them on the net with the note “I accidentally uncovered the expenditure list of civil servants’ foreign inspection tour.’ The list and 37 photos created an Internet buzz and have since called “Inspection gate.” The officials involved were from Jiangxi province, Xinyu Municipality and Zhejiang province, Wanzhou Municipality. The documents show that “11 member of Xinxu human resource inspection group” spent a total of 35,000 yuan in 13 days. The “Wanzhou training group” of 23 members spent a total of 65,000 yuan in 21 days. Both groups of officials were immediately investigated and finally disciplined. The officials also have to repay the expenditure of the trip personally.\textsuperscript{51}

In early 2008, Jiangsu province, Suzhou Municipality, Quanshan District, District

\textsuperscript{48} “Grassroots” Internet supervision power emerges, realization of progress in democracy.” Ben Yue Kan (Bi-monthlyMagazine Jan. 23, 2009. \url{http://news.xinhuanet.com/zgjx/2009-01/23/content_10707844.htm}


\textsuperscript{50} Yang Gengshen Ji Huitao and Han Xue, “Do Netizens Have the Right to Take the Law Into Their Own Hands?” \textit{Beijing Review}, Vol. 50 (25): 46-7 (June 21 2007)

\textsuperscript{51} Ibid.
Political Committee, Secretary Dong Feng’s wife sought out China Mineral University Professor Wang Peiron and supplied Wang with evidence of Deng Feng’s economic and personal work style problems. On May 11, 2008, Wang dispatched such materials to CCP Inspection and Discipline Department by speed mail. There was no reply for two months. On July 6, 2008, Professor Wang submitted a blog entry entitled “The nation’s most corrupted and shameless district committee secretary”. Upon receipt of the entry, the web master followed up with a web essay: “Jiangsu Xuzhoy, district committee secretary directs and performs an incredulous “one husband two wives” act”. This was picked up and spread by many other web sites. The Xuzhou Municipality learned of the Internet expose, and decided to investigate and take discipline action. On July 11, 2008, Dong Feng was suspended from duties. On July 18, 2008, the Party and government formally disciplined Dong. On August 29, Dong was arrested.\textsuperscript{52}

According to the Red Internet “Voices of the People” editor Zhoa Xiong, Internet supervision is popular because it works. “Voices of the People” started in May of 2001. Since then it has issued 3,200 “investigation letters” and provided response to 70,000 inquires. It has provided supervision and solution in 25,000 cases. The response rate is over 85%. For two years in a row, i.e., 2007 and 2008, it has successfully elicited 1000 response each year from provincial and municipal offices, government officials and lawyers. In 2008, “People’s Voices” was awarded number one media price.\textsuperscript{53}

The power and utility of Internet supervision is confirmed by a public opinion survey conducted in January of 2009. On March 3, 2009, \textit{People’s Daily} reported the

\textsuperscript{52} “Grassroots” Internet supervision power emerges, realization of progress in democracy.” Ben Yue Kan (Bi-monthlyMagazine Jan. 23, 2009. \url{http://news.xinhuanet.com/zgjx/2009-01/23/content_10707844.htm}

\textsuperscript{53} \textit{Id.}
result of an online survey on the popularity and influence of the net as a public opinion – supervision (网络监督) tool. The survey reveals that Internet is a preferred mode of supervision and expression of opinion. To the question “Do you think Internet supervision is necessary?” 51% responded yes, Internet is “very necessary as a supplement to traditional public opinion supervision.” 41% while recognizing Internet’s importance thought that it is illegitimate. “Does not possess legality, only kind of Internet violence.” As to necessity, 7% believed people “can do with or without it. Should be integrated into the mainstream public opinion cannels.” Others are 2%. More tellingly, to the question “When you observed socially undesirable event, will you select the Internet to expose?” 93.3% of the respondents responded positively. Finally, when asked whether they pay attention to Internet opinion supervision,” 87.9” said they pay a lot of attention, 7.1% average attention, 2.2% sometimes pay attention, and 2.6% no attention.

Internet justice

Netizens use Internet for many things, from searching for information to providing for entertainment to helping with self-actualization. Lately the Internet has been used to pursue informal (Internet) justice of all kinds – moral, legal, social, economical. For example, in May 2007 the students humiliated a senior geography teacher. The netizens tracked down the students and demanded an apology. They


blocked the web site of the school, identified the students by name and address and
demanded for a pubic apology. On Feb. 26, 2006, a lady was found crushing the head of
a cat. The photos were circulated on the net. The lady was hunted down and compelled to
apologize.

In regard to “Internet justice”, on December 29 2007 a 31 years old Beijing
woman committed suicide after blogging about her husband's infidelity. A netizen
decided to post a blog entry on Tianya: “The final blog diaries of the MM who committed
by suicide by jumping down 24 floors.” Many sympathetic netizens responded. Most of
them condemned the husband. This precipitated a net vigilante movement. The netizens
mounted an Internet search (“ren rou sou sou”) for the where about of Wang Fei, the
unfaithful husband. After finding him, the netizens demanded justice. They confronted
him. They wrote graffiti on the apartment wall, such as “A blood debt must be repaid
with blood.” Wang Fei and his girl friend was fired by the advertisement company. In
March 2008, Wang decided to sue the web master and two other websites for defamation
in the Beijing Chaoyang District Intermediate People's Court, claiming damages for
mental suffering. The case has been called the No 1 “Renrou” case. The case raises a
number of legal as well as moral issues, including: (a) netizens’ right to search for a
person’s identity vs. privacy rights; (b) webmaster’s legal responsibility to monitor
inappropriate messages of netizens; (c) proper limits of moral criticism posed by netizens

56 The Bogger’s name is Jiang Nan. Her last blog was entitled: “The Migrant Bird That
57 “Suicide MM's Blog” EastSouthWestNorth
http://www.zonaeuropa.com/20080120_1.htm
58 Sky Canaves and Julie Ye, “China's Online Culture Goes Unchecked,” Wall Street
There are divergent opinions on pros and cons of Internet justice:

Yan Gangshe from “Youth China Daily” is against using the Internet to deliver informal justice. All justice must be achieved by means of law. Internet justice has the potentiality of infringing on people’s rights and privacy. In this regard, summary justice is no justice at all.

Hue Xue from “Procuratorate Daily” observed that Internet could be used to shame immoral people and safeguard social safety. However, net justice can be messy and unruly. Without proper supervision, netizens might trample on the rights of individuals and harm people’s reputation with supported assertions or incomplete facts.

Gao Fushen of “Workers’ Daily” proposed that virtual media should be publicly supervised and legally restrained. Virtual manhunt resulted from righteous indignation and blind sympathy, rather than calm refaction and logical reasoning.

Li Jinsong of hlj.red.net.cn opined that Internet is just another way to hold people responsible, for their conduct. If people can easily escape social condemnation for misdeed, social order and morality will breakdown.

Liu Pingxin of “Procurator Daily” stated that there is not much harm to net investigation as a way to expose immorality and make people aware of social injustice, provided that it is done reasonably, responsibly and within the law.

Bingyu Zijing of souhou.com observed that human flesh hunting online is a new form of punishment. As a result of public furor and mass hysteria, it is usually conducted violently and in-discriminatory. Online justice offers a last bastion of protection for the meek and weak who are less able to protect themselves or otherwise have little resource

---

to get justice from the legal system.60

Problem with Internet public opinion

Li Wufeng, Bureau Chief of the State Council Information Office Internet Affairs Bureau pointed out the potential problems of runaway public opinion on the web. 61

First, Internet expression is driven by media hype. Online discussion can only carried out in a harmonious manner if the news is reported in an orderly way. Thus it is extremely important to regulate and ensure the proper dissemination of online news.

Second, the problems with republishing of news stories include - indiscriminate recycling of news stories, from whatever source and without regard for truth or impact; creating “news laundering“62 to avoid news publication regulations; posting inappropriate, objectionable and illegal content through interactive interfaces (forums, blogs); newspapers and websites feeding on each other, generating an artificial media hype, e.g., the Internet reporting and debate over of Deng Yujiao incident63 and

61 http://chinadigitaltimes.net/china/li-wufeng/
62 “News laundering” is similar to “money laundering” where the first publisher who has no permission to publish news seeks to ‘republish” a news item by “laundering” it through a first publisher.
63 “Waitress Deng Yujiao who stabbed to death Communist official walks free,” Times Online June 19, 2009. (“A young waitress hailed as a heroine after fatally stabbing a Communist Party official who demanded sex walked free today after a court ruled that she acted in self-defence. Deng Yujiao, 21, became a cause célèbre, in a case perceived widely to show a young woman having the courage to stand up to the power of the State.”) The case has been cited as an example of people – Internet power.
http://www.timesonline.co.uk/tol/news/world/asia/article6513750.ece
Hongzhou street car race\textsuperscript{64} cases was distorted and disproportionate to original impact of such cases;

Third, there are many issues involved with republishing, e.g., as a result of media hyping, little incidents become big issues, and small issues have the potential of being turned into crisis; media hype creates a base and vulgar culture; a few unsubstantiated source or a few manipulative bloggers can influence the direction and mood of public opinion on a given issue.

Zhu Huaxin (祝华新), is the Editor and Secretary of the "Sentiments Monitoring Office" of State owned People's Net Online (人民网). Zhu is also an editor and journalist on the site. On July 24, 2009, Zhu offered up ten guidelines for local governments on how to handle Internet public opinion.\textsuperscript{65}

\textit{First, this is a new era of public opinion.} Now anyone who has a computer or Blackberry can make his voice heard on the Internet, unmediated and without censored (most of the time). Since then Internet has become "a distribution center for cultural information and a magnifying glass for social opinion." This fulfill 17th CPC National Congress quest for people's rights to gain information, rights to participate, rights for expression, and the rights to monitor.

\textit{Second, officials should be ready to deal with the emergence of one huge} "pressure group" with 338 million (June 2009) Internet users, since 226 million netizens

\textsuperscript{64} Wang Hongyi, “Putting the skids under street racing,” \textit{China Daily}, September 5, 2009. (In May, 2009, Hu Bin, a kid from a wealthy family was racing in the street of Hangzhou at 84 – 101 km when he ran into Tan Zhuo and killed him after throwing him 5 m into the air. Original police reported only 70 km in a 30 km zone.)

read online news, 100 million people visit BBSs, 108.2 million netizens have blogs and 15.5 million netizens use their mobile phones to get on the Internet.

Third, officials should be on top of incident news development. “In the case of breaking incidents, the government has to try to publish the news at the first opportunity, to win the rights for speech, and be the first there in order to have a leading position. The "management of crisis" is in reality the "management of communication in a crisis."

Fourth, local leaders should learn to depoliticize social issues. Others local issues might turn into a national incident if they are not handled properly.

Fifth, local government should deal with small problems before it gets out of hand and becomes an Internet – nationwide concern.

Sixth, local government, and especially Propaganda Departments, must capture the high ground in dealing with the public and Internet voices. Such can be achieved by winning the hearts and mind of the people in a democratic way.

Seventh, mass incidents can be effectively dealt with in four ways: publish the reality of the situation, punishing people who are responsible, holding officials accountable, and restoring social order, and disciplining irresponsible officials. Lessons can be had from Weng’an incident. 66

Eight, government should leverage and see "primary advantage" in guiding public opinion. 67 Since the government has more access to all the information available

67 Citizens have the right to know. “The Decree of Government Information Openness” (政府信息公开条例) (May 1, 2008). But, publishing, news reporting and the media is heavily regulated. Regulations for the Administration of Publishing (Promulgated on December 25, 2001, by the State Council as Decree No. 343. Effective February 1, 2002); Regulations for the Administration of Radio and Television (Promulgated on
to individual netizens, it can and should influence and direct the content and flow of news media (whether newspapers, television or websites). And most importantly, the government should provide timely, truthful, comprehensive and systematic news to the people.

*Ninth, the Propaganda Department of the local government should develop "friends" in the Internet community (BBS, micro-blogging, QQ groups) as well as with citizen reporters and with the leaders of Internet opinion.*

*Tenth, government officials should handle public sentiments over the Internet in a sensitive and compassionate manner.*

In order to correct the distortive influence of the media and web and set the record straight, the Party and government has turned to “guiding” the news and media with their own Internet commentators. In order to do so, starting in October 2004, the Municipal
Secretariat Office, Municipal Party Committee School, Municipal Party Committee Research Office started to recruit and train a group of supervised Internet commentators (IC) to direct and comment on news event in favor of the government. The ICs are paid a basic salary of 600 yuan per month and 50 cents (“wu mao qian”) for each additional Internet postings. They main duty is to closely supervise Internet opinion, supply public opinion information, and selectively conduct Internet promotion campaign, especially during crisis, such as Wang’an incident.

The Internet Commentator team would pick a topic each week and promote Chang Sha Municipality’s latest achievements, methods and experience in government with 30 web sites all over the nation, such as Renmin.com, Minmng.com, Sinhua.com. IC commentaries duties include tracking negative reporting, responding to attacks and working with web master to deleting any Internet material that are deemed harmful to the Municipality. The ultimate objective is to promote and polish Chang Sha’s image in eyes of the public nation wide.68

Since then, PRC government at each level has organized “Internet Public Opinion and Promotion of Government Class” lasting from a few days to a few weeks to train people to be ICs. The classes focus on the impact of Internet for government work in crisis, including: “Government agenda setting system and public opinion guidance”, “Major incident writing advocacy skills and experience” and “News propaganda and government image, Mass incident response and crisis management”69

68 “Regarding Nanchang, Changsha, Chengzhu progpanda culture work” (“关于南昌、长沙、郑州宣传文化 工作的考察报告”) http://friendfeed.com/yihuaderen/45787d69/4
69 http://www.mail-archive.com/gfw-blog@googlegroups.com/msg00336.html
The ICs are not always well received. There are a number of problems with ICs: First, the qualification and competence of the IC are not all the same. Their output and impact is not uniform. Second, ICs are supposed to present facts and articulate viewpoints favorable to the government. At a minimum, they are there to provide contrary (more complete) facts and/or render different accounts to the story. This might not be possible, without skewing the truth or misrepresenting the facts, or otherwise sounding patronizing or contrive. This would lose the interest of the readers, trust of the people and creditability of the government. Instead of helping to promote/defend the government it has the opposite effect of creating credibility and integrity problems. In essence, ICs might turn the people into cynics. Third, the ICs are supposed to mix with other netizens, be at one with them, including seeing things from their perspective and talking like them. In so doing, the CIs can relate to the netizens on their own terms, not courting their resentment or rejection. This is often difficult to do, especially in cases where the netizens are at odd with the government on the issues. In most, if not all cases, the ICs must agree with the netizens to disagree, e.g., acknowledge that the government is in wrong first before suggesting a better way of doing things. Finally, more damning, the ICs’ job is to promote government image. In concrete terms this boils down to promoting (defending) the leaders against negative publicity. Given such a charge, the ICs are likely to post comments with the sole purpose of pleasing the boss. This is at odd with the original tasking of ICs which is to promote the image of the government, and if need be to be critical of the leaders.70

Civil society

Lastly, the Internet fosters the development of civil society\textsuperscript{71} in China. Many people use the cyberspace as a private retreat, personal playground and common meeting place. In this regard, the Internet provides an uncensored medium for self-expression and group association. It makes possible political activism, social liberation and civil engagement. The following is a few observations on the impact of Internet on civil society by Professor Guobin Yang:

First, with respect to China’s public sphere, the social uses of the Internet have fostered public debate and problem articulation. The Internet has demonstrated the potential to play a supervisory role in Chinese politics. Second, the Internet has shaped social organizations by expanding old principles of association, facilitating the activities of existing organizations and creating a new associational form, the virtual community. Finally, the Internet has introduced new elements into the dynamics of protest.\textsuperscript{72}

Social-political impact

In a CASS research report published in November of 2008, researchers found that

\textsuperscript{71} Civil society is characterized by: (1) autonomous individuals; (2) civic associations; (3) privately organized activities; (4) a public sphere away from the state. Adam Seligman, \textit{The Idea of Civil Society} (New York: Free Press, 1992), p. 179.

the Internet has transformed the how the government communication with the people. Since the establishment of the PRC, the state has controlled the media as an education and propaganda device. With the discovery of virtual space and advent of Internet the state has to come to terms with free expression of opinion in the “public space.”

Accordingly to a recent (2008) survey of 12 Chinese cities released by the State Council 71.8% of the web users and 69.7% of the non-web users agree (totally agree or agree) with the statement “with the use of the Internet there are more opportunities to express ones political view.” With the question: “with the use of the Internet there are more opportunities to express ones political view” 68.8% of the web users and 61.5% of the non-web users either totally agree or agree. With the question: “with the use of the Internet, people can get to understand more about government policy” 79.2% of the web users and 77.4% of the non-web users totally agree or agree. With the question: “with the use of the Internet, people can get to understand more about government policy” 79.2%. of the web users and 77.4% of the non-web users totally agree or agree. Finally, with the question: “with the use of the Internet, high officials are more able to understand common citizens opinions” 72.3% of the web users and 73.3% of the non-web users totally agree or agree.

In the book MEDIA, IDENTITY, AND STRUGGLE IN TWENTY-FIRST-CENTURY CHINA, the authors Rachel Murphy and Vanessa Fong made the following statements:

73 “通过使用互联网有更多的机会发表自己的政治观点”
74 “通过使用互联网，人们有更多的机会批评政府的政策”
75 “通过使用互联网，人们能更了解政府的政策”
76 “通过使用因特网，高层官员能更好的了解普通民众的意见”
77 Hung Ninghao, “Chinese Internet Discourse: In the International Relations Arena and with Government Interaction” CASS Report 2008-11-07 18:53:45
http://www.sociology.cass.cn/shxw/shwl/t20071002_13808.htm
observation:

“Internet has transformed the way Chinese people and government interact and communicate with each other in untold and unexpected ways. For example, people are using Internets in not only for personal liberation or attack on government, but or realize its own received identity and rediscover hand down culture. Thus it is fool hearted to see it as the last bastion of person freedom from government and political dissent. (p. 255.) More pointed, liberating from watchful eyes of society is not the same as liberating to Western values.”

Western misperception

Internet research of and about China from abroad tends to focus on: censorship, blocking, democratization and dissent. The conventional wisdom in the West is that the technological characteristics and functional features of the Internet (pre) determines the outcome of IT revolution, i.e., spread of Internet would inevitably lead to yearning for freedom of speech and result in the demise of authoritative government. Such prognosis is rarely supported by empirical evidence, other than episodic, anecdotal and selective examples.

A researcher, using data collected from BBB (on usage and content), show that both the Westerners (liberating narrative and Chinese (control discourse, leapfrog

---


79 Research conducted in 2003-4 in Fuzhou & Xiamen in Fujian Province.
discourse) have wrongfully assessed the utilities and functions, and in turn misjudge the impact and implications of the Internet development in reformed China. The wrongful assessment by Western pundits resulted as much from blind ideological zeal and passionate advocacy, as it is from a lack of interest in understanding the reality through empirical investigation. 80 Specifically, the author found:

First, netizens were mostly male (60%), young (80% under 35), educated (70% with senior high education).

Second, Westerners, while complained of blockage to Western and offense sites, such as CNN, failed to disclose that they have unrestricted access to many other sources of information offered in the WWW. Internet users are inconvenienced, not totally deprived. They are denied some information but are also given many other sources of information, not available in their own country.

Third, many local Chinese, especially those who are older and educated, understand the need for reining in a runaway Internet. As a matter of philosophy, a lot more people want meaningful regulation of the Internet in order to protect the kids Internet filth. They embrace the government’s attempt to protect the society, promote (wholesome) culture and outlaw immorality. More importantly, they are fearful of luan (chaos) in society caused by irresponsible speech leading up immoral thinking and disorderly conduct, as with the disintegration of Russia or chaotic economic and political development in Taiwan.

Fourth, a majority of the young people in small towns (58% in 2004) was more interested in playing Internet games and surfing the net, than discussing politics (Western

80 Kam C. Wong, Police Reform in China: A Chinese Perspective (Taylor and Francis, 2011).
assumption) or doing business (Chinese assumption).

Fifth, denizens are willing and able to lodge complain on the web in cases of injustice, but few call for systemic change of the political system in favor of more freedom and democracy. In essence Western observation and obsession with Chinese web dissent as indicative of widespread discontent over free speech is misguided. Chinese people do not want total free speech. They want more control (over filth) and more freedom (to associate) in the cyberspace at the same time.

Sixth, Internet is entering a post-modern age. Netizens are using Internet in self-serving and individualistic way. This defies traditional model of Internet being good at fostering political participation and social involvement. For example, Geis confirmed that Chinese netizens prefer using BBB for inter-personal social-emotional communication, not political – logical exchange. According to Guobin Yang and Giese such discourse is personal, intimate and anchored within Chinese history and culture.

**Internet growth**

In China, the growth in the use of CMC has been tremendous over the past few years. The growth is exponential, not incremental. By 2010, China has invested 4.3 trillion yuan in Internet infrastructure construction over past 13 years. The network has a


84 “China invests 4.3 trillion yuan in Internet infrastructure construction over past 13
total length of 8.267 million kilometers, 840,000 kilometers of which were long-distance optical cables. Internet is accessible to 99.3 percent of towns and 91.5 percent of villages. 96 percent of the towns have broadband. The plan is to achieve Internet penetration of 45% by 2015. \textsuperscript{85} 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.\textsuperscript{86} In 2009 it is 338 million. By July 2010 it is 420 million.

The Internet has become an engine promoting the economic development of China. "IT including the Internet and its industry has made significant contributions to the rapid growth of the Chinese economy." \textsuperscript{87} Between 1994 and 2010, the average growth rate of the added value of Chinese IT industry grew at over 26.6 percent annually. IT’s proportional contribution to national economy increase from less than 1 percent to 10 percent. In 2009 alone, the gaming industry had a turnover of 25.8 billion yuan (3.79 billion U.S. dollars), an increase of 39.5 percent over 2008. “In the past five years, the average annual increase rate of online advertisement has maintained a level of 30 percent, with its turnover reaching 20 billion yuan (2.94 billion U.S. dollars) in 2009.”\textsuperscript{88}

\textit{Informationization of China}

As a planned economy, China has a well thought out national strategy to develop the IT industry in aid of the nation’s economic and social development, with leadership years,” \textit{Xhunhua}, June 8, 2010.

\textsuperscript{85} \textsuperscript{86} “The Semiannual Survey Report on the Development of China’s Internet (January 2002)”, \textit{The China Internet Network Information Center (CNNIC)}, at \texttt{http://www.cnnic.net.cn}. (Visited on February 27, 2002).

\textsuperscript{87} White Paper on “The Internet in China.” (2010)

\textsuperscript{88} Id.
and infrastructure to match. The White Paper on “The Internet in China” (2010) has this to say about China’s IT development plan:

“I. Endeavors to Spur the Development and Application of the Internet

“China takes Internet development as a significant opportunity to boost its reform and opening-up policies and modernization drive...In 1993 the State Economic Informationization Joint Meeting was initiated to lead the construction of a national network of public economic information. In 1997 the Ninth Five-Year Plan for State Informationization and the Long-range Objective of the Year 2010 was formulated, which listed the Internet as part of the state information infrastructure, and set the goal of pushing forward national economic informationization by vigorous development of the Internet industry. In 2002 the Specialized Plan for Informationization in the Tenth Five-Year Plan for National Economic and Social Development was promulgated, which defined China's priorities in this regard, including promotion of e-government, vigorous development of software industry, strengthening of development and utilization of information resources, and acceleration of the development of e-commerce. In November 2002 the 16th National Congress of the Communist Party of China (CPC) set the goal of “using IT to propel industrialization, which will in turn stimulate IT application, blazing a new trail to industrialization.” In November 2005 the State Informationization Strategy (2006-2020) was formulated, which further clarified the priorities of Internet development as promoting national economic informationization while adjusting the economic structure and
transforming the patterns of economic growth; building e-government while enhancing the capability of governance; and spurring the informationization of social services while building a harmonious society.

In March 2006 the National People's Congress (NPC) reviewed and adopted the Outline of the 11th Five-Year Plan for National Economic and Social Development, which envisaged the speeding up of the integration of the networks of telecommunication, radio, television and the Internet, to build the next-generation Internet and accelerate its commercial application. In April 2007 the Political Bureau of the CPC Central Committee decided to build up a cyber culture industry and the production of relevant facilities. In October 2007 the 17th National Congress of the CPC developed the strategy of "developing a modern industrial system, integrating IT application with industrialization, and turning scale-oriented industries into strength-oriented industries." In January 2010 the State Council decided to accelerate the integration of the networks of telecommunication, radio, television and the Internet, so as to promote the development of the information and culture industries.” 89

In order to achieve success, PRC has to focus on developing and perfecting seven IT areas, namely ICT and ICT Industries (Manufacture, Service); ICT Applications (E-Gov, E-Commerce); Information Resources (Content); Information Infrastructure (Network); Information Security; Talents (All Kinds) and Laws, Regulations, Standards, Standards, Standards,

89 “China has 45,000 government Internet portals: white paper,” Xinhua, June 8, 2010.
Specifications (p. 4). In terms of leadership, from the very beginning, informatization initiative is led Vice Premier, Leading Group of National Informatization (1999 to 1998), within the CCCPC and State Council Informatization officers with Advisory Committees in Administration, Policy, Security, Application, E-Government, Secretariat.


As of 2009, China had established more than 45,000 government Internet portals. 75 central and state organs, 32 provincial governments and 333 prefectural governments and over 80 percent county-level governments had set up their websites, providing various online services to facilitate people's work and life. "The building of e-government has substantially improved the work efficiency and transparency of government

---

90 “Process, progress and duration all the way from the industry society to the information society” and “All the means to accelerate the process from the industry society to the information society.” “Practice and Strategy of Informatization in China.” Presentation of Xiaofan Zhao Professor, Director General Department of IT Application Promotion, State Council Informatization Office, People’s Republic of China. 2006-10-18, Shanghai, China.
information." 91 White Paper on “The Internet in China” (2010) reports:

“Citing a sample survey, the paper said that in 2009 alone, about 230 million people in China gathered information using search engines, 240 million communicated through real-time telecommunications devices, 46 million received education with the help of the Internet, 35 million conducted securities trading on the Internet, 15 million sought jobs through the Internet, and 14 million arranged trips via the Internet. "In China, more and more people are collecting information, enriching their knowledge, establishing businesses and realizing their aspirations, and communicating to know each other better through the Internet." 92

**National Strategy**

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”. 93 China IT scholars have likewise observed that: “Investments in information goods and services are key sources of productivity

---

91 *Id.*

92 “China has 45,000 government Internet portals: white paper,” *Xinhua*, June 8, 2010.

93 On February 27, 2002, Chinese Premier Zhu Rongji 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.
improvements and economic growth. In postindustrial economies, the future seems to entail the development of a media-saturated society and an information-intensive economy.” 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, and military preparedness – are depending on CMC for efficient and effective operations.

On May 11, 2006, the State Council released its first State Information Development Strategy:


next 15 years are: providing information infrastructure nationwide; strengthening capacities of independent innovation of information technology; optimizing the information industry structure; improving information security; making effective progress on building more information-oriented national economy and society; establishing the new type of industrialization model; building a perfect national policy and system for the Informatization process; enhancing the capability of applying the information technology among the public.

In the Strategy, nine key aspects are emphasized: promoting Informatization of the national economy; popularizing e-government; establishing advanced Internet culture; pushing ahead social Informatization; popularizing information infrastructure; exploiting information resources more efficiently; improving information industry competition; building national information security system; improving people's ability in using information technology and cultivating more talents in information technology.” 95

**Computer crime**

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. 96 In

96 For details on types of computer attacks and vulnerabilities, see David Icove, Karl
other words, computers, particularly the Internet, facilitate criminality and have engendered a different form of crime.

**Computer crime defined**

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.” 97

According to Professor Parker’s definition, computer crime cases may involve computers in one or more of the following roles as: 1. Object such as destruction of

---

98 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.
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 nonexistent computers for intimidation or deception.99

**Focus and organization of book**

This book 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. It 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.

Chapter One: “Introduction” – providing the background of this study and information technology in China. In the main the chapter focuses on the development (strategy and policy), deployment (governance and civil society) and impact (utility and harm) of Internet on China’s society.

Chapter Two: “Researching into Cyberspace Governance in China” – explaining some research difficulties, data sources and limitations.

Chapter Three: “Internet in China” – outlining IT development and emergence of

99 Unless other specified, the terms including “computer crime”, “computer-related crime”, “computer abuse”, and “Internet crime”, are used interchangeably throughout this paper.
computer crime in China; the origin and development of Internet in China; and analyzing the disparate growth in the use of Internet.


Chapter Five: “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.

Chapter Six: “Cyberspace Governance with Chinese Characteristics: The case of Google vs. China” borrows Huntington’s “Clash of Civilizations” to explain the difference of approach between China and the United States over cyberspace free speech vs. control debate. The thesis here is that China and United States share little in common in history and culture, and expectedly now clashes over ideology and values over cyberspace governance. The best way to defuse the “clash of civilizations” is not to claim ones ideology, values and culture as superior, still less universal, but to accept other sovereign’s right to choose for themselves what a good life mean or entail.

Chapter Eight: “Conclusion” – first discuss the effectiveness comprehensive control and concludes with various recommendations in improving cyberspace governance and Internet regulation foster law and order in cyberspace in China.
Chapter Two
Researching into Cyberspace Governance in China

Conceptualization

Internet crime is the use of computer – Internet as instrumentality of crime or making computer–Internet as an object of crime. The are three basic characteristics of a computer crime: (1) acts which compromise the integrity, security, capacity and functionality of computer data processing system, such as hacking or denial of service. (2) the use of computer system to perpetrate traditional crime, such Internet theft, fraud and pornography. (3) the use of computer skills to perpetrate crime involving the production, processing or exchange of electronic data, such as virus attack.  

Causation

There are many factors contributing to Internet criminality:

“As a global communication system, the Internet cannot be entirely safe or secured. It is a hybrid system consisting of many ill-fitting components and weak connections. There are many vulnerable spots within and between the computer and Internet system waiting to be exploited for personal gain. It is thus easily subjected to attack at its weakest link, such as design faults or human

---

errors. On the other hand it is completely open and easily accessible to all, with little screening for users and few restrictions for use.”

Internet is full of unwholesome and immoral influences, such as PK (or Player Killing) games that invite the players to kill each other virtually with no personal remorse or moral responsibility. “Player killing”, Ganking or PKing, is non-consensual PvP resulting in a character's death. Some games offer "open PvP" (also sometimes called "world PvP"), where one player can attack another without warning anywhere in the game world. An aggressor attacks an opponent without agreement to any set of rules of engagement or combat.” 102 In order to attract customers, especially young ones who do not have (unsupervised) access to computer at home, the “Internet bars” offer up vices - sex, violence and game – to attract at risk youth. 103

**Difficulties with investigation**

There are many difficulties in investigating and prosecuting Internet crime. 104

First, there is no legislation or administrative regulation proscribing how Internet crime should be conducted, e.g., what and how to search and seize computer,105 where,

---

103 “China’s Internet Bar Association’s Self-Discipline Pledge,” *ChinaView* Dec. 11, 2009.
105 Whether to search individual computer vs. office vs. corporate networks for evidence
what and how to look for digital evidence; how to distinguish computer as an instrumentality vs. evidence of crime; how to preserve digital evidence, how to extradite computer criminals.

Second, there is no evidentiary rule governing the prosecution of computer crime, such as burden or standard of proof.

Third, there is a lack of computer literate police, prosecutor and judicial officer.

Fourth, victim awareness is a huge and insurmountable problem. Computer crimes cases are rarely discovered by the victims; (2) even if they are discovered, they are discovered long after the violation; (3) even if computer crimes are

of crime.

For instance, in child pornography cases, investigators should look not only for the graphic images, but also the associated communication and transfer programs that might have been used to capture, download, modify, view and produce the image. Programs and files such as e-mail attachments, original compressed files, news & file retrieval agents, browser programs, dial-up information, file captures, session logs and many others can have a wealth of valuable information. Associated computer evidence found in various computer files can and often will reveal the time, date, manner, location, email address history logs, web site, file transfer location, IP Internet address and other useful information.” Sergeant John J. McLean, “Basic Considerations in Investigating Computer Crime, Executing Computer Search Warrants and Seizing High Technology Equipment” 14th BILETA Conference: “CYBERSPACE 1999: Crime, Criminal Justice and the Internet” Monday, March 29th & Tuesday, March 30th, 1999. College of Ripon & York St. John, York, England.

In a bribery case, the use of computer to facilitate (conceal) a bribe vs. keeping bribery transaction records.

timely discovered, victims might not realize the extent of damages or degree of harm
done, initially or seriousness of loss in the aggregate.\textsuperscript{109}

Fifth, victim cooperation is a big obstacle. Computer crime victims often choose
not to report crime because they consider: (1) loss as minor;\textsuperscript{110} (2) police are not willing
or able to solve the crime;\textsuperscript{111} (3) nothing can be done; (4) it takes too much time and
effort; (5) it is not worth while to report due to business reasons.\textsuperscript{112}

Sixth, the occurrence of crime is separated by time and space to make
investigation impossible, particularly when the police are under resourced.

\textsuperscript{110} To a computer user, a malware attack often seems trivial and inconsequential, e.g., it
is a nuisance to put up with streams of unwanted ads.
\textsuperscript{111} Lee, a 24 years old graduate student is hooked on Internet gaming. One day he was
informed that he won a RMB 5,000 price. In order to claim the price he has to first pay
RMB 400 which he did. Lee did not get the price. He reported to the police. The police
told him that the case is a difficult one to investigate and refused to record it. A PSB
chief explained. First, street officers at a police post have little understa
n
\textsuperscript{112} U.S. Department of Commerce, National Institute of Standards and Technology
(NIST), “Computer Security Incident Handling Guide” NIST §3.3.3: “Identifying the
attacker can be a time-consuming and futile process that can prevent a team from
achieving its primary goal—minimizing the business impact.”
Seventh, the police lack the financial, technology, expertise\textsuperscript{113} and human resources to properly conduct a computer crime investigation. This is especially the case with sophisticated and complicated computer crime.

Eight, there are difficulties in establishing the true cost of computer crime for punishment, recovery and/or remedial purposes.\textsuperscript{114}

Finally, according to aid Wang Yongquan, a professor at the East China University of Political Science and Law: “But while China has made progress, the country can still improve its legal regime and technical capabilities to fight cybercrime. Law enforcement has been a problem in China.” According to another report on cybercrime in China: “Cybercrime happens a lot, but it's not discovered very often…Cybercriminals can be difficult to trace because they often hide behind remote IP

\textsuperscript{113} When conducting network search, it is best to rely on computer network specialist and local company computer staff who knows the ins and outs of the system configuration and data processing/storage routines.

\textsuperscript{114} J. Granick. “Faking it: Calculating loss in computer crime sentencing,” \textit{I/S: A Journal of Law and Policy for the Information Society}, Vol. 2(2):207–228 (2006). (“calculating losses from computer intrusions is a difficult endeavor because security incidents are characterized by intangible harms like interference with system availability and interference with the integrity of data.”) The real challenge is in fixing losses based on individual victim’s expectation and tolerance for loss and across incidents. There is a tendency to calculate prospective costs, e.g., security enhancement due to minor intrusion into vital data, more so than recovering tradition losses, e.g., forgoing of costly forensic investigation of a major breach in favor of moving business forward to avoid interruption of business.)
addresses…Low technical proficiency among Chinese police and court officials, especially in rural areas, can complicate evidence gathering and prosecution.” 115

**Characteristics**

The characteristics of computer crime are:

The cost of executing computer crime is low. All it takes is a computer and Internet access. In the case of China as the cost of computing drops and the income of people jump, computing is no longer limited the exclusive few. Computer is now a fixture in most homes and offices. Internet is accessible everywhere, even while on the run. Computer crime can be committed virtually by everyone, anytime and all places. The risk of detection for computer crime is low, usually less than 10%. The reach of computer crime is wide and fast. It guarantees high probability of success with multiple victims and sizable return. Computer crime is an intellectual, professional and white-collar crime. The criminals are technologically always one step ahead of the police. Computer crime is virtue and hidden from view. It is not easily detectable, even for computer experts, much less a regular user with little knowledge. For example, it takes hours, if not days to find the hidden malware code. The tracking crime and tracing of criminals is made difficult with millions of IP addresses world wide, many of which are kidnapped as zombie sites. One person or a computer can create enormous harm, worldwide, which take thousands of people and millions of dollars to ratify.


Research difficulties

Researching into cyberspace governance and Internet regulation¹¹⁶ in China is not easy, nor straightforward. This is particularly so before 1995 when there was little research into cyberspace governance. The situation improves substantially and progressively after 1995. However, the existing Chinese literatures show that there are more reporting on computer crimes cases and detailing of legislative measures than understanding the nature of the problem and impact of the regulations. A trip to the library shows that there are more descriptive account of the historical development and current state of regulatory framework, than philosophical debate, theoretical discussion and policy analysis on why and how best to deal with computer related crimes.

Currently, there are three major problems in the area of cyberspace governance and computer crime study in China. First, there is a lack of knowledgeable researchers. Second, there is a lack of systematic collection of computer crime cases in supporting analysis of content or data to document trend. Third, there is a lack of specialized research institution to conduct research in computer crime, especially in mounting cross-disciplinary investigation into other subject areas contributing to the causation or response to computer crime, such as electronics, computing science, criminology, ¹¹⁶

Though cyberspace governance and internet regulation reference different intellectual domains and requires separate investigation projects, i.e., the former is concerned with the overall control framework – philosophy, theory, policy, and strategy, the later is focused on particularly regulatory regime, methods, measures and practices – 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.
sociology, and history, etc.\textsuperscript{117}

Overall, there is a lack of scientific investigations, i.e., theoretically driven and empirically based research,\textsuperscript{118} on the subject of cyberspace governance, computer crime and Internet control in China.

Computer related crime came to China as an emerging techno-social-legal problem since late 20\textsuperscript{th} century with the availability of computers to the Chinese people and accessibility of the Internet to the general public.\textsuperscript{119} The first computer crime case in China was officially\textsuperscript{120} reported\textsuperscript{121} in 1986 and the Country was officially accessible to the Internet worldwide starting late 1994\textsuperscript{122}. The short history of Internet

\textsuperscript{117} For more detailed discussion on history and problems of cyberspace governance research in China, see Jiang Ping, \textit{Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)} (Beijing: Commercial Press, 2000), pp. 37-45.

\textsuperscript{118} In order to make any scientific research credible, theory and empirical data are important.

\textsuperscript{119} 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,” \textit{Communications of the ACM} (1999).

\textsuperscript{120} There is no computer crime legislation in 1987. Computer crimes were reported as regular theft.

\textsuperscript{121} 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. A similar case was reported in a different branch of the bank two months later. Chen, a bank computer operator, was successful in transferring the bank money to his designated account through unauthorized access to the database. See Yu Zhigang and Others, \textit{Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime)} (Jilin: Jilin renmin chubanshe, 2001), p.1.

\textsuperscript{122} 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
development\textsuperscript{123} and the few cases of computer crime reported\textsuperscript{124} 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 was a political concern, as evident by the joining hand of China Computer Safety Professional Committee and Ministry of Public Security, Computer Management and Supervision Bureau. Driven by the pragmatic nature of Chinese culture and can do spirit of the MPS, research activities have focused on setting safety standards, devising security measures, and implementing data protection. The research output is more geared towards securing e-platform for business and economic development. There are only a handful of active computer crime researchers, most of them in the private sector. For example, Jiang Ping is one of the very few experienced researchers who specialized in monitoring computer security and fighting computer related crime. Jiang’s research has provided a foundation for future researchers\textsuperscript{125} I will have more to say on his work in the later section.

Cooperation and the National Science Foundation of the United States. Thereafter China is officially recognized as a country with accessibility to the Internet and connected to the outside world with a full-functioning linkage.

\textsuperscript{123} 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. In case of any discrepancy between the Chinese report and its English translation, the local language version preempts.


\textsuperscript{125} 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 his work. More troublesome, his work is not scientific as much as it is an attempt to provide for independent research on the problem.
Generally, there is a lack of systematic and comprehensive Internet crime studies that is based on valid and reliable first hand data, such as computer crime victimization survey. \textsuperscript{126} Before 1995, there is no separate computer crime category to report, record, or classify a computer crime. This retarded academic research. \textsuperscript{127}

Currently, computer crime is not reported separately in annual PRC police reports. \textsuperscript{128} It is very difficult to single out cyber-crime specific cases among traditional crime records. There is no shortage of media accounts of computer (related) crimes. However, such accounts are not good measurement of nature, incident, prevalent, trend or distribution of crime. More significantly such media reports are usually compiled for propaganda purpose and/or to achieve socialist educational needs. \textsuperscript{129} 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. Department of Defense, Richard Power mounted an attack on 8,932 computer systems, as a test. It was found that only 19 of the managers reported such attacks upon discovery. \textsuperscript{130} China faces similar problems of dark

\textsuperscript{126} China conducted its first victimization survey in the early 1990s. The survey does not cover computer crime.

\textsuperscript{127} See MPS internal criminal statistic compilation, \textit{Gongan Neiqin Gongzuo Shouce (Police Administrative Manual)} (Beijing: Jingguan jiaoyu chubanshe, 1994). See also the relevant categories on statistics, \textit{Zhongguo gongan baike quanshu (Chinese Public Security Encyclopedia)} (Changchun: Jilin chubanshe, 1989).

\textsuperscript{128} See \textit{Procuratorial Yearbook of China (annual) (Zhongguo Jiancha Nianjian)}.

\textsuperscript{129} 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.

\textsuperscript{130} David Icove, Karl Seger, and William VonStorch, \textit{Computer Crime: A}
figures. Sophisticated and knowledgeable offenders working “undercover” with the code perpetrate computer crimes. In most cases the victims are not even aware of the crime. Many corporations, especially those in service sectors, such as banking and finance, are reluctant to report a cyber-crime case, for fear of jeopardizing their corporate image and credibility to their customers. In China, with state owned enterprises, officials might have to be held political responsible for computer crime.

The situation of data availability for Internet research has improved somewhat since 1997 with the promulgation of the “Interim Regulations of the PRC on the Management of International Networking of Computer Information” (Amended), and revision of Criminal Law of the PRC. Computer crimes are now formally recognized as a crime.

Chapter VI to Criminal Law of PRC provide for computer crime:

Article 285 states that “Whoever, in violation of State regulations, invades the computer information system in the fields of State affairs, national defense 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 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 to be that of E-Government year. This marked a concerted government effort to improve communication between the people and government agencies through Internet131. With this open campaign launched in 1999-2000, more and more cyberspace related information, including law, policy, regulation, criminal cases and control measures, are now readily available on government web.

Literature in Chinese

Before the web has become a popular media 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\textsuperscript{132} at The Chinese University of Hong Kong. There are several journals informing the early development of Internet research studies by Chinese scholars and practitioners\textsuperscript{133} before the 20\textsuperscript{th} century. In fact, most articles under review report on computer security, software and data protection, intellectual property right, and legal issues in E-Commerce. Occasionally there are isolated articles reporting on 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 1.

### Table 1 - Chinese Law Journals with Relevant Articles up to 2000

<table>
<thead>
<tr>
<th>Chinese Journal</th>
<th>Period</th>
<th>Publisher/Editorial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keqi Yu Falu (Science and Technology Law)</td>
<td>1992 to 1996</td>
<td>Zhongguo Kexue Qizhu Faxuehui (China Science Technology and Law Institute)</td>
</tr>
<tr>
<td>Jingji Yu Fa (Economy and Law)</td>
<td>1997 to 2000</td>
<td>Jingji Yu Fa Zazhishe (Economy and Law Publisher)</td>
</tr>
<tr>
<td>Fazhi Yu Jingji (Legal System and)</td>
<td>1998 to 1999</td>
<td>Quangxi Zhuangzu Zizhigu Fajiju (Legal System Bureau of Quangxi Zhuangzu)</td>
</tr>
</tbody>
</table>

\textsuperscript{132}“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](http://www.usc.cuhk.edu.hk).

\textsuperscript{133}For those articles that are in printed format without electronic copies, hard copies are filed with author.
<table>
<thead>
<tr>
<th>Journal/University/Affiliation</th>
<th>Year(s)</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xiandai Faxue (Modern Law Sciences)</td>
<td>1998</td>
<td>Xinan Zhengfa Xueyuan (Southwest University of Political Science and Law)</td>
</tr>
<tr>
<td>Falu Kexue (Law Science)</td>
<td>2000</td>
<td>Xibei Zhengfu Xueyuan (Northwest University of Politics and Law)</td>
</tr>
<tr>
<td>Zhongguo Lushi (Chinese Lawyer)</td>
<td>1999 to 2000</td>
<td>Zhonghua Quanguo Lushihui (China National Association of Lawyers)</td>
</tr>
<tr>
<td>Zhishi Changquan (Intellectual Property)</td>
<td>1999</td>
<td>Zhishi Changquan Zazhishe (Intellectual Property Publisher)</td>
</tr>
<tr>
<td>Falu Shiyong (Applying Law)</td>
<td>2000</td>
<td>Guojia Faquan Xueyuan (National Institute of Judges)</td>
</tr>
<tr>
<td>Xinfaqui Yuekan (New Regulations Monthly)</td>
<td>2000</td>
<td>Shanghaishi Jingjifa Yanjiuhui (Shanghai Research Institute on Law of Economy)</td>
</tr>
</tbody>
</table>

Most of the articles were written in 1999/2000. The first article touching on the subject was found in 1992 discussing the “Michelangelo” virus.\(^{134}\) Huang Guomin\(^{135}\), Wang Shizhou\(^{136}\), Zhao Bingzhi and Yu Zhigang\(^{137}\) are few of the pioneers in the initial

\(^{134}\) Guo Liben, “You ‘Michelangelo’ Bingdu Suoxiangqi De” (‘Reflection on ‘Michelangelo’ Virus’), *Keqi Yu Falu* (Science Technology and Law) No. 2 1992. Starting with the ‘Michelangelo’ virus incident, 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.

\(^{135}\) Huang Guomin, “Shilun Jiasuanji Fanzui” (On Crime by Computer), *Keqi Yu Falu* (Science Technology and Law) No. 3 1995. The article discusses the nature of computer crime 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.

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. As, there is not yet a regular journal published by Chinese scholars that specializes on computer crime, cyberspace governance, or Internet regulation in China, but one might be on the way. 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.” 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.

On April 14, 2004 Peking University Law School Internet Law Center was launched, supported by Yahoo Corporation and PKU Founder Group. “The mission of the

---

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

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

139 For a better understanding on Chinese gongan (public security) and research literature, see Kam C. Wong, Chinese Policing: History and Reform (Peter Lang, 2009). Chapter One.
Center is to communicate closely with the government and the relevant industry, to research on concrete legal problems and policy issues arising in the internet development home and abroad, and to bring out the project through positive interaction.” The Peking University Intellectual Property School and Internet Law Center jointly publishes the Internet Law Review, edited by Professor Jiang Ping.

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. 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, also provides valuable reference in analyzing the crime cases from criminology and Criminal Law perspectives.

Internet resources certainly are keys to any research work of cyberspace related subjects. In addition to the legal publishing agencies, such as the Bureau of

140 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).


142 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
Legislative Affairs of 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 (MII), the MPS, the China Police Daily Online, and the China Police Report. 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 PSBs of various provinces report selectively report computer crime cases on their web. 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 a great asset to Internet crime research. This corner is dedicated to reporting on the latest development in Internet crime and control back to late 2000. Local news agencies, such as the People’s Research Guide and Selective Annotated Bibliography”, 88 Law Libr. J. 402 (1996)

Daily\textsuperscript{149} and Xinhua News Agency\textsuperscript{150}, are also very helpful in reporting cyberspace policy, Internet regulation and computer crime stories, online. 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.

\textsuperscript{149} Renmin Wang (People’s Daily Online) at \url{http://www.peopledaily.com.cn}.

\textsuperscript{150} Xinhua Wang (Xinhua News Agency Online) at \url{http://www.xinhuanet.com}.
Chapter Three

Internet in China

IT Development in China and Emergence of Computer Crime

Before we start our investigation into the computer crime situation in China, we need first to understand the development of information technology (IT) and its impact on Chinese society.

Since 1990s, China’s information technology (IT) industry 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, Minister of Information Industry "The information industry is expected to grow at annual rate of some 20 percent in the next five years."

151 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. Ordóñez de Pablos, Patricia; Lytras, Miltiadis D. (Eds.), The China Information Technology Handbook (Springer, 2009)

152 Before 1998, multiple government agencies were involved in 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.

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

154 Wu Jichuan, Minister of MII, made the remark at the opening ceremony of the 2000 International Forum on the Information Industry, jointly sponsored by the MII and Xinhua News Agency on 23-Aug-2000. See “China Attaches Strategic Importance to IT
In time the IT will become “a strategic industry and a new 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 leadership. In December 2001, at the first meeting of the national leading group on informationalization, 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 reflect current IT 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”.157

---

155 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.


157 See “President Urges Faster Development of Information Technology”, People’s
Looking ahead then, 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 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. …”

The first task in building flexible, efficient and safe information infrastructures is to address the exponential growth in the use of Internet in recent years. The Internet is viewed instrumental in transforming China after the World Trade Organization (WTO), particularly in the areas of education and economy development. A senior

---


159 China becomes an official member of the World Trade Organization (WTO) effective
economist in Beijing University, Zhou Qiren pointed out that “China is at a turning point and changing from a supply economy to a demand economy. The applications based on a broadband network will be a good way to stimulate people’s consumption.” 160

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 created conditions and provided opportunities in producing network-related criminal behavior. A commentary published on the front page of the People’s Daily on July 12, 2001 speaks to the anxieties and commitment of Chinese leaders about cyberspace governance, increasingly getting out of hand:

“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 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.\textsuperscript{161} In the following discussion, I will describe the milestones of Internet development in China.\textsuperscript{162} I will further 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\textsuperscript{163}**

*Technology development*

In September 1987, Professor Qian Tianbai sent China’s first e-mail “Crossing the Great Wall to Join the World” through Chinese Academic Network (CANET), a joint project by the Beijing Municipal Computer Application Research Institute and Karlsruhe University of former East Germany. This marks the beginning of Internet development in China. From day one, the Chinese government has been very supportive on Internet related research with a primary objective of boosting the country’s economy and technology advancement. During the period between 1988 and 1993, a majority of the network-related activities, in terms of project size and deliverables, took place in academic and research institutes. In December of 1988 Qinghua University campus network was linked to University of British Columbia, Canada with e-mail application.


\textsuperscript{162} “Evolution of Internet in China”, *China Internet Network Information Center (CNNIC)* at \url{http://www.cnnic.net.cn/evolution.shtml} (Visited on 27-Feb-2002).

\textsuperscript{163} “INTERNET DEVELOPMENT IN CHINA: ITS IMPACT ON POLITICS AND SOCIETY” Brookings Institute, Washington, D.C., Tuesday, December 4, 2007.
In September of 1989, College Network (CASNET) build a high speed network interconnecting Beijing University (PUNET), Qinghua University (TUNET) and the Chinese Academy of Sciences, as a way of establishing 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. In October of 1990 China’s Internet top domain name was officially registered as “CN” at DDN-NIC, a 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 all China e-mail communication worldwide.

The Institute of High-Energy Physics (IHEP) established the first direct link from China to the Internet in 1993, which is part of the Chinese Academy of Sciences (CAS). IHEP was 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 National Computing and Network Facility Center (NCFC) unit was designated as the network center and China’s top domain server, 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). This 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

164 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.
in 1993, funded by government and managed by the Chinese State Education Commission\textsuperscript{165}. CERNET is chartered to connect with all Chinese universities and institutes and all K12 schools. In 1994, China’s network (NCFC) was formally connected to 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 was officially recognized as a country with accessibility to the Internet worldwide.

In March 1993, Deputy Premier Zhu Rongji proposed the Golden Bridge Project to establish the National Public Economic Information Processing Network. In August of the same year, Premier Li Peng approved USD 3 million funding in support of the initial construction phase of the Golden Bridge Project. Since then, several more Golden Projects\textsuperscript{166} were introduced. They have contributed significantly to IT government and IT information sharing capacities. With the infrastructure in place, China launched a campaign in 1999-2000 for open government policy and E-administration, or E-

\textsuperscript{165} 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 \url{http://www.tprc.org/abstract/tan.txt}. According to CNNIC, CERNET work was started in 1994. There are few other events these two sources dated differently as a result of different interpretation of start dates of Internet projects. The historical dates cited should be read with care.
\textsuperscript{166} 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.
government on the web.\textsuperscript{167}

Between 1994 and 1995, the government took a number of steps to improve the Internet environment and create new web features at different sectors. For example, the country's first set of web pages was 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 (Cheung 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).

\textit{Censorship development}

Parallel to building up of IT infrastructure and capacity, 1996 marks the beginning of China’s conscientious and concerted efforts to regulate the Internet and govern the cyberspace by legal and other 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’s homepages and protest newsletters on the web.168

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. Since then, effort to control the Internet has been unrelenting, and controversial. As this June 30, 2009, New York Time report attests: 169

“Internet censorship in China is among the most stringent in the world. The government blocks Web sites that discuss the Dalai Lama, the 1989 crackdown on Tiananmen Square protesters and Falun Gong, the banned spiritual movement, among other Internet sites. In June 2009, the government announced that starting July 1 mandatory new software would be installed on all new Chinese-made computers that would effectively monitor a user's every move.170 After strong resistance at home and abroad, however, China indefinitely delayed enforcement of the rule requiring the filtering software's installation.171”


170 “The software is designed to filter out sexually explicit images and words, according to the company that designed it. Computer experts, however, warn that once installed, the software could be directed to block all manner of content or allow the government to monitor Internet use and collect personal information.” *Id.*

On Tuesday, February 27, 2007, Luo Gang, a renowned scholar of cultural studies and literary theory at Eastern China Normal University, gave a talk at UCLA’s Center for Chinese Studies on Internet and democracy in China:

“Luo divided the development of Internet usage in China into two phases. In 1996, when the Internet had just begun to be known to the public, the government -- underestimating the political energy the Internet could generate -- imposed few restrictions on it. On the contrary, in order to capture more public attention and interest, the government provided a vast amount of free web space to individual users….Starting from the year 2000, the government’s monitoring and control of the Internet have become much more rigid with the launching of a series of new laws and regulations. Several notable trends here include the posting censorship system, whereby Internet users are not allowed to post spontaneously on forums. All postings have to be reviewed by the web masters before they can reach a public readership. Key-word filtering acting as a censorship measure is another case that illustrates how information technology can assist totalitarianism. Politically sensitive words or terms are blocked out in search engine findings, and thus people are unable to obtain the information they want. Luo particularly mentioned the case of Google’s making compromises with the Chinese government in this regard so as to get access to a vast profit-generating market, compromises that violate the fundamental principle of equal information sharing that underpins the Internet’s promise for democracy. A common strategy of many web users for breaking through restrictions is to find proxy servers in foreign
countries that can connect with sites banned in China. To fight this, the government has disseminated many fake proxy servers with surveillance features that can collect private information of the users who attempt to log onto forbidden websites. Another highly controversial control, which was initiated in 2002 and was fully implemented starting in 2005, is the real-name system, which requires web users to register their actual name and obtain an officially assigned ID number before they can post on the Internet. The authorities claim that this policy is intended to curb the rampant practice of using fake names and disguised identity to spread groundless or false information, but it has provoked severe criticism among online communities for possibly prohibiting users from expressing their personal opinions on politically sensitive issues. The increasingly rigid control over the Internet culminated in the launching of a new law -- Regulations on Internet News Information and Service Management -- in 2005. These regulations defined the term “news information” in a broad and highly ambiguous way. The regulations not only limit the authority to distribute news information to a very limited number of websites, but they also define the posting of commentaries on the Internet as a form of news distribution. This has placed many websites at risk for allowing users to post comments on current affairs without restriction and therefore will oblige web managers to estimate the risks involved in allowing daring comments to appear on the Internet. In July 2006, Century China -- a highly influential website among intellectual circles in China -- was forced to shut down by the Beijing City Bureau of Information Administration
for violating these regulations. This incident generated widespread
Internet discussion of the boundaries of governmental intervention and the
public sphere. 172

The PRC government, however, feel that censorship of the Internet is not only
necessary but legal and reasonable. Premier Wen Jiabao recently observed: “China’s
management of the Internet is consistent with established international practice. We
exercise our control of the Internet according to our laws. We also maintain that the
industry should exercise more self-discipline.” 173

Chinese state authority try to weed out corrupting, dissenting and subversive
speech from the Internet by establishing a sophisticated system of blocking and filtering,
with the help of foreign experts and international corporation. 174 The system is called
"Golden Shield" (Jin Dun) or more commonly "The Great Firewall of China." 175 The
system works on several levels: (1) Service Providers (ISPs) inspects for unwanted
content and “Golden Shield” filters out disagreeable materials and proscribed URL.

172 “The Internet in China: A Force for Democracy or Oppression?” UCLA Center for
http://www.international.ucla.edu/china/article.asp?parentid=67152
CHINA MORNING POST, Mar. 15, 2006, at A5
174 “Race to the Bottom: Corporate Complicity in Chinese Internet Censorship,” Human
Right Watch. August 9, 2006.
175 Id.
(2) Internet Content Providers (ICPs) engage in self-censorship or risk losing their licenses. This is known as “third party policing”\textsuperscript{176}. (3) Public Security Bureau is on the lookout for offensive content, e.g., search computer for incriminating evidence.\textsuperscript{177}

Some of the key milestone of Internet censorship from 2003, include:

On 20 June 2003, Internet activists and journalists were able to force the government, through Internet uprising, to abolish the Custody and repatriation procedure and replaced it with “Measures for Assisting Vagrants and Beggars with No Means of Support in Cities”, by providing care for poor beggars or homeless persons.\textsuperscript{178} The uprising was also instrumental in establishing a Standing Committee of the National People's Congress – Constitutional Committee.

On July 11, 2003, the PRC government for first time granted licenses to open nation-wide Internet cafe chains.\textsuperscript{179}

On April 20, 2004, Shi Tao, 37, head of the news division at the Dangdai Shangbao (Contemporary Business News) in Changsha, Hunan province, attended a staff meeting where the Chinese Communist Party (CCP) Central Propaganda Bureau document Number 11 "A notice concerning the work for maintaining stability" (关于当

\textsuperscript{176} Lorraine Green Mazerolle, Janet Ransley, \textit{Third Party Policing} (Cambridge University Press, 2006)

\textsuperscript{177} “Race to the Bottom: Corporate Complicity in Chinese Internet Censorship,” Human Right Watch. August 9, 2006.


The document warned journalists not to interview and report on overseas pro-democracy Chinese dissidents returning to mainland China during the 15th anniversary of the Tiananmen Square Protests of 1989 on June 4. News media were also asked not to report on Falun Gong or people calling for politico-social change. That night Shi sent a brief of the document to Asia Democracy Foundation with Yahoo mail. Beijing State Security Bureau instructed Yahoo! To release information about Shi with the following letter: “Your office is in possession of the following items relating to a case of suspected illegal provision of state secrets to foreign entities…” Yahoo disclosed Shi’s identity and communication to Beijing State Security Bureau. On November 24, 2004 Shi was arrested and tried for “illegally providing state secrets overseas” under Article 111 of the People's Republic of China (PRC) Criminal Law on April 27, 2005. He was sentenced to 10 years imprisonment, with appeal denied on June 2, 2005. 181

Shi’s lawyer, Guo Guoting (郭国汀), famous for taking human rights cases, objected to Shi’s arrest. He was put under house arrest with his license to practice law suspended for one year by Shanghai’s Department of Law.

The incident raised concerns and issues around the world regarding Yahoo!’s business ethics and social responsibility. Reporters Without Borders criticized Yahoo! for acting as a “police informant”. The United States Congress held a hearing on the issues with Yahoo!, Google, and MSN, etc. In August 2007, Congress asked Yahoo! founder Jerry Yang to testify before Congress. On August 28, 2007, the World

---

181 The Case of Shi Tao (师涛) EastSouthWestNorth
http://www.zonaeuropa.com/20050501_1.htm
Organization for Human Rights USA sued Yahoo! for allegedly providing information (email and IP address) of Shi Tao and Wang Xiaoming to the Chinese government.

In the summer of 2005, the PRC purchased over 200 customized routers from Cisco Systems with technical assistance. The equipment and expertise allowed the PRC government to conduct more advanced technological censoring of Internet traffic.182

On October 18, 2005, the PRC government restarted its policy of blocking access to Wikipedia.183 Wikipedia was blocks twice, both in 2004, due to sensitive subjects, i.e., Taiwanese independence and the Tiananmen Square Protests of 1989.184

On February 14, 2006, a group of former senior Communist party officials in China criticized the Internet censorship, stating that strict censorship may "sow the seeds of disaster" for China's political transition.185 The petition letter reads:

“At the turning point in our history from a totalitarian to a constitutional system, depriving the public of freedom of speech will bring disaster for our social and political transition and give rise to group confrontation and social unrest," the letter said. "Experience has proved that allowing a free flow of ideas can improve stability and alleviate social problems."186

186 Id.
In February 2006, Google agreed to obey Chinese law in blocking websites deemed offensive to Chinese government. It installed new search engines that would screen out sensitive words, like Falun Gong or "Tibet." 187

On March 8, 2008, two popular Chinese blogs shut themselves down voluntarily to make a case against Western bias. In announcing their shut down, the blogs made the following statement: “Due to unavoidable reasons with which everyone is familiar, this blog is temporarily closed.” Within hours, Western media reported foul play by Chinese authority causing the shut down. 188 The two blogs use this incident to show that the West is prone to attaching Chinese censorship in cyberspace without investigation or factual support in each and every case.

In May 2006, Chinese Internet Hotmail users encountered difficulties. Again, many foreign media speculated it was linked to Chinese Internet censorship, without any evidence.189

In July 2006, researchers at Cambridge University claimed “not only to have breached the Great Firewall of China, but have found a way to use the firewall to launch denial-of-service attacks against specific Internet Protocol addresses in the country.”190

On January 24, 2007, Chinese state media reported that Hu Jintao had vowed to

"purify" the Internet.\footnote{91}

\section*{Social impact}

Beginning 2001, CASS began scientific survey on Internet in China. The first one (2001) was conducted in Beijing, Shanghai, Guangzhou, the largest three cities, and Chengdu and Changsha, two provincial capitals. The last (4th) survey was in 2007: “Surveying Internet Usage and its Impact in Seven Chinese Cities.”\footnote{92} The survey was conducted in Beijing, Shanghai, Guangzhou, Chengdu, Changsha, Xi’an and Shenyang.

\section*{The key findings of the survey are:}\footnote{93}

\section*{Perception and attitudes toward the Internet}

(1) Chinese Internet users perceive the Internet significantly more positively than do non-users.

(2) All agreed that “Much of the Internet content is not suitable for children.”

(3) Internet users having greater trust in online content than non-users. However, trust of Internet users have declined significantly.

(4) More than 80 percent of all those surveyed believe that it is necessary or very necessary to have certain types of Internet content controlled, and increasing.

(5) Porn, violence and junk mail remain of highest concern.

\footnote{91} "China's Hu vows to "purify" Internet," \textit{Reuters} January 1, 20004.  
\footnote{92} “Surveying Internet Usage and its Impact in Seven Chinese Cities,” Center for Social Development, Chinese Academy of Social Sciences (November, 2007)  
\footnote{93} The previous surveys were conducted in 2001, 2003 and 2005.  
\footnote{93} Findings extracted verbatim from CASS report (2007).
(6) There was a steep increase in the percentage of respondents who felt that political content should be controlled—from 8 percent in 2005 to 41 percent in 2007.

(7) 84.8 percent of all respondents feel that government should be responsible for Internet management and control.

**Internet Adoption**

(1) As in the previous surveys, the Internet remains mainly used by young, well educated and urban males.

(2) Despite the differences in economic development across the cities surveyed, all had a penetration rate of about 50 percent.

(3) Among non-users, more than 60 percent had some online experience (drop-out users).

**Internet Usage**

(1) Due to inexpensiveness, 81 percent of Internet users go online from home using a broadband connection.

(2) Only 32 percent are going online at an Internet café (often in addition to their home, work or school connections). Internet café users are mainly young males with low incomes.

(3) Despite the common belief that Internet cafes are mainly used for entertainment purposes, the survey found that information seeking and chatting are the most frequent online activities at cafes.

(4) A significant increase in duration and frequency of use is observed, probably due to the establishment of inexpensive monthly access fees.
(5) Heavy users (those who spend more 4 hours online every day) are predominantly based in the main metropolitan cities of Beijing, Shanghai and Guangzhou.

(6) The Internet in China is mainly used for reading news (mainly infotainment), seeking entertainment (music, movies and games) and communicating with others (via instant messaging or email).

(7) However, search engine use has increased significantly from 43 percent in 2003 to 79 percent in 2007, suggesting that the Internet is increasingly being used as an information and study tool.

**Political participation and government services**

(1) Compared with earlier surveys, people are still convinced that the Internet is a positive force for increased political participation and communication with government.

(2) While there is widely accepted view that government can serve people better by using the Internet, there is limited knowledge and use of e-government websites.

The CNNC survey statistics presented below will further help us to understand better the recent trends in Internet development and the potential problems or risks anticipated by the country leaders.

**Disparate growth in the use of Internet**

The tremendous growth in the numbers of Internet users since 1997 is far beyond the imagination of the world including IT experts, businessmen, scholars and the Chinese
According to the latest survey report released in July 2009\textsuperscript{194} by the China Internet Network Information Center\textsuperscript{195} (CNNIC)\textsuperscript{196}, there was a total of 33.7 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.\textsuperscript{197} This has increased to 338

\textsuperscript{194} The 24\textsuperscript{th} semi-annual “Statistical Report on Internet Development in China” (July 2009) (used to be called “The Semiannual Survey Report on the Development of China’s Internet (January 2002)”) was published by the China Internet Network Information Center (CNNIC) in July 2009.

\textsuperscript{195} 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. 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; 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.

\textsuperscript{196} 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).

\textsuperscript{197} The CNNIC surveys and reports remains to be the most authoritative data source

Since CNNIC is an authorized agency by Chinese officials, some parties may challenge the credibility of the survey reports. However, overall, people are in agreement with the rapid growth and the number of Internet users in China. Internet growth in China is the largest among nations in the Asia Pacific region. As of 2001, China eclipsed USA in Internet use in February of 2008: 220 vs. 216 million.

According to the Report, China has 12.54 million computers linked to the Internet with a bandwidth of 7,679.5M. Table 1 provides a summary of the annual growth in the number of Internet user, computer host, “.CN” domain name, “WWW” website, as well 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).

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' 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).
as the total bandwidth from year 1997 to 2001, again 2009. 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. By 2009 Internet users, penetration and bandwidth width has all eclipsed 2001 by over 10 times.

Table 1 –CNNIC Statistics on the Development of China’s Internet (1997 to 2001)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet User (Million)</td>
<td>338 (13.4%)</td>
<td>33.7</td>
<td>22.5</td>
<td>8.9</td>
<td>2.1</td>
<td>0.62</td>
<td>1.0</td>
</tr>
<tr>
<td>Internet Penetration (Million)</td>
<td>338 (25.5%)</td>
<td>33.7 (2.6%)</td>
<td>22.5 (1.7%)</td>
<td>8.9</td>
<td>N/A</td>
<td>2.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Computer Host (Million)</td>
<td>205.03 (13.1%)</td>
<td>12.5</td>
<td>8.92</td>
<td>3.5</td>
<td>0.747</td>
<td>0.299</td>
<td></td>
</tr>
<tr>
<td>“.CN” Domain Name</td>
<td>13.5 (-4.5%)</td>
<td>127,319</td>
<td>122,099</td>
<td>48,695</td>
<td>18,396</td>
<td>4,066</td>
<td></td>
</tr>
<tr>
<td>“WWW” Website</td>
<td>2.876 (16.8%)</td>
<td>277,100</td>
<td>265,405</td>
<td>15,153</td>
<td>5,300</td>
<td>1,500</td>
<td></td>
</tr>
<tr>
<td>Broadband User (Penetration) (Million)</td>
<td>320 (94.3%) (3.7%)</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Bandwidth (Million)</td>
<td>640,286.67 (16.8%)</td>
<td>7,597.5</td>
<td>2,799</td>
<td>351</td>
<td>143.2</td>
<td>25.4</td>
<td></td>
</tr>
</tbody>
</table>

199 Statistical Report on Internet Development in China (July 2009), CNNIC.
200 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.
201 Internet Protocol (IP) address
(Source: CNNIC)

Table 2: Internet Usage and Population Statistics:

<table>
<thead>
<tr>
<th>YEAR</th>
<th>Users</th>
<th>Population</th>
<th>% Pen.</th>
<th>Usage Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>22,500,000</td>
<td>1,288,307,100</td>
<td>1.7 %</td>
<td>ITU</td>
</tr>
<tr>
<td>2001</td>
<td>33,700,000</td>
<td>1,288,307,100</td>
<td>2.6 %</td>
<td>ITU</td>
</tr>
<tr>
<td>2002</td>
<td>59,100,000</td>
<td>1,288,307,100</td>
<td>4.6 %</td>
<td>ITU</td>
</tr>
<tr>
<td>2003</td>
<td>69,000,000</td>
<td>1,288,307,100</td>
<td>5.4 %</td>
<td>CNNIC</td>
</tr>
<tr>
<td>2004</td>
<td>94,000,000</td>
<td>1,288,307,100</td>
<td>7.3 %</td>
<td>CNNIC</td>
</tr>
<tr>
<td>2005</td>
<td>103,000,000</td>
<td>1,289,664,808</td>
<td>7.9 %</td>
<td>CNNIC</td>
</tr>
<tr>
<td>2006</td>
<td>137,000,000</td>
<td>1,317,431,495</td>
<td>10.4 %</td>
<td>CNNIC</td>
</tr>
<tr>
<td>2007</td>
<td>162,000,000</td>
<td>1,317,431,495</td>
<td>12.3 %</td>
<td>CNNIC</td>
</tr>
<tr>
<td>2008</td>
<td>253,000,000</td>
<td>1,330,044,605</td>
<td>19.0 %</td>
<td>CNNIC</td>
</tr>
<tr>
<td>2009</td>
<td>338,000,000</td>
<td>1,338,612,968</td>
<td>25.3 %</td>
<td>CNNIC</td>
</tr>
</tbody>
</table>
Table 3: Internet Users in China
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).

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. There was a trend fold growth of Internet users between 2009 and 2001 alone. The growth in Internet usage and penetration is possibly due to reduction in cost of personal computers, lower rate in accessing the Internet, growing affluence of people, and variability of websites available.

The popularization of Internet causes concern to the communist leaders who are used to controlling the media and message. From the beginning, the media is the mouthpiece of the CCP. Now, more westernized thoughts and “polluted” culture are
freely available on the www, especially from websites overseas. This has a great impact on to the young and less educated, and other less discriminate audience. This poses a challenge to the one-party ruling position of CPC.

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. The trend is also clear. Internet users are becoming younger. The number of users below age 18 surged from only 2.4% in 1999 to 15.3% in 2001, and again 33.9% in 2009. This presents one of the major challenges to the Chinese leaders as the teenagers are typically more energetic, with much spare time, curious, fast learners and inexperienced. They are easily led to try on new things on Internet without knowing that they have broken the law, worse being led astray. In 2008, Internet addiction became an official mental disease recognized by the Beijing Department of mental health.\textsuperscript{202} The symptoms of Internet addiction includes:\textsuperscript{203}

“Symptoms of addiction included yearning to get back online, mental or physical distress, irritation and difficulty concentrating or sleeping. The definition, based on a study of more than 1,300 problematic computer users, classifies as addicts those who spend at least six hours online a day and have shown at least one symptom in the past three months.”\textsuperscript{204}

\textsuperscript{202} Jane Macartney, “Internet addiction made an official disorder in China,” \textit{The Times}, February 11, 2008. (“Beijing’s Health Ministry is expected to adopt a new manual on internet addiction next year, based on the research of Chinese psychologists. It will recognise the condition as similar to compulsive gambling or alcoholism.)

\textsuperscript{203} “China issues first definition of Internet addiction,” \textit{Xinhua}, November 11, 2008.

\textsuperscript{204} \textit{Ibid.}
Internet addiction in China is on the rise. In 2009, according to survey by China Youth Association for Network Development (CYAND), there are 29 million addicted, twice that of 2005. The survey was conducted every two years. The 2010 survey was conducted with 7,000 respondents aged 6 to 29 in 30 provinces, municipalities and autonomous regions from last September to January. “As many as 15.6 percent of netizens aged 18 to 23 were Internet addicts, accounting for the largest percentage compared with other age groups, while 8.8 percent of Internet users aged 6 to 12 were web addicts, the lowest percentage, according to the survey. "Compared with 2005, the number of Internet addicts’ aged 18 to 23 has increased, while addicts in the 6-12 age group have decreased. It shows that the years of efforts by the authorities to try and prevent children from getting hooked are effective." A study in 2009, shows, as compared to the United States Internet addiction in China is more serious than in the United States. In a 2007, a survey by Chinese Academy of Science found that Chinese youth get addicted to the Internet younger. 13% of the Chinese youth under 18 played or chatted online for more than 38 hours a week. In order to protect the youth, Ministry of Industry and Information Technology (MIIT) launched the Green Dam Youth Escort (绿坝·花季护航 or Lǜbà·Huājì Hùháng) program to take effect on July 1, 2009.

205 Young Internet addicts on the rise
206 Ibid.
207 Ibid.
“In order to build a green, healthy, and harmonious online environment, and to avoid the effects on and the poisoning of our youth’s minds by harmful information on the internet, the Ministry of Industry and Information Technology (MIIT), Civilization Office of the Central Committee of the Communist Party of China (CPC), and Ministry of Finance, in accordance with the Government Procurement Law, have used CPC financial capital to purchase one-year exclusive rights to use “Green Dam Youth Escort” Green Online Filtering Software (hereinafter referred to as “Green Dam Youth Escort”) along with related services so that the whole society may use it free of charge. After comprehensive testing and pilot use, the software has been shown to effectively filter harmful content in text and graphics on the Internet and has already satisfied the conditions for pre-installation by computer manufacturers.”

The project was delayed and aborted due to domestic and foreign objections.

Juvenile crime statistics indicate that offenders are getting younger in recent years. Between 1997 and 2000, juvenile delinquency of age below 17 represents 5% (1997), 11% (2000) respectively of total crimes in the year. One of the major contributing factors is due to ignorance of the law and not fully understanding the implication of violations. A study of Internet crimes in Hexi area of Tianjin between January and

---

210 Chapter 8.
212 For detailed statistics, see Liu Tianfeng, “1991-2000 Woguo Qingshaonian Fanzui De Tedian Yuanyin Yu Yufang Duice (The Characteristics, Causes and Preventive
July of 2001 indicates that 75% of the offenders are below the age of 18.\textsuperscript{213} The CPC strongly believes that failure in setting and directing the behavior of this age group will lead to serious social and political problems. \textsuperscript{214}

The number of female users increases gradually from 12.3% in 1997 to 40% in 2001, and finally 47% in 2009. In the meantime, male users have been dropping from a high of 87.7% in 1997 to 53.7% in 2009. A possible reason is that increasingly more and more female citizens have access to educational opportunities and they are required to use computers at work. This is an emerging area drawing attention from policy makers in China when designing a controlled framework to fight against Internet crime.

The education level of users statistics indicate that the trend is moving gradually towards junior and high school level (67% in 2001) from college graduate level (50% in 1998), i.e., users are getting less educated. This will impact on the content and style of cyberspace e-discourse. Together with the movement in age group described above, education data indicates that most of the Internet users are young students with ability to learn and master the technology quickly and at ease. The challenge to the Party is to consider whether the young and un-educated is matured enough to handle the readily available inform from the www. In this regard, the Party and government have adopted a paternalistic stance in protecting the youth from unwholesome influence of the Internet. The nation agrees.

\begin{flushleft}

\end{flushleft}
### Table 4 – Profile of Internet Users in China (1997 – 2001, 2009)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet User (Thousand)</strong></td>
<td>380,000</td>
<td>33,700</td>
<td>22,500</td>
<td>8,900</td>
<td>2,100</td>
<td>620</td>
</tr>
<tr>
<td><strong>Gender Ratio:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>53.7%</td>
<td>60%</td>
<td>69.6%</td>
<td>79%</td>
<td>86%</td>
<td>87.7%</td>
</tr>
<tr>
<td>Female</td>
<td>47%</td>
<td>40%</td>
<td>30.4%</td>
<td>21%</td>
<td>14%</td>
<td>12.3%</td>
</tr>
<tr>
<td><strong>Age Group:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Below 18</td>
<td>33.9%</td>
<td>15.3%</td>
<td>14.9%</td>
<td>2.4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age 18 to 24</td>
<td>29.8%</td>
<td>36.2%</td>
<td>41.2%</td>
<td>42.8%</td>
<td>51.4%</td>
<td>41.9%</td>
</tr>
<tr>
<td>Age 25 to 30</td>
<td>NA</td>
<td>16.3%</td>
<td>18.8%</td>
<td>32.8%</td>
<td>27.1%</td>
<td>29%</td>
</tr>
<tr>
<td>Age 31 to 35</td>
<td>20.7%</td>
<td>12.1%</td>
<td>8.9%</td>
<td>10.2%</td>
<td>11.3%</td>
<td>13.2%</td>
</tr>
<tr>
<td>Age 36 to 40</td>
<td>NA</td>
<td>8.2%</td>
<td>7.1%</td>
<td>5.7%</td>
<td>4.9%</td>
<td>4.3%</td>
</tr>
<tr>
<td>Age 41 to 50</td>
<td>9.9%</td>
<td>7.6%</td>
<td>5.7%</td>
<td>4.5%</td>
<td>4%</td>
<td>6.8%</td>
</tr>
<tr>
<td>Above 50</td>
<td>5.7%</td>
<td>4.3%</td>
<td>3.4%</td>
<td>1.6%</td>
<td>1.3%</td>
<td>4.8%</td>
</tr>
<tr>
<td><strong>Education Level:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High School or Below</td>
<td>74.9%</td>
<td>10.2%</td>
<td>6.4%</td>
<td>3%</td>
<td>6.9%</td>
<td>n/a</td>
</tr>
<tr>
<td>Junior College</td>
<td>12.7%</td>
<td>56.9%</td>
<td>52.4%</td>
<td>45%</td>
<td>34.2%</td>
<td>n/a</td>
</tr>
<tr>
<td>College Graduate</td>
<td>12.4%</td>
<td>30.4%</td>
<td>38.8%</td>
<td>45%</td>
<td>49.6%</td>
<td>n/a</td>
</tr>
<tr>
<td>Master &amp; Above</td>
<td>NA</td>
<td>2.5%</td>
<td>2.3%</td>
<td>7%</td>
<td>9.3%</td>
<td>n/a</td>
</tr>
</tbody>
</table>

(Source: CNNIC)

---

215 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.

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

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

218 Education Level statistics for 1998 are as of 30-Jun. The grouping of year-end figures is not applicable.
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 under examination. 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 represent over one-third of the user population in 1997. It dropped significantly to 9.8% in 2001. 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. Table 5 summarizes the geographical distribution of Internet users between 2001 and 1997. In later discussion, we’ll observe how Internet crime and control activity are dispersed in various locations of China.

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Guangdong</td>
<td>10.4%</td>
<td>9.69%</td>
<td>12.94%</td>
<td>20.93%</td>
<td>8.3%</td>
</tr>
<tr>
<td>Beijing</td>
<td>9.8%</td>
<td>12.39%</td>
<td>21.24%</td>
<td>23.93%</td>
<td>36%</td>
</tr>
<tr>
<td>Shanghai</td>
<td>9.2%</td>
<td>8.97%</td>
<td>11.21%</td>
<td>4.34%</td>
<td>8%</td>
</tr>
<tr>
<td>Jiangsu</td>
<td>8%</td>
<td>5.43%</td>
<td>5.91%</td>
<td>5.31%</td>
<td>5.9%</td>
</tr>
<tr>
<td>Zhejiang</td>
<td>6.6%</td>
<td>6.62%</td>
<td>4.51%</td>
<td>4.63%</td>
<td>3.7%</td>
</tr>
<tr>
<td>Sichuan</td>
<td>5.2%</td>
<td>5.03%</td>
<td>3%</td>
<td>3.54%</td>
<td>2.4%</td>
</tr>
<tr>
<td>Shandong</td>
<td>4.3%</td>
<td>5.33%</td>
<td>5.19%</td>
<td>3.65%</td>
<td>4%</td>
</tr>
<tr>
<td>Hubei</td>
<td>4.3%</td>
<td>3.52%</td>
<td>3.32%</td>
<td>3.28%</td>
<td>6%</td>
</tr>
<tr>
<td>Liaoning</td>
<td>3.8%</td>
<td>4.66%</td>
<td>4.27%</td>
<td>3.64%</td>
<td>2.9%</td>
</tr>
<tr>
<td>Fujian</td>
<td>3.6%</td>
<td>3.59%</td>
<td>2.69%</td>
<td>3.07%</td>
<td>2.8%</td>
</tr>
<tr>
<td>Hunan</td>
<td>3.4%</td>
<td>3.97%</td>
<td>3.44%</td>
<td>1.69%</td>
<td>1.8%</td>
</tr>
</tbody>
</table>

219 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.

220 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.
There are 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 a 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, chat rooms and even porn websites. 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

---

(Source: CNNIC)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Henan</td>
<td>3.1%</td>
<td>2.33%</td>
<td>2.11%</td>
<td>2.14%</td>
<td>2.8%</td>
</tr>
<tr>
<td>Heilongjiang</td>
<td>2.8%</td>
<td>2.46%</td>
<td>1.66%</td>
<td>2.09%</td>
<td>1.4%</td>
</tr>
<tr>
<td>Hebei</td>
<td>2.8%</td>
<td>2.47%</td>
<td>2.59%</td>
<td>1.65%</td>
<td>2.5%</td>
</tr>
<tr>
<td>Tianjin</td>
<td>2.7%</td>
<td>2.53%</td>
<td>2.68%</td>
<td>1.68%</td>
<td>1.6%</td>
</tr>
<tr>
<td>Guangxi</td>
<td>2.6%</td>
<td>2.02%</td>
<td>1.34%</td>
<td>1.96%</td>
<td>1.3%</td>
</tr>
<tr>
<td>Anhui</td>
<td>2.5%</td>
<td>2.43%</td>
<td>0.97%</td>
<td>1.4%</td>
<td>2%</td>
</tr>
<tr>
<td>Jilin</td>
<td>1.8%</td>
<td>2.41%</td>
<td>1.5%</td>
<td>1.06%</td>
<td>0.9%</td>
</tr>
<tr>
<td>Jiangxi</td>
<td>1.8%</td>
<td>2.07%</td>
<td>1.14%</td>
<td>1.66%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Chongqing</td>
<td>1.6%</td>
<td>2.03%</td>
<td>1.9%</td>
<td>1.48%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Yunnan</td>
<td>1.5%</td>
<td>1.46%</td>
<td>0.63%</td>
<td>0.44%</td>
<td>0.8%</td>
</tr>
<tr>
<td>Shaanxi</td>
<td>1.5%</td>
<td>1.47%</td>
<td>1.96%</td>
<td>2.4%</td>
<td>1.2%</td>
</tr>
<tr>
<td>Xinjiang</td>
<td>1.3%</td>
<td>1.51%</td>
<td>0.47%</td>
<td>0.65%</td>
<td>0.1%</td>
</tr>
<tr>
<td>Gansu</td>
<td>1.3%</td>
<td>1.13%</td>
<td>0.57%</td>
<td>0.58%</td>
<td>0.5%</td>
</tr>
<tr>
<td>Shanxi</td>
<td>1.2%</td>
<td>1.34%</td>
<td>1.04%</td>
<td>1.03%</td>
<td>0.6%</td>
</tr>
<tr>
<td>Inner Mongolia</td>
<td>1.2%</td>
<td>1.21%</td>
<td>0.5%</td>
<td>0.39%</td>
<td>0.3%</td>
</tr>
<tr>
<td>Guizhou</td>
<td>0.6%</td>
<td>0.8%</td>
<td>0.46%</td>
<td>0.49%</td>
<td>0.4%</td>
</tr>
<tr>
<td>Hainan</td>
<td>0.5%</td>
<td>0.31%</td>
<td>0.49%</td>
<td>0.52%</td>
<td>0.3%</td>
</tr>
<tr>
<td>Ningxia</td>
<td>0.3%</td>
<td>0.48%</td>
<td>0.16%</td>
<td>0.25%</td>
<td>0%</td>
</tr>
<tr>
<td>Qinghai</td>
<td>0.2%</td>
<td>0.31%</td>
<td>0.08%</td>
<td>0.1%</td>
<td>0.1%</td>
</tr>
<tr>
<td>Tibet</td>
<td>0.1%</td>
<td>0.03%</td>
<td>0.03%</td>
<td>0.02%</td>
<td>0%</td>
</tr>
</tbody>
</table>

(Source: CNNIC)

pornographic websites, and less than 20% of them search for information. 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.

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 secure and their rights being protected by law, they will be less inclined to refuse engage in E-commerce. The Chinese government is making every effort in legislation in filling the gap.

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Internet Access Expenditure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At company expense</td>
<td>10.7%</td>
<td>14.15%</td>
<td>21%</td>
<td>26%</td>
</tr>
<tr>
<td>At personal expense</td>
<td>73.7%</td>
<td>63.37%</td>
<td>59%</td>
<td>45%</td>
</tr>
<tr>
<td>Both</td>
<td>15.6%</td>
<td>22.48%</td>
<td>20%</td>
<td>29%</td>
</tr>
<tr>
<td>2. Most Serious Concerns of Online Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security is uncertain</td>
<td>31.0%</td>
<td>31.20%</td>
<td>36.54%</td>
<td>n/a</td>
</tr>
<tr>
<td>Product quality, post-sales service and credibility of the manufacturer are uncertain</td>
<td>30.2%</td>
<td>32.03%</td>
<td>27.64%</td>
<td>n/a</td>
</tr>
<tr>
<td>Obstructed delivery channel</td>
<td>13.9%</td>
<td>9.86%</td>
<td>9.26%</td>
<td>n/a</td>
</tr>
<tr>
<td>Payment is inconvenient</td>
<td>11.8%</td>
<td>12.59%</td>
<td>17.68%</td>
<td>n/a</td>
</tr>
<tr>
<td>Unattractive price</td>
<td>6.3%</td>
<td>7.39%</td>
<td>7.78%</td>
<td>n/a</td>
</tr>
<tr>
<td>Information is unreliable</td>
<td>6.3%</td>
<td>5.91%</td>
<td>N/A</td>
<td>n/a</td>
</tr>
<tr>
<td>Others</td>
<td>0.5%</td>
<td>1.02%</td>
<td>1.10%</td>
<td>n/a</td>
</tr>
<tr>
<td>3. Willingness to Purchase Online</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The 24th Statistical Report on Internet Development in China (Report) published by China Internet Network Information Center (CNNIC) on July 16, 2009 shows that by June 30, 2009 China Internet keeps on growing at a fast pace, without easing up.

All three indicators—number of Internet users (338 million) (+13.4%), number of broadband users (320 million) (91.4% of all users) and registration volume of top-level domain names (12.96 million) are rising. Mobile Internet users have reached 155 million, accounting for 46% of all Internet users. This group of users grew by and 32.1% within six months.

CNNIC’s Report shows that the disproportionate Chinese Internet users use the Internet for entertainment (online music), information (search) and networking (e-mail).

### Internet usage in Chinese rural areas - 2007

On September 7, 2007, the China Internet Network Information Center (CNNIC) published “Survey Report on the Internet Usage in Chinese Rural Area”. This is the first rural utilization report by CNNIC. The findings of the report is instructive in highlighting the differences between urban vs. rural Internet use. Some of the more important findings are:

1. There is a clear, but narrowing, Digital Divide between urban and rural areas.
2. There were 37.41 millions Internet users in Chinese rural areas.
3. The Internet penetration rate is 5.1% over 737 million rural residents, as compared to that of 21% in urban areas.
(4) The penetration rate between rural and urban Internet use has narrowed. Internet penetration for rural areas in Dec. 2006 is only 3.1%.

(5) The problem with penetration is one of lack of computing resources. At yearend of 2006, there were only 2.7 computers for every 100 households in rural areas vs. 47.2 computers for urban areas.

(6) According to survey, the main reason not being connected is “have no facility”, which accounted for 39.5% of all non-users in rural areas vs. 26.6% urban areas.

(7) Most rural users (53.9% or one out of two) surfed online in Internet cafes vs. 37.2% in urban areas.

(8) Most rural people use the Internet for online entertainment, such as music, as with their urban counterparts.

(9) More specifically, Internet application in rural areas is not as advance as the urban areas:

(9.1) Online news reading: 66.5% (rural) vs. 81.5% (urban)

(9.2) Use of search engine: 65.8% (rural) vs. 78.4% (urban)

(9.3) Online music, games, TV/movies: 68.9%, 47.1% and 60.9% (rural) vs. 68.4%, 47.0% and 61.2% (urban).

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 have been used for criminal
purposes, both as a tool and object.
Chapter Four
Nature and Prevalence 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 heightened political concerns. Computer and Internet introduce various kinds of computer-mediated criminality and network-related social/political deviance into China. As a recent study (2007) shows, Chinese black market for illegal malicious ware websites and web ware is growing and menacing:

“The World Wide Web gains more and more popularity within China with more than 1.31 million websites on the Chinese Web in June 2007. Driven by the economic profits, cyber criminals are on the rise and use the Web to exploit innocent users. In fact, a real underground black market with thousand of participants has developed which brings together malicious users who trade exploits, malware, virtual assets, stolen credentials, and more. In this paper, we provide a detailed overview of this underground

223 Jianwei Zhuge, Thorsten Holz, Chengyu Song, Jinpeng Guo, Xinhui Han, and Wei Zou, “Studying Malicious Websites and the Underground Economy on the Chinese Web,” Reihe Informatik. TR-2007-011 (“Abstract: We substantiate our model with the help of measurement results within the Chinese Web. First, we show that the amount of virtual assets traded on this underground market is huge. Second, our research proofs that a significant amount of websites within China’s part of the Web are malicious: our measurements reveal that about 1.49% of the examined sites contain some kind of malicious content.”

black market and present a model to describe the market.”224

In this chapter, I will be describing the nature, prevalence and distribution of computer crime, as revealed by Chinese data sources and as understood by the PRC scholars, policy makers and law enforcers. 225

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.226 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.227 A similar crime was reported at a different branch of the bank two months later. A computer

224 Ibid.


226 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,” Stanford Law Review 48: 1367 (1996).

227 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.
operator of the bank, Chen succeeded in transferring the bank’s money to his designated account through unauthorized access to the database.\(^{228}\) 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 Zhejiang, was successful in withdrawing RMB1.61 million in cash from the bank deposits accounts by abusing his access privilege in the course of his duty.\(^{229}\) So far, the cases recorded were related to individual banking systems.\(^{230}\)

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.\(^{231}\) A yearly breakdown of the figures are summarized in Table 1 below.

**Table 1 – Statistics of Cybercrime in China (1998-2001)**

---


\(^{229}\) Ibid. Wei Min.

\(^{230}\) In historical context, no one has any money except the bank. More significantly, no one is using computer except the government, particularly the bank.

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:

First, the using of computer to make, copy and spread pornographic materials. Some pornographic CD’s and literature are sold on the net to make money. This category

232 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, MPS) 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.
accounts for over 50 percent, 2,000 odd cases, of all computer related crime under investigation in 2001.

Second, the commission of 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.

Third, a 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.

Fourth, the infringement upon citizens’ personal rights and democratic right, such as personal attack and libel through the Internet. In 2001, 186 such cases were investigated were criminal offenses, representing a rise of more than three times over that of previous year.

Fifth, more and bigger cases using Internet to jeopardize national security such as Falun Gong and national-splitists spreading messages in attacking CPC and Chinese government.

The above official statistics do not provide for a complete picture of the current status of Internet crime in China. However, it informs us that, from the perspective of the police authority, 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 a special section, Jingti: Wangluo Xianjing (Warning: Internet Trap), to counteract the rising trend in Internet criminality by reporting cases and offering warnings. 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.

Before we proceed, a word or two on Jiang and his data set. 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 are now dated. There is no comparable data set available. Second, the cases were collected from newspapers, hardly a reliable source of information, especially during the 1990s era. Particularly, computer crimes are first reported to the police before public release. The police report crime only when it serves their purposes, e.g., educational and mobilization reasons. 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.

Jiang had collected 185 typical cases of computer related crimes between 1986 and June 1999 of which 183 cases had recorded a known environment in committing the
crime\textsuperscript{233}. His analysis on the 183 cases is listed in the Table 2 below.

The figures show that 169 cases, representing over 90% of the Jiang’s total study, are computer crime committed over the network.

<table>
<thead>
<tr>
<th>Commission Environment</th>
<th>Stand alone Computer</th>
<th>Intranet</th>
<th>Extranet</th>
<th>Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Crime</td>
<td>14</td>
<td>123</td>
<td>8</td>
<td>38</td>
</tr>
<tr>
<td>Percentage of 183 Cases</td>
<td>7.65%</td>
<td>67.21%</td>
<td>4.37%</td>
<td>20.77%</td>
</tr>
</tbody>
</table>


In Jiang’s research into computer crime problems, he 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 (Table 3)\textsuperscript{234}

<table>
<thead>
<tr>
<th>Classification</th>
<th>Brief Descriptions of the Computer Crime Case</th>
</tr>
</thead>
</table>
| Pornography on Web | 1. On March 21995, the PSB 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 March 25 1995, the PSB 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 PSB 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

\textsuperscript{233} Jiang Ping, \textit{Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)} (Beijing: Commercial Press, 2000), p.79.

\textsuperscript{234} See Jiang Ping, \textit{Jisuanji Fanzui Wenti Yanjiu (Research into Computer Crime Problems)} (Beijing: Commercial Press, 2000), pp.138-149.
involved with issues in pornography and drugs.

4. In July 1995, the PSB of Nanjing arrested Gao, a major supplier of computer pornographics to Nanjing students of high schools, colleges and universities.

5. In April 1996, a company in Jiangsu 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 PSB of Beijing investigated an Internet site that had downloaded 70+ obscene photos and 14 e-magazines.

<table>
<thead>
<tr>
<th>Computer Virus</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>10. In 1999, China computers were attacked by viruses Maleesa and CIH propagated from outside networks.</td>
</tr>
<tr>
<td>11. In 2000, China computers were attacked by the virus “I Love You” propagated from outside networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial Frauds using Credit Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. In July 1995, Li and Wen from Heilongjiang used their credit card to overdraw over RMB10,000, with each transaction below RMB500, in various locations including Jinan, Tsingtao, Shanghai, Hangzhou, Ningbo, etc.</td>
</tr>
<tr>
<td>13. In December of 1998 the credit card section of a bank noticed that there were abnormal transactions in three closed accounts and reported the case to the PSB. After investigation, it was discovered that Sun, a program developer of the bank, has successfully planted 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.</td>
</tr>
<tr>
<td>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 by using a credit card with RMB200 deposit only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hacking Information Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>15. In October of 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.</td>
</tr>
</tbody>
</table>
| 16. In Feb. 1998, an information service provider (ISP) in Guangzhou lost access control twice for a 4-hours duration each. In turned out that out of curiosity and to show-off their skills, Lu and Yuan intruded into the
network by changing the password of the system server, and thus was able to take complete control of the entire network.

17. In Sep. 1998, a provincial library system was attacked by hackers. The homepage was unlawfully altered. The hyperlinks to other sites were also re-directed randomly. Such an intrusion had forced the library website to close down for 6 days.


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

Most of the crimes reported were in the finance sector. 54.05% of the cybercrime cases are related to the financial systems. Business enterprises followed with 32.97%. This rank order of Internet crime differs somewhat in 2001, when there was a huge jump personal computer use and abuse.

A majority of the principal offenders are educated youngsters who worked as computer operator (59.85%), system administrator (31.39%), or program developer (3.65%). The remaining 5.11% are students. Most of the accomplices are students (52.38%) or computer operators (38.10%). Most of the financial sector cases were perpetrated by insiders who have internal access to the computer network and corporate

---


236 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 make for many “motivated” offenders. Second, technologically, computer makes it easy to steal and conceal. Third, structurally, financial loss in public institutions (banking) cannot be hidden from public view for long.
information to accomplish the offense.

A majority of the principal offenders are university graduates (40.42%). Undergraduate and post-graduate students make up another 15% and 10.64%, respectively. Only 29.79% of the total have completed high school education level or below. This appears logical in as much as computer criminality requires a sophisticated knowledge in computing and mastering of technical know-how.

Only 117 cases have gender information. A review of such cases show that 91.45% of the principal offenders are male and 8.55% are female. However, it is female offenders have are increasing fast. The increase is due in part to an increase in growth in female Internet users, from 12.3% in 1997 to 40% in 2001.

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 Ph,D 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 book237 according to the structure of the Part Two, Specific Provisions, of the Criminal Law (1997).

<table>
<thead>
<tr>
<th>Criminal Law Chapter</th>
<th>Descriptions</th>
<th>Sample Case of Computer Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

237 Yu Zhigang and Others, *Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime)* (Jilin: Jilin Renmin Chubanshe, 2001)
<table>
<thead>
<tr>
<th>I</th>
<th>Crimes of Endangering National Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chen was a Taiwanese who worked for his uncle as a 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 the 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. He further sent 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)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>II</th>
<th>Crimes of Endangering Public Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Liu was a train station worked. He hated the management due job evaluation and housing allocation. Instead of working in the station, he engaged in Internet chat all day. One day, he met with a guy during Internet chatting. Liu ans the person expressed their mutual discontentment with the station management. Both subsequently planned to create a train accident with details agreed. Fortunately, the plot was uncovered by another Internet user who reported to the police. Both Liu and the guy was caught and prosecuted for committing crime endangering public security. (p. 137)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>III</th>
<th>Crimes of Disrupting the Order of the Socialist Market Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 manufacturing and selling similar products under its own brand name. The market competition between these companies 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. Huanyu was subsequently caught and prosecuted by public security authority. (p. 196)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IV</th>
<th>Crimes of Infringing Upon Citizen’s Right of the Person and Democratic Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 being corrupt to PSB, Procuratorate, and Anti-corruption Bureau. He made up a story saying that the manager received 100,000 yuan as bribe in the construction of factory building. As a result, the manager was suspended, pending investigation. Zhu was later prosecuted and charged with crime of calumny. (p. 292)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V</th>
<th>Crimes of Property Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yang was a staff of a stated-owned enterprise, which has successfully completed a research on a new product to be launch in 1998. All the research data of the new product was stored in the company computer system. Yang planned</td>
</tr>
<tr>
<td></td>
<td>Crimes of</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VI</td>
<td>Obstructing the Administration of Public Order</td>
</tr>
<tr>
<td>VII</td>
<td>Impairing the Interests of National Defense</td>
</tr>
<tr>
<td>VIII</td>
<td>Embezzlement and Bribery</td>
</tr>
<tr>
<td>IX</td>
<td>Dereliction of Duty</td>
</tr>
<tr>
<td>X</td>
<td>Servicemen’s Transgression of Duties</td>
</tr>
</tbody>
</table>

(Source: Yu Zhigang)²³⁸

In closing it is best to reference State Council’s White Paper: “Internet in China”

²³⁸ Yu Zhigang and Others, *Wangluo Fanzui Dingxing Zhengyi Yu Xueli Fenxi (Analyzing the Nature of Internet Crime)* (Jilin: Jilin Renmin Chubanshe, 2001)
on the current state of computer crime in China:

“Combating computer crime in accordance with the law. In recent years, computer crimes in China have been on the increase. The tendency of the combination of various traditional crimes and computer crimes has become gradually more obvious. Online fraud, online theft and other forms of crimes which encroach on the property of others are increasing rapidly. Crimes such as producing and spreading computer viruses, and computer and network hacking are increasing. Criminal activities such as disseminating obscenity, pornography and gambling are still pressing problems. PSB departments dealt with 142 computer crime cases in 1998, 29,000 in 2007, 35,000 in 2008 and 48,000 in 2009. In order to effectively combat computer crimes, the Chinese laws stipulate that criminal activities conducted by making use of the Internet or against the Internet shall be investigated and dealt with in accordance with the Criminal Law of the People's Republic of China; if such activities are not serious enough to constitute crimes, administrative punishment shall be meted out in accordance with the Law of the People's Republic of China on Punishments in Public Order and Security Administration and Measures on the Administration of Security Protection of the International Networking of Computer Information Networks.

239 The Internet in China (Beijing: Information Office of the State Council of the People's Republic of China, June 8, 2010)
Opposing all forms of computer hacking. Like other countries, China faces a severe challenge of online criminal activities such as computer hacking and viruses. China is one of the countries suffering most from hacking. According to incomplete statistics, more than one million IP addresses in China were controlled from overseas in 2009, 42,000 websites were distorted by hackers, 18 million Chinese computers are infected by the Conficker virus every month, about 30% of the computers infected globally. Chinese laws prohibit all forms of hacking. The Decision of the National People's Congress Standing Committee on Guarding Internet Security stipulates that acts deconstructing Internet security which constitute crimes, such as "intentionally inventing and spreading destructive programs such as computer viruses to attack the computer system and the communications network, thus damaging the computer system and the communications network," shall be investigated for criminal liability in accordance with the relevant provisions in the Criminal Law. Articles 285 and 286 of the Criminal Law of the People's Republic of China contain concrete provisions on the criminal punishment of illegal activities such as illegally obtaining data stored in or handled or transmitted by the computer information system, or providing destructive programs or tools for invasion and illegal control of computer information systems.”

\[240\] Id. “V. Protecting Internet Security”
Chapter Five
Cyberspace Governance in China

*China Policy towards cyberspace governance and Internet regulations*\(^{241}\)

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 Internet is to be tightly controlled and strictly regulated to

---

\(^{241}\) Deibert, R. (2010). China’s Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy, Canadian International Council China Papers Number 7, February 2010 (“Chinese Internet content regulation consisted of DNS (domain name) tampering, keyword filtering and Internet protocol (IP) blocking. DNS tampering works by interfering with the system that cross-references domain names with the numerical address associated with them. Users are directed to an invalid IP as if the site they requested did not exist. By contrast, IP blocking targets the numerical address. This type of blocking can cause major collateral filtering of unrelated content because different domain names can share the same IP address host. Keyword filtering targets the Uniform Resource Locator (URL) path (and, it can be suspected, increasingly the body of the web page as well) searching for banned terms. Upon finding one, the routers send what are known as “RST packets” that terminate the connection between sending and receiving computers, effectively penalizing that computer from making requests to the same server for an indefinite period of time.3 Users making requests for banned information receive an error message on their web browser, which appears to the user as if the information is not available or that there is something wrong with their Internet connection. In other words, users in China trying to access banned content do not receive a block page informing them that the content is officially filtered, as is the case in some other countries that censor the Internet. Filtering is centralized and largely consistent across each of the international gateways; no matter the ISP or café from which ones connects to the Internet in China, this gateway level of filtering is an unavoidable last line of defense.”)
forestall against any inappropriate and non-approved use of the Internet. 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. 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. The priorities on hand then and now are: (1) perfect regulation and control of Internet through legislation; (2) promote civilized and cultural (wenming) use of Internet; (3) enhance and participate in international cooperation in Internet control; (4) actively promote training and education of party


243 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 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.

244 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, (31 years old Yang Lihua 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 qingxiaoian 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.

245 Akin to development of ethical culture with the Internet users and community.
leaders and government offices to computer use and Internet. To date, Jiang’s statement at this policy meeting remains to the most representative and authoritative rendition of China’s official policy position on cyberspace governance.

Judging from Jiang’s statement and later government policy pronouncements on cyberspace control, political leaders, government officials and police executives in China are 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. 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 IT 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”.

The dilemma of cyberspace control is real. On the one hand, a slow growing economy will risk social and political instability, e.g., uneven distribution and relative deprivation in the midst of robust growth. On the other hand, uninhibited growth would result in loss of control. For example, Internet changes the nature and kind of

---

information available to the people. CPC believes in the need for information control, to promote government policy or educate the mass. In the past, the CPC and PRC government have dominated over all mass communication channels with a total control over public information distribution in China.

With the advent of Internet, the CPC and PRC government find it increasingly difficult, if not impossible, to control people’s access to information by way of CMC.\textsuperscript{247} Internet has totally transformed the means, content and patterns of communication in China. As a result, there are diversified opinions on the web, some of them challenge the CPC’s ideology and others undermine Chinese traditional morality. The open Internet structure presents a seemingly insurmountable challenge to a closed political system. From a political and cultural point of view, China as a nation, Chinese as a people and CPC as a Party have many reasons to regulate the free for all 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 Falun gong and other cults. …

\textsuperscript{247} June 4 and Falun gong are two good 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 across the nation.
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 …”.

**Felson’s Routine Activity Theory and Comprehensive Control in China**

China adopts a comprehensive control (“zonghe zhili”) framework to control cybercrime and regulate Internet. Comprehensive Internet control is influenced of the “routine activity model” by Marcus Felson and his associates (Cohen and Felson 1979; Cohen, Felson, and Land 1980; Felson 1983; Felson 1987; Felson 1992). 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”. Felson’s routine activity theory is immensely popular among researchers and police agencies in China.

Comprehensive control in China is an integrated scheme of crime control with

---


249 China is leaning towards Felson in two aspects. First, some scholars have come up with a Chinese Felson Theory. Second, the principles underscoring the Felson theory and PRC approach to crime are very similar.


251 See Li Wenyan and Others, Jisuanji Fanzui Yanjiu (Computer Crime Research) (Beijing: Zhongguo Fangzheng Chubanshe, 2001), pp. 5-6.
prevention as its core. Other crime control measures are built around prevention with education as a key component, followed by co-operations from local communities. The comprehensive control scheme echoes “Problem Oriented” policing. It treats incidence of crime not as an independent and standalone phenomenon. Instead it treats crime as an integrated social and economical problem to be dealt with as a whole, and at its roots.

The policy of comprehensive crime control approach in China could be traced to a document published some 20 years ago, namely: “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. The Decision was published for the purpose of creating a safe and orderly social environment to facilitate the state economic development plan.252

The Decision provides comprehensive control guidelines for maintaining social order, public safety and country stability, to ensure smooth progress in economic reform and socialist modernization. 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.253 The Decision espoused many of Felson’s routine activity theoretical principles.

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

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

primary role. Education in moral and legislation to the youth is emphasized.” – At its heart Felson’s theory is a pro-active prevention theory. This statement aims at reducing the number of motivated (Internet) offenders through moral education and parental supervision and communal surveillance of teenagers who are the prime users of Internet.

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 Internet crime opportunities through integrative and layered environmental control from (computer) design, e.g., “Green Dam” project to screen web access and personal precaution to secure against identity theft.

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 mobilize the public to act as guardians on the lookout for irresponsible Internet behavior, virtually within the web and physically at the Internet bars 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 through linking Internet activities with responsible persons, e.g., web master is being held responsible for web content.

The above directives inform us that the Chinese leaders are very serious in controlling the Internet with the deployment of a comprehensive control scheme and leaving nothing to chances. In terms of applying comprehensive control strategy to cybercrime, emphasis is put on educating the youngsters to the civilized use of Internet,
promoting legal awareness training for the public, and providing guardianship in the Internet. In 2002, a teleconference was jointly held by eight government agencies, including 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, to develop a nation-wide program to regulate and control the Internet, keeping it clean from malevolent information. At the meeting, the importance of a comprehensive approach was reiterated. Meeting participants are urged for quick and stern implementation regiment.254

Legal and Regulatory Regime

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. The PRC cyberspace regulatory scheme is described as follows by the White Paper on “Internet in China” (2010):

IV. Basic Principles and Practices of Internet Administration

China adheres to scientific and effective Internet administration by law, strives to improve an Internet administration system combining laws and regulations, administrative supervision, self-regulation, technical protection, public supervision and social education. The basic goals of China's Internet administration are to promote general and hassle-free

254 See “Eight Ministries Joint Conference on Special Program to Keep the Internet Clean from Malevolent Information”, Xinhua News Agency Online May 1, 2002.
Internet accessibility, and sustainable and healthy development, guarantee citizens' freedom of speech online, regulate the order of Internet information transmission, promote the positive and effective application of the Internet, create a market environment for fair competition, guarantee the citizens' rights and interests vested in the Constitution and law, and guarantee safety for Internet information and state security.

Protection of Minors, Law of the People's Republic of China on Punishments in Public Order and Security Administration and other laws are applicable in the case of Internet administration.255

Cyberspace regulatory scheme256

In the following section, I’ll discuss on how Chinese 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,257 revised and enacted on October 1, 1997, contains no clear definitions of Internet crimes. With the 1997 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 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 defense, 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.

Judicial Interpretations

A. Supreme People’s Court and the Supreme People’s procuratorate jointly released “Interpretations on the Application of Laws Concerning Criminal Cases of Using Internet, Mobile Telecommunication Terminals and Radios to Produce, Reproduce, Publish, Sell, and Disseminate Pornographic Electronic Information” (September 2004):

Article 1: Those using the Internet, mobile telecommunication terminals and radios to produce, reproduce, publish, sell, and spread obscene electronic information in order to gain a profit, and which fall into one of the following categories, shall be punished for committing the crime of producing, reproducing, publishing, selling, or disseminating obscene materials with the purpose of making a profit, as per section 1, article 363 of the criminal law:

A. Producing, reproducing, publishing, selling, or disseminating more than 20 video documents of obscene movies, shows and motion pictures.

B. Producing, reproducing, publishing, selling, or disseminating more than 100 obscene audio documents.

C. Producing, reproducing, publishing, selling, or disseminating more than 200 obscene electronic publications, pictures, articles and short messages.

D. Establishing a membership system, with over 200 registered members, to produce, reproduce, publish, sell or disseminate obscene electronic information.

E. Using obscene electronic information to collect advertisement fees, membership registration fees, or other fees, with an illegal gain of over 10,000 RMB.

F. Although not reaching any of the limits of categories A-E above, any action which falls
into more than two of the listed categories, and respectively exceeds half of the limits.

G. Causes grave consequences.

Any action that falls into one of the categories of section one and that uses chat rooms, BBS, instant telecommunication software, or e-mail shall be punished under section 1, article 363 of the criminal law for committing the crime of producing, reproducing, publishing, selling, or disseminating obscene materials with the purpose of making a profit.

Article 2: Any action that falls into one of the categories of section one, and that reaches five times any of the limits of categories A-F, shall be considered as having caused grave consequences. If it exceeds 25 times the limit, it shall be considered to have caused especially grave consequences.

Article 3: Whomever uses the Internet or mobile telecommunications not for profit, in order to produce, reproduce, publish, sell, and spread obscene electronic information, and who falls into one of the following cases shall be punished under section 1, article 364 of the criminal law for committing the crime of producing, reproducing, publishing, selling, or disseminating obscene materials:

A. Where the amount is over two times the limits listed in article one, section one, A-E.
B. Respectively reaches the standard of more than two of the cases listed in article one, section one, A-E.
C. Causes grave consequences.

Any action that falls into one of the categories of section one and that uses chat rooms, BBS, instant telecommunication software, or e-mail shall be punished under section 1, article 364 of the criminal law for committing the crime of producing, reproducing, publishing, selling, or disseminating obscene materials.
**Article 4:** Anyone who knowingly provides direct links to obscene electronic information on a website or webpage that he or she owns, manages or uses shall be convicted. The limit standards will be calculated according to the type of obscene electronic matter that is provided by link.

**Article 5:** Those directly in charge of or responsible for using, producing, reproducing, publishing, selling, or disseminating obscene electronic information through radio stations, with the purpose of making a profits, and which fall into one of the following categories, shall be punished under section 1, article 363 of the criminal law for committing the crime of producing, reproducing, publishing, selling, or disseminating obscene materials, with the purpose of making a profit:

A: Spreading information to over 100 people;
B. Making illegal profits of over 10,000 Yuan.
C. Causing grave consequences.

Actions that exceed five times the limits in A and B shall be considered as having caused grave consequences; if they exceed 25 times the limit they shall under section 1, article 363 of the criminal law be considered as having caused especially grave consequences.

**Article 6:** Whomever commits any of the crimes of the last five articles, and which falls into one of the following cases, shall be severely punished according to section 1, article 363 and section 1, article 364 of the criminal law:

A. Producing, reproducing, publishing, selling, or disseminating obscene electronic information containing specific descriptions of sexual activities involving minors under 18 years old.

B. Whomever knows that it is obscene electronic information containing specific descriptions of sexual activities involving minors under 18 years old but still provides
direct links on websites or webpage owned, managed or used by them.

C. Selling or spreading obscene electronic information or voice information to minors under 18 years old.

D. Forcing users to visit or download obscene electronic information by using destructive programs, target codes in order to modify the setting of a user’s computers.

**Article 7**: Whomever knows that others are committing the crime of producing, reproducing, publishing, selling, or disseminating obscene electronic information but still aides others by providing them with Internet access, server trust, Internet storage space, information transmission links, or accounting services. The people in charge and other responsible members shall be held as jointly liable.

**Article 8**: Selling or distributing obscene materials in the form of books and magazines, movies, video tapes, or audio tapes shall be punished according to The Supreme People’s Court’s Interpretation on the Application of Laws in Criminal Cases Concerning Illegal Publications.

**Article 9**: “Other obscene materials” in section 1, article 367 of the criminal law includes specific descriptions of sexual activities, lewd electronic information through Internet and mobile telecommunication terminals and voice information through radios. These include: video documents, audio documents, electronic publications, pictures, articles, and short messages. Electronic information and voice information through radio about physiological and medical knowledge are not obscene materials. Electronic literature and artworks of artistic value which involve sexual contents are not considered as obscene materials.

B. “Interpretation from the Supreme People’s Court and Supreme People’s Procuratorate on the Application of Law in Criminal Cases Concerning Gambling” (2005)
Article 2: Setting up gambling websites or working as an agent of such websites and receiving bets for the purpose of making profits are subjected to “Opening a gambling house” in article 303 of the criminal law.

Article 4: Whomever knows that others are gambling but still directly helps them by providing money, Internet access, communication services, or accounting services shall be convicted as an accomplice in illegal gambling.

Article 8: Materials and money used as bets, exchanged for chips or won through gambling are considered under the law as gambling capital. For gambling through computer Internet, the gambling capital can be calculated by multiplying the on-line bet or the winning points with the actual money it represents.

Regulatory 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. For example, the MPS issued a notice, on April 5, 1995 calling for actions 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 website and several Chinese dissident homepages and protest newsletters. 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 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 to regulate the Internet and govern the cyberspace using legal means while the Internet Content Regulation issued in 2000 establishes 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.259

In brief, this category of regulations controls 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 andExiting Channels for 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 security procedures to provide for computer

protection, such as access controls and administrative supervision. It was issued even before Internet access was freely available to most Chinese people. In 2000, a host of key regulations protecting state 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 was promulgated to ensure security for state secrets. The Regulations strengthen secrets administration within an 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 Secret. The Internet Security Decision further lists numerous acts if committed by or with computer systems and the Internet 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 is serious enough to constitutes a crime, it would be 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 summary administrative 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 such other laws. If a party uses the Internet to infringe on 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. They 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 MPS on January 29, 1996);

- *Notice on Strengthening the Administration of the Information Security in the International Networking of Information Networks* (Issued by the MPS on July 1, 1996);

- *Measures for the Protection of Security and Administration of International Connection of Computer Information Networks* (Issued by the MPS 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);


- *Measures for the Prevention and Control of Computer Viruses* (Issued by the MPS 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.\(^{260}\) CNNIC is the only authorized body to issue domain names in China. In an effort to provide for 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 the approval from the MII - Telecom Administrative Bureau no organizations or individuals can engage in domain name registration and related business and services.\(^{261}\) This category of regulations serves as an important mechanism for censorship of Internet website operators: to restrict creation of new websites and keep

\(^{260}\) See “Refreshing Your Understanding of the Internet,” *China Daily*, April 23, 2002

\(^{261}\) “Websites to Play the Name Game”, *China Daily*, November 12, 2000.
track of 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 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 Internet, and processing of commercial transactions via Internet. Regulations in these areas are has grown substantially in compliance with the World Trade Organization (WTO) agreements and to cope with international business needs.²⁶² 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

²⁶² 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 license from the Shanghai Municipal Industry and Commerce Commission. The regulation became effective on September 1, 2000. “City Tackles Lawless Net”, *China Daily*, September 3, 2000.
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 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);

- Regulations on Commercial Encryption (Issued by the State Council on October 7, 1999);\(^{263}\)

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

**Related regulations on electronic evidence in *Electronic Signature Law***

- **Article 5**: Any data message meeting the following requirements shall be regarded as satisfying the requirement for an original form as prescribed by laws and regulations: A. Data message that is capable of effectively representing the contents it specifies, and may be picked up for reference and use at any time; and B. Data message that can reliably ensure that the contents are complete and

\(^{263}\) Most of its overreaching provisions, though, were effectively rescinded in March 2000
unaltered from the original final document. Moreover, the integrality of the data message will not be influenced by adding any endorsements in the data message, and the transformation of forms that occurred during the course of data interchange, storage and display.

- **Article 6**: Any data message meeting the following requirements shall be regarded as satisfying the requirement for document conservation as prescribed by laws and regulations: A. Being capable of effectively representing the contents it specifies, and may be sourced for reference and use at any time; B. The format of the data message is the same as that when it is created, sent or received, or the format is different, but is able to accurately represent the contents of original creation, sending, or receiving; C. Being capable of identifying the addresser and addressee of the data message and the time of sending and receiving it.

- **Article 7**: Any data message may not be refused for being used as evidence only because it is created, sent, received or stored by ways of electronic, optical, magnetic, or similar means.

- **Article 8**: When examining the authenticity of any data message as evidence, the following factors shall be taken into consideration: A. The reliability of the methods for creation, storage or transmission of data messages; B. The reliability of the methods for keeping the integrality of the contents; C. The reliability of the methods for identifying the addresser; D. Other relevant factors.

**Law Enforcement**

The Supervision Bureau for Public Information Security of the MPS was formed in September 1998. It is a specialized unit responsible for policing the cyberspace in
China. Today, the MPS 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 municipalities 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 those who intrude into and damage computer-information system in accordance with law, and study and form polices in the prevention of computer crime. Since the establishment of the supervision bureau, a total of 6,889 cybercrime cases have been cleared between 1998 and 2001, roughly representing a clearance rate of 89% against 7,700 reported cases. Campaign style Internet bar raids are used to demonstrate MPS’ commitment to fight against the increasing crime in Internet bars. In 2007, there is renewed called for more stringent law enforcement against Internet bar. Bar owners who failed to

---

264 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).

265 “Internet Police First Appears in Shanghai” (“Wangluo jingcha” zai Shanghai liangxiang”) China Police Daily Online, June 30, 2001,

266 See “Wangluo Jingcha Shenshou Bufan” (Highly Competent Cyberpolice), China Police Daily Online, April 11, 2002.
check young patrons ID would be fined for the first offense, 15 days business suspension for a second violation and license withdrawn after three violations. In 2010 Chinese government has launched clean Internet bar especially for youth.

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, gambling, fraud, and infringement of copyright. Recently, the term “electronic heroine” is coined to depict the adverse impacts brought about by the Internet in an uncontrolled environment such as Internet bars.

269 For example, in April 2001, Yang Linhua and his wife set up a “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.
270 Net gambling is a growing concern to PRC police. PRC noted the growth of net-gambling company as a worldwide phenomenon. In 1996 there were only 15 net gambling companies 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, November 1, 2001.
Many parents and teachers are worried that kids are hooked by Internet due to easy and unsupervised access at 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 as a result of indulging in playing computer games for long hours, daily and continually for months.271 The monitoring and regulating efforts on Internet bars will continue as long as the juvenile are deemed easy prey and at risk with abusive Internet use. Back in late 2000, over 20,000 Internet bars and 12,000 computer games shops were suspended in a campaign to regulate the Internet services market.272 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 of 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.273


From time to time, the MPS will launch campaign style operations to deal with wholesome influence of the Internet, such as violence, pornography and gambling.\textsuperscript{274} For example,

In 2007 MPS launched a nation wide crackdown on Internet pornography, gambling and fraud.\textsuperscript{275} The crack down was launched to keep a healthy Internet environment and protect the juveniles from corrupting and undue influence of the web.\textsuperscript{276} Wu Heping, spokesman of the Ministry of Public Security, observed that 80 percent of juvenile delinquents have been lured into crime by "evil content" on the Internet “From the cases we cracked in recent years, we found a high proportion of young people who were found guilty of cheating, rape or robbery were using the Internet and were corrupted by online filth.”\textsuperscript{277} Such crackdowns are also part of a larger cultural war. They have been used to paint Western – US culture in a negative light\textsuperscript{278} to be resisted with all means.\textsuperscript{279}

The 2007 Internet “purification” campaign netted the following criminals. Zhang Xuhui from Xuchang City, Henan Province was arrested for setting up a "blue" website with more than 120 pornographic movies in October 2006. 5,600 netizens visited the site.

\begin{flushright}
\textsuperscript{274} Tini Tran, “China's Internet use rises along with growth of policing system,” \textit{AP}, December 30, 2010. \\
\textsuperscript{275} “Chinese police crack down on internet crimes,” \textit{Xinhua} April 13, 2007. \\
\textsuperscript{276} “Internet Violence, Porn Main Cause of Juvenile Crimes: Official,” \textit{Xinhua} April 19, 2007. \\
\textsuperscript{277} Id. \\
\textsuperscript{278} Id. \\
\textsuperscript{279} “Police crack down on porn sites with foreign proxies,” Xinhua, July 13, 2009. Westerners think that such measures are used to suppress dissenters and restrict freedom of speech. “The Porn Shield:Beijing's crackdown on obscenity online may be a cover for a broader suppression of dissent,” \textit{Newsweek} January 14, 2009. 
\end{flushright}
Zhang was sentenced to jail for 1 year with 1 year reprieve. Zhang Yuancheng from Jingzhou City, Hubei Province was prosecuted with operating two pornographic websites in 2006. The sites boasted 4,000 members with daily profit of RMB 10,000. Zhang Yuancheng was sentenced to four years in prison. Nanjing PSB, Jiangsu Province, arrested a 12 members prostitution ring which used the computer and Internet to promote their business. Finally Yangzhou City PSB, Jiangsu Province cracked down on on-line gambling involving RMB 4 billions.

In 2010, the MPS reported the following achievements in another year of crackdown of the net:

--- Around 44.37 million copies of illegal publications, including 981,000 copies of lewd content, 37.35 million pirated copies, some 3.93 million illegal copies of newspapers and magazines, among others, have been confiscated across China.

--- More than 16,000 cases, including over 10,000 ones of pirated publications, 1,669 cases involving pornography, and 371 cases involving fake journalists, news reports or media outlets, have been uncovered this year.

--- China has shut down more than 60,000 porn websites since launching a crackdown in December 2009.

--- Law enforcers across China during a campaign launched in April had destroyed a total of 36.39 million copies of pirated or illegal publications.

audio and video discs.

-- The office has received over 170,000 tip-offs, mostly about the online or cellphone-based spreading of porn content this year and 534 people have been rewarded 544,000 yuan (81,964 dollars) for the information provided.

-- Authorities in Zhongshan City of southern Guangdong Province shut down a huge disc-producing outfit with five production lines and confiscated 3.87 million illegal discs.

MP S keeps up its pledge to keep the information highway clean by monitoring the text messages. For example, cellular companies in Beijing and Shanghai, such as China Mobile, have been told to suspend text services to cellphone users who are found to have sent messages with “illegal or unhealthy content,”

**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.282 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).283 In the meantime, there are 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.284

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

---

283 “Young People Have Ethical Norms on Internet Conduct” (Qingshaonian yaoliao wangluo xingwei daode guifan), China Police Daily Online, November 30, 2001.
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." 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 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 a warfare in a virtual space requiring technical know-how and cross-border co-operation, from warriors around the world and around the clock. Such a battle requires a strong understanding of IT. China is in a disadvantage position. China is on the receiving end with most IT products since most of the advance computer technology are imported. As a result, Chinese government has to live with pre-existing IT system design flaws and weakness. China also has to work with Internet infrastructure built 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.286

Preventing and combating hackers is an area that MPS allocates substantial resources in order to protect computer network safety and provide for 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.287 In June 2000, a 36-year old hacker in Hangzhou, Fang Yong was


287 “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
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. In April 2002, Luo Yun-bin, a hacker to a telecom system in Jiujiang of Zhejiang was on trial and pleaded guilty. The case is the first one reported for attacking an entire information system. It is the second one being prosecuted for destroying a computer system in the country. 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 was reported as 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


289 Luo Yunbin, a graduate in Information and Electronic Engineering of Zhejiang University, worked as a system technician in Unicom and Telecom Bureau of Taizhou city. He was charged with illegal access into the billing database of the Telecom Bureau by Internet in order to delete customer billing data on September 13, 2001. The system reported a 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 Jan. 1, 2011)
In terms of technological details in fighting hackers, very little information is released by MPS or made available to the public. This probably is due to the fact that hackings are rarely reported. If they do, such technical information is classified as confidential. The public is informed of other non-technological approaches to resolving the problem. For example, there was a hacking plan organized by five organizations to attack overseas websites on May 1, 2001. The plan was finally called-off 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

---

[^290]: Zheng Guwei, a medical technology college graduate, participated in the stock market trading (Zhejiang 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 RMB 21,100, i.e., from RMB 30,000 to RMB 10,000. Challenged by the experience, Zheng started to break into three other accounts. On March 12, 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 resulting in 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, Feb. 20, 2002.

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, postal office, government departments, education and science research centers. According to a survey by the China National Security Office and the MPS 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.292

Even though little could be done to cope with technological changes in Internet, China remains committed to imposing Internet censorship to control information flow and limit information access for political and moral reasons. Many scholars, especially those outside of China, have spent much time and effort to study the efficacy, utility and impact of Chinese firewalls.293 “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.”294

Community control

Increasingly, the MPS are enlisting the help of citizens to patrol the Internet and clean up the information highway. The first of such effort is that of enlisting mothers to clean the net of pornography. On January 19, 2010, the Beijing Internet Community organized “Mothers Against Pornography” (MAP) to supervise sexual content on the net. Twenty mothers were hired. Zong Chunshan, the group leader, called MAP “government-mother cooperation” system. The idea came from the U.S., such as MAD. In the first year MAP was able to closed 80,000 pornographic websites with the help of MPS.

The MAP is not without its detractors. In an article entitled: “Does the Mothers Group Want to Turn the Internet into a Children’s Amusement Park,” Yang Hengjun criticizes the MAP as follows:

First, MAP activities are against the Constitution. The cleaning up of the Internet by comprehensive monitoring of content and selectively deleting of web sites is in violation of the PRC Constitution. Chinese citizens 18 and over have a right to read and watch what they like.

Second, MAP has no legal authority to monitor and supervise other people’s use of Internet, based on idealistic notion of “a beautiful garden nor an amusement park.” Internet are not build for children alone.

Third, MAP’s objective is unclear, and invites overreaching or abuse. The definition of “pornography or unhealthy information” is very unclear and subjective. If

strictly enforced, all websites in China are not suitable for children and should be closed down.

Fourth, MAP should teach their children not closing down websites.

Summary

In this chapter, we look at how the Chinese government attempts to combat cybercrime with four kinds of measures, i.e., legislative, education, management, and technology. The overall strategy is to prevent (“fang”), combat (“da”), and regulate (“guan”) and control (zhi). The approach to cyberspace control and Internet regulation in China is an extension of the comprehensive crime control scheme. In the next chapter, I will discuss the impact and limitations of such a comprehensive control approach to cyberspace governance and Internet regulation in China.
Chapter Six

Cyberspace Governance with Chinese Characteristics:

A Case Study of Google vs. China

Introduction

Thus far, this book has focused on how cyberspace governance in China operates, in theory and practice. This chapter looks at Chinese philosophy towards cyberspace governance. More specifically, it investigates into why China censors the Internet, in light of her history, culture and ideology? Or, how does China’s understanding of crime, speech, law and order impact upon cyberspace governance and Internet regulation?

This study is conducted as a comparative case study of free speech exercise, namely how and why China departs from the United States in her approach to cyberspace governance. The major thesis is that the difference in approach to cyberspace governance and free speech between China and United States has a historical origin and are embedded in culture that cannot easily be reconciled.

This chapter is organized in the following manner. Section I “Google Leaving China” provides a detail account of Google’s decision to leave the Chinese market as a context to understand China vs. United States differences over freedom of speech and cyberspace content control. The section is divided into two sub-sections. Sub-section “A” details the “Google decision to leave” and “B” describes “Public Opinion” in reaction to the decision. Section II “Framework of Analysis” first discusses China vs. United States views towards free speech and cyberspace control before offering up Huntington’s “Clash of
“Civilizations” (1993) thesis to explain China vs. United States confrontation over cyberspace governance. Section III summarizes Secretary of State Clinton’s foreign policy speech of January 21, 2010 promising to make free Internet world wide the center piece of United States foreign policy. The speech, read in geo-political context, is “A Call to Arms by the United States” (Section III) against China. In so doing, it denigrates China’s Internet censorship policy as parochial and oppressive and champion United States’ free speech principle as universal and liberating. Ideological hegemony and cultural imperialism is here is stay. Section IV “Fundamental Disputation from China” offers a trenchant retort to Western conception of democracy and human rights principles as universal. It offers up a value pluralism framework as a better way to accommodate the plethora of ideologies and myriads of value systems subscribed to by different nations of the world towards democracy, human rights and free speech. Section V: “Points of Contentions” variously outline the positions of United States vs. China’s towards freedom of speech and its control. The section closes with a case study of PRC effort to launch the “Green Dam” PC computer filtering program as a way of keeping the Internet clean. The debate surrounding the debate neatly summarizing the issues explored in this case study of Google vs. China.

I

Google Leaving China

A. Google decision to leave China

On January 12, 2010, Google China announced that it would leave the Chinese
market over issues of content censorship and hacker attacks, if such activities persist.\textsuperscript{296} The decision was made from Google corporate HQ in the US without consultation with domestic Chinese Google staff, the United States government or Chinese authority. After the public announcement Google executives declared that they “are going to the Chinese government, and we hope we can work things out. But we want to be transparent. We don't want to keep secrets. So we decided to first make a public announcement and now we are having discussions with the Chinese government.”\textsuperscript{297}

According to news account, the decision making process was a protracted and agonizing one. It involved pitting a Google founder’s vision vs. corporate mission, private interests vs. public goods, and above all core values vs. market potential.\textsuperscript{298}

Co-founder of Google, Sergey Brin, a native of Moscow,\textsuperscript{299} has been ambivalent

\textsuperscript{296} “A new approach to China,” \textit{Official Google Blog} 1/12/2010 03:00:00 PM
\textsuperscript{299} “Sergey Brin: Co-founder and president, technology, Google Inc. Sergey Brin, a native of Moscow, received a bachelor of science degree with honors in mathematics and computer science from the University of Maryland at College Park. He is currently on leave from the Ph.D. program in computer science at Stanford University, where he received his master's degree. Sergey is a recipient of a National Science Foundation Graduate Fellowship as well as an honorary MBA from Instituto de Empresa. It was at Stanford where he met Larry Page and worked on the project that became Google. Together they founded Google Inc. in 1998, and Sergey continues to share responsibility for day-to-day operations with Larry Page and Eric Schmidt. Sergey's research interests include search engines, information extraction from unstructured sources, and data mining of large text collections and scientific data.” \textit{Wall Street Journal}
about doing business in China. From the beginning Brin insisted on sticking to “Don’t do evil” corporate motto, i.e., no censorship to Google products. Mr. Schmidt the non-founding CEO argued otherwise. He felt that “Don’t do evil” in not the best corporate policy, as applied to China. To him, doing business in China is not only about making money but also about opening up the regime, a moral imperative. Google cannot have any impact unless it is fully engaged in China.

In the end, Brin prevailed. David Drummond, SVP, Corporate Development and Chief Legal Officer explained the basis of the exit decision in a Google Blog:

“In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China. … First, this

http://topics.wsj.com/person/b/sergey-brin/584

http://online.wsj.com/article/SB10001424052748704675104575001281662251848.html

302 See Video at “Google May Close Operations in China,” New York Times, January 12, 2010. (“CNBC interview with David Drummond, chief legal officer at Google, who discusses the Internet giant's reaction to an assault by hackers who sought to penetrate the e-mail accounts of Chinese human rights activists.”)

303 There is no evidence that the Chinese government is behind the attack, or has knowledge or consented. Id. The Chinese government has emphatically denied any involvement and promised enforcement actions. There is unconfirmed report that the attacks came from Google’s Shanghai office and most probably perpetrated by infiltrated Chinese agents. “Internal secrets of Goolge exiting China revealed!” January 20, 2010

http://blog.goo.ne.jp/duck-tail_2009/e/608b78e5f6df484dd3a5de3664801871_A As evidence, in Google’s letter to China it referenced the attacker as
attack was not just on Google…Second …the attackers was accessing the Gmail accounts of Chinese human rights activists….Third …we have discovered that the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties…We launched Google.cn in January 2006 in the belief that the benefits of increased access to information for people in China and a more open Internet outweighed our discomfort in agreeing to censor some results….These attacks and the surveillance they have uncovered--combined with the attempts over the past year to further limit free speech on the web--have led us to …decided we are no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China.”

As made clear in the above Google blog statement, Google threatened to leave because China’s Internet censorship policy is incompatible with Google’s core values, brand name and market positioning, world-wide.

As a global information company, Google has been most protective of speech freedom, both as a high moral principle and a basic business asset. In

wanggou@guobao.heibang.cn, which is literally translated as webdog@statesecurity.blackgan.cn.

304 “A new approach to China,” Official Google Blog 1/12/2010 03:00:00 PM
305 “Google Vs Censorship “http://googlebusinessmodel.wikidot.com/google-censorship
summer of 2004, Google hired Kai-fu Lee to head its operations in China. Lee summed up Google’s management philosophy to Chinese students as follows:

“youth + freedom + equality + bottom-up innovation + user focus + don't be evil = The Miracle of Google.”

“Don’t do evil” is one of the 10 Google corporate mottos. Indeed, in Google’s official filing with SEC, the founders, Sergey Brin and Larry Page, described Google as "a company that is trustworthy and interested in the public good."

The United States government, from the White House to the Speaker of the House to Secretary of State, is firmly and uniformly in support of Google’s decision.

The Secretary of State, Hillary Clinton, was the first to issue a supportive statement on January 12, 2010:

______________________


http://courses.washington.edu/imt551/content/NYT_Magazine_Gooogles_China_Problem.pdf


308 1. Focus on the user and all else will follow; 2. It's best to do one thing really, really well; 3. Fast is better than slow; 4. Democracy on the web works; 5. You don't need to be at your desk to need an answer; 6. You can make money without doing evil; 7. There's always more information out there; 8. The need for information crosses all borders; 9. You can be serious without a suit; 10. Great just isn't good enough.

http://www.google.com/corporate/tenthings.html


http://news.yahoo.com/s/afp/20100113/pl_afp/uschinaitpoliticsinternetspygoogleobama
“We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. I will be giving an address next week on the centrality of internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear.”310

As promised, on January 21, 2010 on a wide ranging policy speech Secretary of State Hillary Clinton urged China to investigate cyber intrusions on Google and publish its findings, saying:

"We look to Chinese authorities to conduct a thorough review of the cyber intrusions that led Google to make its announcement …We also look for that investigation and its results to be transparent….Censorship should not be in any way accepted by any company from anywhere…And in America, American companies need to make a principled stand. This needs to be part of our national brand."311

On January 14, 2010, in a press conference, the White House made clear

"We have had conversations and discussions with them (Google) about what they have talked about yesterday…The president and this

administration have beliefs about the freedom of the Internet … The right of a free Internet is what many of you heard the president talk about in China … (The President) … strong supporter of open Internet use … big supporter of non-censorship.” 312

On January 13, 2010, the Speaker of the House, Nancy Pelosi issued a statement on her reception of Google’s intent to leave China:

“Google is to be commended for taking action in response to cyber attacks originating from China targeting Chinese human rights advocates, and the intellectual property and corporate data of Google and more than 30 other companies. The announcement that Google will fully review its business operations in China and will no longer tolerate censorship of its search engine should serve as an example to businesses and governments. “The Chinese government operates one of the most sophisticated operations in the world to control the Internet. It is essential that technology companies not assist in efforts that violate human rights or prohibit the free exchange of ideas.” 313


The Chinese response is a guarded and officious one. On January 13, 2010 Foreign Ministry spokesperson Jiang Yu stated:

“China's Internet is open... China has tried creating a favorable environment for Internet. China welcomes international Internet companies to conduct business within the country according to law. China's law prohibits cyber crimes including hacker attacks.”

Meantime, the Chinese government continued to seek clarification from Google and conduct her own internal assessment of the situation. A senior official with China's State Council Information Office expressed China’s perplexity and anxiety: “"It is still hard to say whether Google will quit China or not. Nobody knows,"

On January 18, 2010, six days after Google’s public announcement to leave China, the Chinese government issued an official response in the form of a commentary in the China Daily. The whole purpose of the commentary is to raise issues with and shift responsibility to Google.

The commentary started with a rhetorical question challenging the real motive of

---

314 Zhou Xisheng, Deputy Chief of Xinhua News Agency, Director-General of Xinhua News Net observed: “Our country’s Internet situation is unique. Compared to all kinds of restrictions in foreign countries, China has the most open Internet in the world,” China Digital Times, Dec. 24, 2009. http://chinadigitaltimes.net/2009/12/zhou-xisheng-%E5%91%A8%E9%94%A1%E7%94%9F-the-social-responsibility-of-the-online-news-media/


As to the true reason, it is too early to tell.

“We don't yet know about its real intention to quit China. But reasons in its statement are not convincing. And it is too early and overly sensitive on the part of Western media outlets to play it up as a political issue and portray Google as a guardian of human rights and freedom of speech.”

Whatever the reason, it is not China’s fault, the commentary observed. China has a right to regulate the Internet for illegal and offensive materials according to law.

Google is on notice before coming to China:

“Google is well informed of the legal and regulatory before coming to China. If Google considered it feasible to develop its Internet business under Chinese law four years ago, it would be ridiculous for it to feel otherwise when the Internet environment here in China has improved tremendously in terms of censorship.”

As to cyber attacks, it is a global not Chinese problem: “Wherever Google operates, attacks from hackers will be a problem it has to deal with. So this is undoubtedly not a plausible reason for the Internet giant to quit a market.”

In the ultimate analysis, the commentary opined that Google’s decision is a business choice with many intended and unanticipated economic and political
fallouts.\textsuperscript{317} 

On the same date (January 18, 2010), China made clear that the Chinese government is not about to be cowed and insisted on calling Google’s bluff: \textsuperscript{318}

“Until now, Google's real intentions to quit China are still not clear. There is no sense of blowing things out of proportion and turning a business issue into a political or diplomatic dispute. Above all, Google's decision is no bigger than a corporate maneuver, no matter where the company comes from or how powerful it is.” (Underline supplied)

The announcement came at a surprise. By all account, Google has been relatively successful in penetrating the China market. China’s search engines business is a 6.95 billion yuan (US$1.02 billion) industry in 2009. Of which, Baidu claimed a 63.1 percent market share, with Google keeping a 33.2 percent share, an increase of 5.9 percent from 2008. \textsuperscript{319} Global Google started in China with a mere 13% market share. \textsuperscript{320}

Facebook, MySpace and Twitter have never been able to crack the market or otherwise live up to expectations, due to government censorship or failure to adjust to local cultural conditions. 321

An electronic poll administered by Wall Street Journal (English) found overwhelming support for Google’s decision. To the question: “Should Google leave China over cyber attacks?” 322 75% (2262 votes) is for departure and 24.8% (748 votes) against. 323 However, when the same question was asked in Wall Street Journal (Chinese edition), the opinions were reversed, i.e., 72% of a total 934 voters said no. 324 The two sets of survey conveniently summed up the cross cultural – ideological debate over free speech vs. control between China vs. United States.

322 The lead in on the poll stated: “Google said it is "reviewing the feasibility of our business operations in China" and may back out of China entirely, as it disclosed it had been hit with major cyber attacks it believes to have originated from the country. In a blog post, Google said it detected a "highly sophisticated and targeted attack on our corporate infrastructure originating from China" in mid-December and that the attack resulted in "the theft of intellectual property from Google." Google said it would be talking with Beijing in coming weeks about how it might operate in China without censorship, long a thorn in the side of Western Web companies operating there. "We have decided we are no longer willing to continue censoring our results" on Google's China Web site, Google.cn, the company's chief legal officer, David Drummond, said. Do you think Google should pull out? How would the move affect Google's rivals and Chinese society?" http://online.wsj.com/community/groups/internet-companies/topics/should-google-leave-china-over
323 http://online.wsj.com/community/groups/internet-companies/topics/should-google-leave-china-over
B. Public Opinion

Google’s move attracted a lot of “buzz” in and out of China. At first glance, the reactions are mixed.

Some Internet business executives question the soundness of the decision. Tang Jun, the former Microsoft China CEO commented that "The decision is not a big deal for Chinese netizens, but this will be the most foolish decision in Google's history; To give up China means to give up half of the world." 325

Many human activists praised Google for standing up (to China) in defense of speech freedom. 326 Sharon Hom, the executive director of Human Rights In China commented:

"Companies that think that they had fully assessed the risk of doing business in China had not. They didn't fully assess the censorship climate …The ball is now in the Chinese government's court. Do they think they can ignore this? What is at stake is so much more than just one company." 327

Most Western media are in support of Google. Many multinationals are however afflicted. They realized that in order to do business in China they have to be a good Chinese citizens, i.e., follow restrictive laws and policies wherever they need, including violation of speech freedom and privacy rights of citizens. Few dare to take a public stance against China as a matter of principle for fear of spoiling their tenuous working relationship with the Party or government. Microsoft Corp. faces the same problems as Google did, i.e., imposed censorship and Internet attack. However, Microsoft chooses to stay. Microsoft Chief Executive Steve Ballmer explains:

"We could say we're going to pull out. I don't think that really helps much of anything. In fact, it's the other way around … We have to obey the laws there. It's either that or we just pull out, because I'm not going to put at our Chinese employees at risk by violating the law."

The lone exception is Yahoo, one of Google’s major competitors in China. Yahoo publicly supported Google.

---

328 *Id.* David Barbaboza.
329 It is ironic that as Google insisted on challenging Chinese free speech policy, the US government was conducting wholesale and unconstitutional surveillance of private citizens’ e-mail in and out of country under the Presidential Surveillance Program, since 9/11. See Kam C. Wong, Presidential Surveillance Program (2010). On file with author.
331 David Barboza and Miguel Helft, “Chinese Site Criticizes Investor for Its Google
“We condemn any attempts to infiltrate company networks to obtain user information…We stand aligned with Google that these kinds of attacks are deeply disturbing and strongly believe that the violation of user privacy is something that we as Internet pioneers must all oppose.”

Rebecca MacKinnon, a veteran CNN journalist turned professor at Hong Kong University took up the mainstream position, in support of Google. *The Wall Street Journal* Op-ed page is appropriately entitled “Google Gets On the Right Side of History.”332 In the article Mackinnon condemned the censor in no uncertain terms:

“This censored environment makes it easier for the Chinese government to lie to its people, steal from them, turn a blind eye when they are poisoned with tainted foodstuffs, and cover up their children's deaths due to substandard building codes. It is a constant struggle, and sometimes literally a crime, for people to share information about such matters or to use the Internet to mobilize against corruption and malfeasance.”333

She then applauded Google in facing up to China after years of accommodation, with little to show for it:


“Four years ago when Google entered the Chinese market and launched Google.cn, Chinese bloggers called it the "neutered Google." … The company's effort to walk a fine line between Chinese regulators and free speech critics ended up being unsustainable. Anticensorship activists still viewed its compromise as contributing to the spread of censorship around the world. On the other hand, the compromise was also unacceptable to Chinese authorities, who were unhappy that Google wasn't censoring as heavily as Baidu.”

To MacKinnon, Google made the right decision. “By announcing it will no longer censor its Chinese search engine and will reconsider its presence in China, Google has taken a bold step onto the right side of history.”

Still, many people challenged the wisdom and impact of such a move. For example, Jay Ogilvy Cofounder at Global Business Network and Chairman of Esalen Institute’s Global Potentials Program provided a critical but balanced assessment of Google’s decision:

First, Google’s “private” business decision takes on “public” policy choice

334 Ibid.

335 Miguel Heft, “Google Would Abandon a Lucrative Market,” New York Times, January 12, 2010. (“Duncan Clark, chairman of BDA, a consulting firm in Beijing that advises major telecommunications and technology companies: “This has ramifications far beyond this case…there have been a raft of decisions and unpredictability, a kind of unpleasantness about what’s happening here. There’s been this received wisdom that no one can afford not to be in China. But that is being questioned now.”)

character and “has tremendous significance for the diplomatic and political-economic arena.” The decision however has few public input and little government coordination, though it is a decision of historical proportion.337

Second, “this move de-legitimates the current Chinese regime”. It shows the Chinese Communist Party and authoritarian government is ill equipped to deal with “open, peer-to-peer network so necessary to economic success in the information era.”

Third, economically speaking Google acted irresponsibly towards the shareholder by exiting one of the faster growing market place.338 However, Google might gain good will and brand loyalty by staying true to its core values: “Do no evil”?

Fourth, Google’ exit decision is a game changer. It foreshadows the separation of State from the Marketplace.

A cursory review of blog entries, comments and responses net the following revealing observations:

(1) The Google decision is a founder’s vs. management decision, and shows hands on involvement and personal courage:

“Google's statement on China is pretty extraordinary. That they are even considering leaving the largest growth market in the world is a stunning

338 “This was not a business decision—the business decision would obviously have been to continue to participate in the Chinese market. It was a decision based on values. We tried to ask what would be best from a global standpoint.” Fareed Zakaria“A Conversation With Google’s Chairman and CEO,” NEWSWEEK, January 15, 2010.
http://www.newsweek.com/id/231117
revelation. And it is unlikely that hired and professional management would make such a decision. Management's primary job is to build value for shareholders and it would seem that leaving the largest growth market in the world is not in the shareholder's interest….I am very impressed with Google and have been for a long time. I think that many of the reasons it is such an amazing company result from having its founders engaged and involved in the key strategic decisions the business faces. The founder factor is a huge intangible force in companies and is most often for the best.339

(2) The public is not being well served, since the founders of Google, not the stockholders, the consumers or the public, have the lone control over the decision:

“Being public but not being publicly controlled by virtue of arbitrary and contrived stock restrictions should simply not be allowed...It is a violation of the fundamental spirit of responsible corporate governance which is a foundation element of public trading of a company's securities as it allows an artificially created subset of shareholders to artificially dictate the composition of a company's Board of Directors which is in direct contravention of the concept of majority independent directors of public and exchange traded common stock…If a stock issuer wants to play that game, then their securities should not be publicly traded.”

(3) China might be big business but U.S. is on the right side of history:

“There is no idea which is "bigger" than fairness and freedom. China is 8
x bigger than the US in population. Their landmass is enormous. Their
history is incredible --- they were literally an empire when we were living
like savages…But the soul of their country is very small while the sense of
America's virtues --- as flawed as our democracy can be at times and as
cynical as we have all become --- is the grandest set of ideas ever put into
practice….When the Colonists revolted against the most powerful nation
and armed force in the world and prevailed, the American spirit of
freedom was brought to life for all time…Unfortunately, only the victors
get to write the histories.”

(4) Google decision is based not only on money but principles of open society:

“Guessed that this would be the answer, but it's not only the money. It's
about freedom, open society, opportunity, individual over tradition, skills
and efforts over class or connections to the administration. Not that
everything is perfect in the US, but at least these are the ... Founders factors.
And good founders leave their mark long after they are dead. But if you tell
me that Mandarin tradition is preferred for you over Franklin and Lincoln, i
respect that - although doubt it will be your choice.”

(5) Google decision is based on money, e.g., in country rivalry, but still gutsy:

“I don't think anyone should be confused. Google did this only after their

340 http://www.avc.com/a_vc/2010/01/the-founder-factor.html#disqus_thread
341 http://www.avc.com/a_vc/2010/01/the-founder-factor.html#disqus_thread
business was threatened, not because they were specifically concerned about China trampling anyone's rights. That being said, it is an admirable and gutsy move and I am excited to see them make it. It goes to show that even if U.S. companies tend to think of the business world as global, other countries may still think in purely nationalistic terms. If Google were a Chinese company it probably would not have been attacked. Then again, a Chinese company would never do what Google has just done. It is not just the founders, it is also the country/environment that those founders are working through/from….It will be very interesting to see the level of power an entrenched Internet company really has. I don't think we've seen something that demonstrates this in the past."342

Many Chinese bloggers lamented the loss of a reliable information source and an influential communication platform. Prominent liberal blogger, Ran Yunfei, wrote: "Google leaving China is definitely not good news….Those (dissidents) who would remain are obedient citizens and [that is] satisfactory to the authorities." Isaac Mao, a Chinese blogger said: "I think Google has eventually made the right decision to fight back based on their principles."343

342 http://www.avc.com/a_vc/2010/01/the-founder-factor.html#disqus_thread
II

Framework of Analysis

The major differences between China and United State attitude and policy towards free speech and Internet control is best rehearsed at U.S.-China Internet Industry Forum held in San Francisco on Dec. 9-10, 2009 in San Francisco.

China on Internet control

China’s position is clearly and forcefully expressed by Cai Mingzhao, Deputy Director of the Chinese Communist Party's Propaganda Department.:

“An important part of network security was to ensure the security of online information … Pornography, fraud, spam, online attacks and computer viruses were serious threats to information security and were impairing the public's confidence in the Internet…Under such circumstances, it is not enough to emphasize the free flow of information alone. Information security should be put in a prominent position…If network information security is not guaranteed, the information flow will become irregular. If illegal and harmful information are allowed to flow rampantly without checks, it will do great harm to the real society. The first priority of ensuring online security should be protecting adolescents, as teenagers had become the largest online group and whose growth was increasingly influenced by the Internet. Each country has its own unique circumstances, differing from each other in Internet penetration, economic and social development, cultural traditions and laws …ensuring online security should fully respect the cultural diversity and concerns of all

---

Samuel P. Huntington, “The Clash of Civilizations?” Foreign Affairs Summer 1993
countries. Therefore, Internet security around the world is unable to be measured by a unified standard. It is impossible to regulate security with a single law or manage it in a single pattern.”

United States on free speech

Robert Hormats, U.S. Undersecretary of State for Economic, Energy, and Agricultural Affairs has this to say about U.S. position and intention on free speech and unrestricted net:

The Internet offers us an unparalleled opportunity to acquire knowledge if we allow ourselves unrestricted access to it….The Internet has produced entire new industries and revolutionized distribution of design and development of both goods and services. Unrestricted access to information is vital to the types of innovation that spark economic growth….It is the users and developers of online content who make our connections to the world wide web so valuable….The right to freedom of expression and the importance of the free flow of information over the Internet were confirmed by all participating governments at both phases of the World Summit on the Information Society in 2003 and then again in 2005, including the Tunis Commitment, and continue to form the foundation of U.S. government efforts on Internet freedom throughout the world. …We also work closely with individual companies and industry groups to foster improved access to information. one example is the Global Network Initiative, a group of leading

345 “U.S.-China Internet forum highlights need to step up online security,” Xinhua Dec. 11, 2009.
private sector companies, NGO's, academicians and investors, that seeks to advance both freedom of expression and privacy in information and communication technologies...We believe that commerce should be open and the information should generally be freely accessible… we recognize that potential downsides and risks may come with new technology, such as threats to children and online ability of terrorists to use the internet to organize...  

Huntington on “Clash of Civilizations”

Google’s defend of free speech at all costs and China promotion of wholesome cyberspace with zealous conviction speaks to larger geo-political forces at work, namely “A Clash of Civilizations” between two major cultural system, one ebbing (United States)\textsuperscript{347} and other accenting (China),\textsuperscript{348} both hacking back to a glorious past, with fond memory and renew vigor.

The “Clash of Civilizations” thesis was first proposed by Huntington. In 1993, Huntington published an influential article in \textit{Atlantic Magazine} arguing that in the post cold war era, global conflicts will be driven by culture more so than by ideology or economics. Civilization not nationalism will cause war to happen:

“It is my hypothesis that the fundamental source of conflict in this new world will not be primarily ideological or primarily economic. The great

\begin{footnotesize}
\begin{enumerate}
\end{enumerate}
\end{footnotesize}
divisions among humankind and the dominating source of conflict will be
cultural. Nation states will remain the most powerful actors in world affairs,
but the principal conflicts of global politics will occur between nations and
groups of different civilizations. The clash of civilizations will be the battle
lines of the future.”

In the main such international conflicts will be “between the West and non-
Western civilizations and among non-Western civilizations.” As to “What do we mean
when we talk of a civilization?”

“A civilization is a cultural entity. Villages, regions, ethnic groups,
nationalities, religious groups, all have distinct cultures at different levels
of cultural heterogeneity....A civilization is thus the highest cultural
grouping of people and the broadest level of cultural identity people have
short of that which distinguishes humans from other species. It is defined
both by common objective elements, such as language, history, religion,
customs, institutions, and by the subjective self-identification of people.
People have levels of identity … The civilization to which he belongs is
the broadest level of identification with which he intensely identifies.”

Looking back and projecting forward, Huntington identified eight major
civilizations that are likely to crash along cultural fault lines. They are: “Western,
Confucian, Japanese, Islamic, Hindu, Slavic-Orthodox, Latin American and possibly
African civilization. The most important conflicts of the future will occur along the
cultural fault lines separating these civilizations from one another.”
Huntington offered six reasons why civilization might clash:

First, civilizations are real, fundamental and of consequence to human existence. Civilization establishes personal identity, structures social relationship, defines moral compass, inculcates human emotions, and mostly importantly inform human actions, dos and don’t. Culture controls how we think, feel and act.

In the end our culture influences

“our ideas; our tastes; our moods; the way we behave; our ambitions, and what we want in life; our opinion of what it means to have a successful life; what makes us happy; our actual level of happiness; our opinion about whether a particular food is delicious or disgusting; our opinion about whether a person is beautiful or ugly; our opinion about whether or not a person is a hero; what we consider right and wrong; what we consider physically dangerous; and our feeling as to whether we are sick or healthy … Civilizations are differentiated from each other by history, language, culture, tradition and, most important, religion. The people of different civilizations have different views on the relations between God and man, the individual and the group, the citizen and the state, parents and children, husband and wife, as well as differing views of the relative importance of rights and responsibilities, liberty and authority, equality and hierarchy. These differences are the product of centuries. They will not soon disappear…”

---

<table>
<thead>
<tr>
<th></th>
<th>Chinese</th>
<th>Americans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conception Of the Self</td>
<td>Collectivist: Higher value placed on group cooperation and individual modesty.</td>
<td>Individualist: Higher value placed on self-reliance. Self-promotion is more accepted. High value placed on &quot;freedom&quot; from externally imposed constraints.</td>
</tr>
<tr>
<td>Social Relationships</td>
<td>Formal, hierarchical. People most comfortable in the presence of a hierarchy in which they know their position and the customs/rules for behavior in the situation.</td>
<td>Informal, egalitarian. People most comfortable with their social equals; importance of social rankings minimized.</td>
</tr>
<tr>
<td>Friendship</td>
<td>Small number of close, lifelong friends who feel deeply obligated to give each other whatever help might seem required.</td>
<td>Large collection of &quot;friends&quot; and acquaintances which changes over time and involves only limited mutual obligations.</td>
</tr>
<tr>
<td>Obligation</td>
<td>Relationships with other people involve reciprocal obligations.</td>
<td>People avoid interdependent relationships and situations that might entail long-term obligations.</td>
</tr>
<tr>
<td>Task vs. Relationship Orientation</td>
<td>Relationship-oriented: Maintaining a harmonious relationship has priority over accomplishing tasks.</td>
<td>Task-oriented. Relationships are less important than getting the work done.</td>
</tr>
<tr>
<td>Harmony vs. &quot;Truth&quot;</td>
<td>Avoid direct confrontation, open criticism, and controversial topics. Concern maintaining harmony and with &quot;face.&quot;</td>
<td>Willing to confront directly, criticize, discuss controversial topics, press personal opinions about what they consider &quot;the truth. Little concern with &quot;face.&quot;</td>
</tr>
<tr>
<td>Role of laws,</td>
<td>More faith in personal</td>
<td>Written rules presumably</td>
</tr>
</tbody>
</table>

---

rules, and regulations | relationships than in written rules and procedures for structuring interactions. | apply to everyone and are assumed to produce fair, reasonable procedures and decisions.
---|---|---
Time Consciousness | Relatively more attention to the past and to the longer-term future. | Less interested in the past; eye on near-term future.
Ascribed vs. Achieved Status | Traditionally, a person's status in the society was based importantly on inherited characteristics such as age, gender, and family. This is changing. | People's status is based mainly on their own achievements, including education obtained and level of success realized in their line of work.

Second, the world is getting smaller and people are interacting more. Cross-cultural exchanges, international business and global communications make us more aware of our own cultural differences and civilization identity, as a world citizen. Manuel Castells in his seminal work investigating the impact of “The Information Age” on cultural identity observed:

“Our world and our lives are being shaped by the conflicting trends of globalization and identity…the widespread surge of powerful expressions of collective identity … challenge globalization . . . on behalf of cultural singularity and people’s control over their lives and environment.”

Dr. Yusuf Örnek put it more bluntly:

“No matter how much globalization is encouraged by the lifting of boundaries in the markets, the struggle for identification on the local

---

(micro) level is increased by that much. Who would want to break off all cultural ties in order to be a world citizen? Or worse, who could claim that cultural ties are in opposition to world citizenship?"\textsuperscript{352}

John Tomlinson provided empirical evidence of local culture resisting global challenge in reform China:

“In the fashionable \textit{Dong An} shopping centre in the Wang Fu Jing district of Beijing you will find a small boutique called \textit{Mu Zhen Liao}. Here, young, discriminating and upwardly mobile Beijingers come to choose clothes, not from the designer labels of the West, but ‘classical’ Chinese clothing: elegant \textit{qipaus, cheongsams} and finely tailored jackets in beautiful silks and other traditional fabrics….\textit{Mu Zhen Liao} – a chain store with branches in many of the provincial capitals – exists, in cultural as in economic terms, as a consequence of globalization.”\textsuperscript{353}

“Third, the processes of economic modernization and social change throughout the world are separating people from longstanding local identities. They also weaken the nation state as a source of identity…”

\textsuperscript{352} Dr. Yusuf Örnek, Globalization and Cultural Identity

Fourth, the West position in the world order is being challenged by the rest of the world coming of age in modernity and economy:

“[T]he growth of civilization-consciousness …On the one hand, the West is at a peak of power. At the same time, however, and perhaps as a result, a return to the roots phenomenon is occurring among non-Western civilizations…A West at the peak of its power confronting non-Wests that increasingly have the desire, the will and the resources to shape the world in non-Western ways….”

“Fifth, cultural characteristics and differences are less mutable and hence less easily compromised and resolved than political and economic ones….It is more difficult to be half-Catholic and half-Muslim…”

“Sixth, economic regionalism is increasing. The proportions of total trade that are intraregional rose between 1980 and 1989 from 51 percent to 59 percent in Europe, 33 percent to 37 percent in East Asia, and 32 percent to 36 percent in North America…Common culture, in contrast, is clearly facilitating the rapid expansion of the economic relations between the People's Republic of China and Hong Kong, Taiwan, Singapore and the overseas Chinese communities in other Asian countries.”

Currently, the world suffers from what Huntington called “west vs. the rest” syndrome. By that he means the Western civilization holds extraordinary military (UN), economic (IMF), and cultural (free world) power in relation to other civilizations.
“Differences in power and struggles for military, economic and institutional power are thus one source of conflict between the West and other civilizations. Differences in culture, that is basic values and beliefs, are a second source of conflict. V. S. Naipaul has argued that Western civilization is the "universal civilization" that "fits all men." At a superficial level much of Western culture has indeed permeated the rest of the world. At a more basic level, however, Western concepts differ fundamentally from those prevalent in other civilizations. Western ideas of individualism, liberalism, constitutionalism, human rights, equality, liberty, the rule of law, democracy, free markets, the separation of church and state, often have little resonance in Islamic, Confucian, Japanese, Hindu, Buddhist or Orthodox cultures. Western efforts to propagate each idea produce instead a reaction against "human rights imperialism" and a reaffirmation of indigenous values, as can be seen in the support for religious fundamentalism by the younger generation in non-Western cultures. The very notion that there could be a "universal civilization" is a Western idea, directly at odds with the particularism of most Asian societies and their emphasis on what distinguishes one people from another. Indeed, the author of a review of 100 comparative studies of values in different societies concluded that "the values that are most important in the West are least important worldwide." 354

III

A Call to Arms by the United States

On January 21, 2010, Secretary of State Hillary Clinton made the following foreign policy speech. The speech makes the promotion of free speech and defense of Internet access around the world a 21st Century foreign policy of the United States, and an imperative of her administration. In so doing, Clinton offered up an explicit challenge to the Chinese authority – stop what you are doing to the netizens and Internet, otherwise we will unilaterally liberate the Internet for you. Some has applauded this bold and visionary “Clinton doctrine.” As many condemned it as “Internet imperialism” reminiscent of the call for “opium” war, wherein the British forced open China with opium trade and gunboat diplomacy.355

Considering the tone, texture and content of the Clinton speech, it can best be described as a “call to arms of the United States” against China. In the words of Huntington “A Clash of Civilizations” is fast developing into a contestation over two visions of the virtual world.

“The spread of information networks is forming a new nervous system for our planet…Now, in many respects, information has never been so free. There are more ways to spread more ideas to more people than at any moment in history. …During his visit to China in November, for example, President Obama …spoke about how access to information helps citizens

hold their own governments accountable, generates new ideas, encourages creativity and entrepreneurship… And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights… On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single internet where all of humanity has equal access to knowledge and ideas… Our responsibility to help ensure the free exchange of ideas goes back to the birth of our republic. The words of the First Amendment to our Constitution are carved in 50 tons of Tennessee marble on the front of this building… But the Internet is a network that magnifies the power and potential of all others. And that’s why we believe it’s critical that its users are assured certain basic freedoms. Freedom of expression is first among them. This freedom is no longer defined solely by whether citizens can go into the town square and criticize their government without fear of retribution. Blogs, emails, social networks, and text messages have opened up new forums for exchanging ideas, and created new targets for censorship… The Berlin Wall symbolized a world divided and it defined an entire era. … Some countries have erected electronic barriers that prevent their people from accessing portions of the world’s networks. They’ve expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. These actions contravene the Universal Declaration on Human Rights, which tells us that all people have the right “to seek,
receive and impart information and ideas through any media and regardless of frontiers”…As in the dictatorships of the past, governments are targeting independent thinkers who use these tools…Now, all societies recognize that free expression has its limits. We do not tolerate those who incite others to violence …And hate speech that targets individuals on the basis of their race, religion, ethnicity, gender, or sexual orientation is reprehensible…Now, just as these technologies must not be used to punish peaceful political speech, they must also not be used to persecute or silence religious minorities. Now, prayers will always travel on higher networks….But make no mistake – some are and will continue to use global information networks for darker purposes. Violent extremists, criminal cartels, sexual predators, and authoritarian governments all seek to exploit these global networks… As we work to advance freedoms, we must also work against those who use communication networks as tools of disruption and fear…Now, the principles I’ve outlined today will guide our approach in addressing the issue of internet freedom and the use of these technologies…We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship. We are providing funds to groups around the world to make sure that those tools get to the people who need them in local languages, and with the training they need to access the internet safely…Both the American people and nations that censor the internet should understand that our government is committed to helping promote internet freedom. ..Now, the United States and China
have different views on this issue, and we intend to address those
differences candidly and consistently in the context of our positive,
cooperative, and comprehensive relationship. …Now, ultimately, this issue
isn’t just about information freedom; it is about what kind of world we
want and what kind of world we will inhabit. It’s about whether we live on
a planet with one internet, one global community, and a common body of
knowledge that benefits and unites us all, or a fragmented planet in which
access to information and opportunity is dependent on where you live and
the whims of censors. “ (Italic provided)

In the above speech, Clinton made clear that United States stands for freedom of
speech while China standards for control of Internet. There is no common ground.
United Sates will do everything and anything to break down the Chinese
“firewall” just as it did with destroying the Berlin war, in another era. The
speech is not only noted for what is being said, i.e., China vs. United States do no
see eye to eye on the fundamental issue of free speech vs. control of Internet, but
for its belligerent tone – bring it on, United States relish a good fight with China
and we will win.

Civilization” has just bean.\footnote{Evgeny Morozov, ”Is Hillary Clinton launching a cyber Cold War?” \textit{Foreign Policy}, January 21, 2010.}
IV

A Fundamental Disputation From China

Western human rights advocates claim that free speech and privacy rights are universal and absolute. They can be ascertained in the abstract and as a matter of principle. China adopts a different view. Human rights are relative and particularistic, contingent upon time, place, people, and situation. They can only be actualized in context.

Human rights activists and democracy champions from the West talk about the importance of human rights, freedom and democracy as universal and fundamental moral principles. Many people from around the world have argued that human rights while important and deserving of our attention, should not remain our exclusive, or even dominant, concern. In our debate over human values, we also need to think about cultural exchange, and not simply imposition of one nation/people/culture values on other autonomous individuals or sovereign nations.

---

358 I have written the disputation in the first voice of the Chinese.
359 Orlando Patterson, Freedom in the Making of Western Culture (Basic Books, 1991) (The idea and ideal of freedom is not naturally derived but socially constructed. It is the existence and perpetuation of freedom in the West which requires explanation and not the lack thereof in non-Western countries should be justified. “Preface”)
361 China championed negative rights, e.g., right to be free of hunger and exploitation while Singapore promoted Asian values.
362 This calls to mind President Bush’s insistent that only American conception of freedom and democracy is worth fighting for. “Freedom fighters’ from other nations are ipso facto terrorists.
To start the debate, we need to observe that there are many values worthy of human pursuit; e.g., freedom from starvation, personal integrity, filial piety, social responsibilities and loyalty to one’s country.\footnote{363}{In this regard, there are four observations to be made. First, it is obviously true that not all values are created equal. For example, material goods pale alongside moral and spiritual ones. Second, it is also clear that no single value, moral principles included, is so fundamental as to absolutely overshadow others at all times, in all places, and in all situations. Even the taking of innocent human lives can at times be justified in the name of stopping a greater evil. Third, judging values in context goes well beyond merely determining which moral principles should apply in a given decision making frame. Many valves are involved. Most of them are in conflict and priorities must be set. The challenge is, given a set of ranked values, national priorities and limited resources, prioritizing.\footnote{364}{Fourth, the ranking of values in the abstract is so loaded with conditions and disclaimers as to be of little use when applied to real-life situations. Indeed, they might create problems even in a theoretical multi-value matrix decision making set. Should I kill one to save the lives of...}}

\footnote{363}{“Not so (respect for life as universal). In the classical Chinese tradition in which I was brought up, we are aught to respect for parents, respect for teachers, respect for ancestors and for duly constituted authority, but the conception of respect due to the individual human beings as such does not exist in that culture.” Basil Mitchell, “The Value of Human Life,” in Peter Byrne, \textit{Medicine, Medical Ethics and the Value of Life} 34-47 (1990).}

\footnote{364}{However, in Buddhist thought the principle of respect for life must be understood within the context of other aspects of Buddhism teaching as well as other percepts. Different traditions within Buddhism balance the concern for respect for life with concern with doing the “most compassionate action.” Kevin WM. Wildes, S.A., “Sanctity of Life: A Study in Ambiguity and Confusion,” in \textit{Japanese and Western Bioethics} 89-101(Kazumasa Hoshino ed., 1997).}
If not, then what right do we have, as a civilized government, to build a highway which, after all, kills? Are the traffic fatalities not victims of a government’s conscious policy choice, to develop highways instead of airports? Do we not call them casualties of human progress? The complexities and difficulties in arriving at agreed values are best described thusly:

“Second: there is no shared set of value priorities. We make much of the fact that we share values and we frequently say that, well, basically humans want the same things so we ought to be able to work things out. Perhaps, at a survival level, but beyond that, and even there, there is not a shared set of priorities with regard to values. Instead, priorities change with circumstance, time, and group. Here are some examples where value priorities differ depending on the group and circumstance. Short term expedience versus long term prudent behavior and vice versa. Group identity versus individual identity. Individual responsibility versus societal responsibility. Freedom vs equality. Local claims versus larger claims for commitment. Universal rights versus local rights (that can repudiate universal rights; fundamentalisms, for example.) Human rights versus national interests (e.g., economic competition or nationalist terrorism). Public interest versus privacy (the encryption conflict, health information, whether private or not). First amendment limits (pornography, etc.). Seeking new knowledge and its potential benefits vs its potential costs. Who sets the rules of the game and who decides? These are all issues

---

where the priority of values are in contention. There is no reliable set of priorities in place that can be used to choose decisively among actions toward the larger issues.” 366

The above are not arguments for value relativity, nor propositions for situational ethics. It is a proposition for value pluralism.367 Value pluralism simply mean that there are many more human values which give meaning to life and happiness to people than the principles of justice, freedom, equality and democracy. Put it in another way, a country can hold other enduring values—love for family, loyalty to friends, duty to society—and still deserve our admiration and respect. A benevolent dictator is better to many than starvation and chaos.

Human rights advocates argue that human rights are so fundamental that all other values pale in comparison. While this argument has surface appeal and is emotionally satisfying, a moment of critical reflection show that this does not conform to our

366 Point: Observations Regarding a Missing Elephant by Donald N. Michael, Emeritus Professor of Planning and Public Policy, University of Michigan (http://www.panetics.org/)
367 Tom L. Beauchamp, “Comparative Studies: Japan and America,” in JAPANESE AND WESTERN BIOETHICS 25-47 (Kazumasa Hoshino ed., 1997). I came to my observation here—similar values but differentially ranked (individually and in conjunction with others) and variously applied (taking up contextual importance)—quiet independent of Beauchamp’s work. But Beauchamp’s work—narrow morality (universal principles) and broad morality (differential application)—share one thing in common with mine, i.e., “the principles upon which men reason in morals are always the same; thought the conclusions which they draw are different.” Id. at 27. For a discussion of moral objectivism and indeterminacy, see Russ Shafer-Landau, “Ethical Disagreement, Ethical Objectivism and Moral Indeterminacy,” 54 PHIL. & PHENOMENOLOGICAL RES. 331-44 (1994) (available at http://www.ku.edu/~philos/faculty/Shafer-Landau/DISAGREE.html).
understanding of how human values are formed, adopted, and evolved. First, human rights advocates deem it “self-evident” that human rights—life, liberty and the pursuit of happiness—\textsuperscript{368} are fundamental in nature, universal in application, and apparent to all. All human beings should and must subscribe to the same set of human rights values—in content, importance, and, when compared with other values, priority. There are no exceptions or deviations. Nothing could be further from the truth. Human values, as with beauty, are in the eyes of the beholder. Likewise, there are many ways to discover human values; as many as there are individuals on this earth.

On a theoretical plane, Kant’s categorical imperatives\textsuperscript{369} or Bentham’s utilitarianism\textsuperscript{370} are good starting points in order for one to discover individual or social

\textsuperscript{368} The Declaration of Independence para.1 (U.S. 1776).

\textsuperscript{369} Immanuel Kant, \textit{Groundwork of the Metaphysic of Morals} (J.K. Patton trans., Harper Perennial 1965) (“Act only according to that maxim by which you can at the same time will that it would become a universal law.”). Kant made this observation when applying his categorical imperative to suicide: “If a man is reduced to despair by a series of misfortunes and feels wearied of life, but is still so far in possession of his reason that he can ask himself whether it would not be contrary to his duty to himself to take his own life, he should ask himself a question. He should inquire whether the maxim of his action could become a universal law of nature. His maxim is: From self-love I adopt it as a principle to shorten my life when its longer duration is likely to bring more evil than satisfaction. It is asked then simply whether this principle founded on self-love can become a universal law of nature. Now we see at once that a system of nature of which it should be a law to destroy life by means of the very feeling whose special nature it is to impel to the improvement of life would contradict itself, and therefore could not exist as a system of nature; hence the maxim cannot possibly exist as a universal law of nature, and consequently would be wholly inconsistent with the supreme principle of all duty.”

\textsuperscript{370} “By the principle of utility is meant that principle which approves or disapproves of every action whatsoever, according to the tendency which it appears to have to augment or diminish the happiness of the party whose interest is in question: or, what is the same thing in other words, to promote or to oppose that happiness.” \textit{Jeremy Bentham, An}
values, but these are not final. Ontological and teleological validation of value choices are not exhaustive.

In more practical terms, rational analysis and positive thinking are not the only, nor even the best, tools to determine the contour and correctness of human values. Indeed, I venture to guess rational analysis is ill-suited to the investigation of value matters which are, after all, more instinctual than cognitive, and more emotive than logical. We love humanity with our heart, and appreciate life with our soul, not with a computer and a brain. In the end, spiritual enlightenment, personal feelings, human experience and collective wisdom can all play a part in one’s endless value search.

Second, human rights belong to each and every individual, and are not monopolized by one ideological camp. Most certainly, values, of which human rights are an integral part, are not beholden to the intellectually bright, militarily strong, economically wealthy or culturally rich. As nations, as communities, as families, and as individuals, we all subscribe to a set of values. Each of us is equally capable of finding a set of values suited to our taste. All of us are equally endowed as moral agents. It is apparent that no one country—no matter how big, how strong, how rich, and how enlightened—can monopolize the creation of desirable values, much less be the net exporter of virtues. 371

Third, national values, as with one’s moral compass, do not come prepackaged. They are a combined and integrated product of personal make-up, cultural heritage, social

371 See M. Angell, Ethical imperialism?, 319 NEW ENG J. MED. 1081-83 (1988) (universal values cannot be compromised without compromising morality itself.); see also C.B. Ijsselmuiden & R.R. Faden, 326 NEW ENG J. MED. 830-34 (1991) (Moral judgment differs not because the value principles are not morally justifiable but that they are factually inapplicable in context.).
consensus, economic circumstances, and even accidental events. In sum, values are a sum total of human existence; wants, needs, phobia, remembrance, dreams, and hopes. Once formed, they are a given fact of nationhood and are seldom right or wrong in the abstract or in total.

Fourth, values are formed experientially, experimentally, naturally, and incrementally, more so than cognitively, absolutely, positively and dramatically. Historical accidents and national happenstance have as much to do with a country’s value formation as do rational discourse and reflective policy. Much of the values Americans take for granted are rooted the manner by which the United States found liberation, independence, and an individuality as a result of rebellion against British rule. Conversely, the Chinese people have sought refuge in paternalism and collectivity because their historical embracing of the teachings of Confucius.

Given this “dynamic” and “dialectical” process of human value formation, it should come as no surprise to anyone to learn that human values never stop growing and evolving, changing in content and mix every minute and hour of the day. “We get wiser as we grow older” is as much a descriptive statement as it is an admonition to the young who are eager to live all that life has to offer in one day. Viewed in this light, the search for human values is not a discovery process but a creative journey. An individual, a people, a community, a nation-state; all are searching for an illusive and transient identity; but never arrive at an ultimate destiny. It is the process of searching for, and not the ultimate finding of, human values, which gives meaning to life.

Lastly and most significantly, values are bound by time and space, and posited within certain places, and societies. Two very important observations flow from this postulate. First, values exist within a context of history, place, people, society, and culture.
There is no ahistorical, asocial or acultural value. To appreciate why Chinese rulers, and, for that matter, many Asian leaders, adopt a paternalistic attitude towards their subjects, it is necessary to consider the importance and structure of the family within Chinese history and culture. A critique of the Chinese style of government is not just an attack on Chinese current leaders but also an indictment against China’s cultural heritage in general, and the role and functions of family in particular. With so much at stake, and such complexities involved, a country passing judgment on others should be more reflective, thoughtful and considerate. It is easy to be misinformed and misjudge.

Second, values are bundled goods. The meaning and importance of a value cannot be easily extracted from the collective of values of which it forms an integral part. The surgical removal and strategic implantation of values will certainly cause political disruption, such as the wholesale abandonment of communism in U.S.S.R., which led to social unrest and political chaos, and social rejection, such as the ban on U.S.-style adversarial journalism in Singapore.

It is most difficult, if not impossible, for a person or country to transcend its intellectual horizon and value space. Cultural myopia is the norm. China calls herself “Central Kingdom” and still acts that way. Intellectual provincialism is the rule. All rationality is bounded.

Marx’s critique of the capitalistic intellectual order, that the consciousness of the mass is conditioned, controlled and dominated by ideas emulating from the economic

---

base, is flawed, less so because it is an overbroad observation than because it is not carried far enough. Marx failed to explain convincingly why he could liberate himself from such an all-embracing ideological confine to lead the charge against capitalism, while others could not. Rawls’ Theory of Justice suffered from a similar cultural straight jacket: the just society behind “the veil of ignorance” envisioned by Rawl looked more like twentieth century Boston than traditional Indonesia or contemporary Japan.

Is it surprising to see first the Romans, then the British and now the Americans preaching the virtues of their culture to the rest of the world; through persuasion if possible (BBC, VOA, CNN) and by force (extra-territoriality, Vietnam, Iraq) if necessary? Echoing Huffington, does it not appear odd that it takes the British a few hundred years to discover the essence of civilization while the Egyptians are still at a loss after 6000 years? Is it possible that the Americans find the best in government in 200 years while the Chinese keep missing them after 4,000 years?

The discovery of universal values has more to do with individual ego and national pride than any intrinsic merit associated with those values. The successful spread of values, from democracy to gay rights, reflects more upon a country’s economic strength and concomitant cultural domination, than on any inherent appeal and demonstrated goodness of certain moral principles.

Cultural domination, abet in subtle form, is here to stay. Singapore’s senior

375 JOHN RAWLS, A THEORY OF JUSTICE (1971)
statesman was right when he said that Asian values are as worthy of respect—because those values tell Asians who they are. 377

V

Points of Contentions

In the West, state is a constructed political entity form by a “social contract” to promote public goods, i.e., safety, health, education, and welfare of the people. Nothing can be achieved if everyone has to live in fear (Hobbes). Society can only advance with people working together for a common good under a general will (Rousseau). State exists to do good things, in the name of the people, i.e., of, by and for the people. This view of governance is build upon individual atomism.

   With China, state is the embodiment and sublimation of an utopian ideal, i.e., peace, prosperity and happiness under heaven and on earth. In the Confucius past, it is to realize the “mandate from heaven.” With the Communist present, it is to actualize “socialism” on earth. State exists to do good, as an indivisible whole of the people, i.e., from the mass to the mass. This state of “being” resulted from holistic corporatism.378

   In the West, individual rights and freedom of speech is the foundation of democracy. With China, collective welfare and appropriate (speech) conduct is the key to utopian state.


378 Catalyzing personal empowerment, societal transformation, and environmental sustainability ("The major problems in the world are the result of the difference between how nature works and the way people think." Gregory Bateson) http://www.attractionretreat.org/Writings/WWUEoS.html
In the West Internet research of and about China tends to focus on: government censorship vs. freedom of speech, and web site blocking vs. political dissent. The conventional wisdom in the West is that the technological characteristics and functional features of the Internet (pre) determines the outcome of IT revolution, i.e., the spread of Internet leads inevitably to the promotion of Western (universal) political values, i.e. freedom of speech and democratic governance. Few have critically examined the postulated link between structural properties of Internet and grounded culture of a people. There are few attempts to look at the validity of such claims, beyond episodic, anecdotal and selective evidence, all designed to preach Western political values, sold as universal human rights.

**Western Contentions**

*Two different schools*

A review of legal U.S. literature shows that most legal researchers have a common interest in the study of Chinese cyberspace governance, i.e., to ascertain whether China will be able to effectively control the free 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, argued that Internet control in China is impossible. On the contrary, some scholars such as Kristina Reed and Clara Liang, held the view that China’s regulatory measures are effectively in controlling Internet content.

*Role of government in cyberspace*
In their study, Richard Cullen and Pinky D. W. Choy explore how the China government seeks to mediate the tensions between control of Internet harm to protect the public and promotion of Internet access for modernization needs. They observe that the fundamental tenet of the Communist Party of China (CPC) is to control the media. Their article describes in detail the historical development of Internet in China, roles and responsibilities of various governing bodies on computer control, and various cyberspace regulations in place. The authors conclude that the government role of “technological modernizers” is in the ascendancy over the role 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.

Cyberspace control will fail

Scott E. Feir discusses the likelihood of Chinese authority succeeding in restraining the free flow of information in China. His article starts with a brief description of existing cyberspace regulations in China, their objectives and government structure in law enforcement. Feir also provides technical information on how to monitor and control information flows in the Internet. Cases were cited on how the Chinese authority has handled incidents related to “state security,” “state secret,” “public order,” and “criminal activity” in the past. As no Internet cases could be cited, the author discusses how the Chinese authority might react to similar Internet related incidents. The

author concludes that restricting access to the Internet through a combination of regulations and physical controls will ultimately fail. 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.” 381

He observes that Internet users in China will continue to seek and provide restricted information on the net. Government control of the Internet will be made more and more difficult with the advance in technology and as the thirst for information and desire for communication grows. 382 This article is the first legal discussion on the subject, and often cited by other authors.

Wendy Lei 383 (a law student) presents a similar view to Feir in her study on likely success of China’s Internet regulatory scheme. Her research is primarily based on newspapers, periodicals and magazines for cases, 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 four phases of Internet control, namely screening of information source, restricting access by user registration, monitoring of information flow, and severe punishment for abusive use.

Fei argues that the regulatory efforts would likely fail from due to advancement in

381 See n.23.
382 The author’s views appear to be typically confined to a foreigner’s perspective in understanding China.
technology, market incentives, and competition and lapse between government agencies. The author further 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 for expression/discussion in China and as a means of securing information from the West. The Internet remains to be as a potential threat to the Chinese authority but its decentralized nature is difficult to control. Various factors have a profound impact on Internet development in China, including economic growth, social/political stability, and economic incentive to join the WTO.

In his study, S. David Cooper\textsuperscript{384} reviews the challenges faced by China in promoting economic development with Internet technology. Specifically, he investigates the possible (democratization) effects brought about by Internet on the future of communism in China. Cooper observes that the control of Internet in China will not be entirely successful with technology and/or regulations. He then briefly discusses the impact of Internet on democracy with cases from Tibet, Hong Kong, Macau and Taiwan. He concludes with the observation that Internet would eventually liberal China from communist rule.

\textit{Cyberspace can be tamed}

Kristina M. Reed published two articles on the impact of “firewall” as a form of content control in China and Germany.\textsuperscript{385} A substantial amount of newspapers,
periodicals and magazines were cited and many websites used as references. The articles compare China and Germany in the following areas:

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

While it is difficult to block all or only illegal sites in the Internet, Reed is convinced that both countries are effectively regulating indiscriminate Internet access in China and Germany with the use of firewall technology. The firewall – screening however has profound and structural impact on business and economy development, including slowing down of trade and reduction in growth of e-commerce markets in both countries. Nevertheless Reed holds an opposite view to that of Feir who believes that Internet control would be impossible.

China has issued a cluster of regulations on Internet in 2000. Clara Liang’s article386 is an assessment of the effectiveness and impact of such and other Internet control measures. Apart from describing the regulations in detail, Liang observes that China authorities are actually following-adapting the same mainstream media control strategies (“bootstrapping”) to the use of Internet. Still Liang considers China’s regulatory regime a guarded success. China has derived moderate benefits from the Internet industry while being relatively successful in keeping political unrest in check. Like Kristina Reed,


Liang holds the view that China has managed to control access of the Internet contents effectively. In that China has successfully achieved a win-win situation in taming the Internet, i.e., being able to balance Internet control with modernization needs.

**Discussion**

The above literature study of the earlier years (1990s to early 2000) suggests that the research work conducted thus far in the field of cyberspace governance and Internet regulation in China has centered on how China attempts to restrict free flow of information to the public without sacrificing the advantages of Internet technology for economical development by the government. All of these studies are descriptive in nature and based mainly on newspaper accounts and secondary data. There is little original data gathering or independent empirical research. There is no critical analysis of data, empirical support of findings and unbiased debate over issues. In these articles, one does not find any independent investigation into the nature and prevalence of Internet abuse or computer attacks. There is no investigation into how the law regulating China Internet is implemented - interpreted, applied, received or impacted. For example, there is no investigation into whether any of the regulatory measures achieved its intended objectives, and how.

Most of the articles follow a similar pattern of organization and presentation: 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 observations and personal commented,
not learned and informed argumentation of relative positions. For example, all the articles start with the basic assumption that freedom of speech and unlimited flow of information is ipso facto good. In this regard, Chinese Internet development is being assessed against a set Western value postulates, as a give.

Being the first legal publication in 1997, Feir’s article is frequently cited in later research studies. But, as a defining literature, it is not well researched (data adequacy and originality issues) nor well argued (attending to different (Chinese) views on need for Internet control.). Fei’s conclusion that China would not be successful in controlling free flow of information in the Internet and that the technology is weakening the control of the Communist Party of China (CPC) over the people, is the mainstream position with many supporters. But there are other scholars who hold a distinctively different view, and should be given a fair hearing. For example, Liang after assessing the impact of Internet Regulations enacted in China since 2000 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 different views of two contending views of Internet control, both the above authors fail to substantiate their research with empirical data. This observation about limitation in research data and evidentiary support equally applies to all other

_________________________

388 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.
articles under review. For example, the imprisonment of Lin Hai\(^{390}\) and death sentences of Hao Jing-long and his brother\(^{391}\) were two popular Internet crime cases referenced but not analyzed with indigenous Chinese sources.

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 than analytical. More significantly, they are more revealing of the researchers (Western) mindset on issues of freedom of speech v.s. control in China than called for by research or support with evidence.

A Chinese rejoinder: Internet with Chinese characteristics

A Chinese researcher, using data collected from BBB (on usage and content),\(^{392}\) finds that both the Westerners (liberating narrative (277), Chinese (control discourse (278) have wrongfully assessed the utilities and functions of the Internet, and in turn fully appreciate the impact and implications of the Internet development in reformed China (274). The wrongful assessment by Western pundits resulted as much from blind

---

\(^{390}\) “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 online 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.

\(^{391}\) “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.

\(^{392}\) Research conducted in 2003-4 in Fuzhou & Xiamen in Fujian Province.
ideological zeal and passionate political advocacy, as it is from a lack of interest in understanding the socio-political reality of China through painstaking and unbiased empirical investigation. Specifically, the author found:

First, netizens mostly were male (60%), young (80% under 35), and educated (70% with senior high education).

Second, Westerners, while they complained of blockage to Western and offensive web sites, such as CNN, they enjoyed the many sources of information offered on the WWW (282). Internet users are inconvenienced, not totally deprived. The Internet makes certain information more available than others.

Third, many local Chinese, especially those who are older and educated, demanded Internet regulation. They understand the need for reining in a runaway Internet as a matter of Chinese moral principle, i.e., the need to protect kids from harmful effect of Internet. They approve and welcome the government’s attempt to protect the society, in promoting wholesome culture and outlawing corrupting ones. More importantly, they are fearful of luan, as with the disintegration of Russia or chaotic economic and political development in Taiwan.

Fourth, a majority of the young people in small towns (58% in 2004) are more interested in playing Internet games and surfing the net, than use it to discuss politics (Western assumption) or to do business (Chinese assumption).

Fifth, denizens are willing and able to lodge complains on the web in cases of injustice, but few call for the systemic change of Chinese political system in favor of a more freedom and democracy one, mimicking Western ones. In essence Western explanation of Chinese dissent is spurious, i.e., Chinese do not want a totally free, and unregulated Internet.
Sixth, Internet is entering a post-modern age. Netizens are using Internet in self-serving and individualistic way. This defies traditional model of political participation and social involvement. For example, Geis confirms that Chinese netizens prefer using BBB for inter-personal social-emotional communication,\textsuperscript{393} and not for political – logical exchange. According to Guobin Yang\textsuperscript{394} and Giese such Internet discourse is personal, intimate and anchored within Chinese history and culture,\textsuperscript{395} more so than those ideas and ideal promoted by the West.

**Chinese Contentions**

**I. Chinese cultural attitude towards crime, speech and control**

**Concept of crime**

In Chinese, “crime” is translated as “fan zui” or “violating” (“fan”) what has been “prohibited” (“zui”).\textsuperscript{396} In this way “fan zui” is more than “weifa” (violation of the law).\textsuperscript{397} It is a personal – moral failing making a person burden with moral guilt or “zui ren.”


\textsuperscript{396} Id. pp. 37 – 38.

\textsuperscript{397} “Fan” is violation of person, boundary, rule or norm. “Zui” is a sense of personal guilt. “Fanzui” is thus a violation of norm which result in personal guilt. *PYCED* 188R.
Historically and linguistically, the character “fan” first appeared in <Huai Nan Zhi. Xiuwu> equating “fan” with “chu”. “Chu” means to “touch” offensively. Thus “chu fan” means to “touch” and “violate” in the process. As to how people can violated the law, the legalist Han Fei (289 – 233 BC) observed in <Hanfeizi (韩非子). Wutu> (“Five Vermin”) that “Scholars violate the law with the pen, martial people violate (“fan”) prohibition by force.”

The character “zui” according to Mozi (470 – 391 BEC) is equated with violation (“fan”) of a normative prohibition (jin”), as in “fan jin”. The old word for “zui” has two radicals, “zhi” on top referring to “noose” and “xin’ the radical down bottom is a form of penal instrument. When “zhi” and “xin” were put together the character looks like the character standing for emperor “Huang - 皇”. Since in imperial China it was forbidden to use any words referring to or related to the emperor directly, the word “zui” was used as a substitute to offend the emperor, attracting punishment. Since then “zui” or “fan zui” means violating what is prohibited, or doing (thinking, saying, acting, appearing) something that should not be done, i.e., acting inappropriately or unreasonable.

In China, “fan zui” means acting out of order or conducting oneself inappropriately. More specifically, acting against what comes naturally and reasonably as embodied in “qing-li-fa.” “Qing” is “ren qing” or “conditions of human” within given a

---

398 Huainanzi (淮南子) also known as the Huainan Honglie 淮南鸿烈 ("The Great Brilliance of Huainan") was complied in 2nd BCE during the Han Dynasty. It presented literary and philosophical debates between Liu An (King of Huainan) and his guests in court.

399 PYCED 103R.
400 “Ru yi wen luan fa”
401 “Xia yi wu fan jin”
context, circumstances, and situation. This is akin to “reasonable person” standard in common law. “Li” is “tianli” (heavenly rule) or “lun li” (established human relations). This is akin to natural law standard in equity. “Fa” is state law (punishment) and family rule (discipline).

In imperial China, problems of “crime” and issues with “punishment” are thought about philosophically and theoretically as integrated governance issues. Historically, ideas of crime and punishment were discussed as part of the larger scheme of things, called the “cosmic order”.

From the beginning of time, the sage thinkers were pre-occupied with how to secure peace and maintain order under heaven. The dominant view is that peace and order is achieved first through personal self-cultivation by individuals as augmented with paternalistic regulations by the family and by virtuous rule of the emperor. In this way, the discussion of crime and punishment, law and order was blended imperceptibly into and merged holistically with the larger intellectual landscape and cultural discourse of political philosophy and social practice of good governance and social control.

The philosophy of good governance has one objective, how to perfect the emperor’s rule approximating mandate of heaven. The ultimate yardstick of good governance is the moral and physical well being of the people. Good governance


requires moral leadership and benevolent rule of the emperor (by and through his officials), manifested as stern discipline for intellectuals, ethical education for the public (especially the intellectuals), sound economic policy and paternalistic social programs by officials; all presented as universal principles and best practices of a good government.

**Freedom of speech**

China from antiquity is a well ordered and highly structured society, defined by *li* (rites) and aspired towards *ren* (benevolence). 405 As an ordered society, idea and ideal of “freedom” of speech, as we come to know it in the Western liberal democracies did not exist. As a “duty” (“zeren”) bound community, the


407 “Freedom of Speech,” *Stanford Encyclopedia of Philosophy* (“The topic of free speech is one of the most contentious issues in a liberal society.”)

http://plato.stanford.edu/entries/freedom-speech/

408 D. S. Shawayder, "The Sense of Duty,” *The Philosophical Quarterly*, Vol. 7 (27): 116 – 125 (1957) (To say some has a sense of duty is to say that he/she is doing what is right for the sake of it, irrespective of how he/she/others feels about it.). To say that someone has a “duty” to do things is not the same as saying someone has an obligation to do that thing; duty is to self while obligation to us. This is an important point to make because the idea that duty and rights are complimentary concepts, i.e., duty gives rise to rights, is misconceived. R. B. Brandt, “The Concepts of Obligation and Duty,” *Mind* New Series, Vol. 73 (291): 74-393, 376 – 377 (1964).

409 In Chinese “duty” is translated as “zeren” or “sense of responsibility (“yingai”). *The Pinyin Chinese – English Dictionary* (Hong Kong: Commercial Press, 1981) (PYCED), p. 868R. Morally, the Chinese do not distinguish between “zeren” and “ying gai” as in
“right” (“quanli”) to free speech is not recognized. This is not to suggest that “bounded freedom” of speech did not find expression in China, especially with the elites. Nor does it mean that there is no “duty to tell the truth”, e.g., intellectuals and officials who risked their life to fulfill a higher moral calling as with the need to “speak truth to power”.

_Bounded freedom of speech_

the saying: “Don’t mention it. We’ve only done our duty.” See “yinggai” at _PYCED_ 830R.

410 Contemporary Chinese translation of “right” is “quanli lì” or authority (“quan”) to benefits (“li”). _PYCED_ 563R. However, if one were to look back in history, the term ‘right’ did not exist. Wang Gungwu, "Power, Rights and Duties in Chinese History,” _The Australian Journal of Chinese Affairs_, No. 3: 1-26, 4. (Jan., 1980),


412 Laurence A. Schneider, _A Madman of Ch'u: The Chinese Myth of Loyalty and Dissent_ (Berkley and Los Angeles: University of California Press, 1980) (Chu Yuan (338 – 278 BC), a banished minister of Chu, exemplified the loyal dissent tradition in imperial China at great sacrifice to self.)

413 The idea of freedom being bound appears to be contradictory in terms. After all, freedom means not to be bounded, or unrestricted, without our willing consent. Freedom is defined as: “the condition of being free; the power to act or speak or think without externally imposed restraints.” [http://wordnet.princeton.edu/perl/webwn](http://wordnet.princeton.edu/perl/webwn) However, a minute’s reflection would reveal that freedom is always bounded, by cognition, by norms, by materials conditions. According to rational choice theory in behavioral economics, bounded rationality: “is used to designate rational choice that takes into account the cognitive limitations of both knowledge and cognitive capacity.” [http://www.sfb504.uni-mannheim.de/glossary/bounded.htm](http://www.sfb504.uni-mannheim.de/glossary/bounded.htm) According to anthropologists, rationality are informed and bounded by culture. Robert Boyd and Peter J Richerson, Norms and Bounded Rationality, In: _Bounded Rationality: The Adaptive Toolbox_. G. Gigerenzer and R. Selten eds. pp.281–296 (MIT Press, Cambridge, 2001). Finally, as argued by Marx
In the West, freedom of speech, as with all other freedoms must be exercised within the boundary of law, as ameliorated by local custom and contingent on personal relationships. In (imperial) China, speech as personal conduct and social activities is to be exercised within the strict confines of Confucianism.414

Confucius and (free) speech

Confucius or his followers did not explicitly discuss free speech or rights of assembly in his writings. For that matter the concept of freedom and liberty was never discussed. Confucius intellectual challenge is to design a perfect system of moral control, leaving nothing to chances. At another level, Confucius instructed upon how to achieve freedom through harmony with self, others and the universe.

“In this way, he could see freedom itself at the height of its sensibility, not merely as an instrument of a moral life, but as serving through the

material conditions of society define and determine the availability of freedom in any society: “But don't wrangle with us so long as you apply, to our intended abolition of bourgeois property, the standard of your bourgeois notions of freedom, culture, law, etc. Your very ideas are but the outgrowth of the conditions of your bourgeois production and bourgeois property, just as your jurisprudence is but the will of your class made into a law for all, a will, whose essential character and direction are determined by the economical conditions of existence of your class.” (Manifesto of the Communist Party) 414 Chester Holcombe, "The Moral Training of the Young in China,” International Journal of Ethics Vol. 14 (4): 445-468 (1904)(The whole purpose of a Confucius education was to create a perfect, virtuous person in every respect. This educational philosophy denied Chinese youth and students any individuality or independent thought. They were taught to fit in the society by practicing the five relations (emperor/subjects, parents/children, husband/wife, brothers/sisters, friends/associates,) and cultivate a virtuous self. Slight deviation from the moral percepts attached grave consequences, from isolation by people, rejection of family, expulsion from community, final banishment by law. Freedom of thought and action was no where to be found.)
imagination as a lens or means for presenting the richness of reality in varied and intensified ways. Freedom, thus understood, is both spectroscope and kaleidoscope of being. As spectroscope it unfolds the full range of the possibilities of human freedom, so that all can be examined, evaluated and admired. As kaleidoscope, it continually works out the endless combinations and patterns of reality so that the beauty of each can be examined, reflected upon and chosen when desired. Freely, purposively and creatively, imagination weaves through reality focusing now upon certain dimensions, now reversing its flow, now making new connections and interrelations. In the process reality manifests not only scientific forms and their potential interrelations, but its power to evoke our free response of love and admiration or of hate and disgust.”

By a careful reading his four books – *The Great learning, The Doctrine of the Mean, Confucian Analects, The Works of Mencius* - discerning readers should be able to understand the proper exercise - entitlement and control - of speech in imperial Chinese society.

First to observe is the fact that speech is an integral part of people’s personal conduct and social activities. It is governed by the moral universe Confucius. Thus observed the proper exercise of speech-conduct as a species of human activities was informed by Confucius basic philosophical postulates, moral percepts and ethical

---

415 GEORGE F. McLEAN, Chapter 16: KANT AND CONFUCIUS: AESTHETIC AWARENESS AND HARMONY.” In Liu Fangtong, Huang Songjie and George F. McLean (eds.) *PHILOSOPHY and MODERNIZATION in CHINA - CHINESE PHILOSOPHICAL STUDIES XIII* (n.d.)
principles, more generally worldview.

Confucius moral order is build upon the twin principles of *li* (rites) and *ren* (benevolence). People were admonished to seek virtue - follow *li* and sought after *ren* - as an unending quest of their life course. The journey to seek virtues started with “self-cultivation” and end with acting in accordance with “propriety.”

Self-cultivation required people to be internally driven and self-disciplined, not policed from without. As observed by this author into Confucianization of the law:

The cultured person who was expected to be self-controlled had to labor under a total control system which was unlimited in scope, policed internally, enforced punctiliously, sanctioned psychologically, seeking for the truth, probing of the mind, and never subject to a mistake. Self-control was thus a much more demanding and exacting form of social control than legal control.

More significantly, there is no special “right” to act as one sees fit in particular instances

---

416 The essence of Chinese cultural thoughts and key to Confucius teachings is that of “harmony” - individual obeying natural cosmic rules and following positive social norms, without question, still less dissent. Individuality is ruthlessly suppressed and personality actively transformed to make people conform to group expectations on way to be an integrated part of the collective whole, where the individual resided anonymously without a name and functioned silently without a voice. View in this manner, the Confucius man recalls the quintessential corporate (IBM) man; a negligible, if indispensable, part of a well oiled machine. Hung-Yok Ip Liang, “Shuming and the Idea of Democracy in Modern China,” *Modern China*, Vol. 17 (4):469-508, 476 (1991).

but a general “duty” to conform to moral expectations under all circumstances, including making or not making speech: “Yen Yuan asked about perfect virtue. The Master said:

“‘To subdue one’s self and return to propriety, is perfect virtue…” 418

Acting proprietarily means that people are to follow existing and exacting rules of conduct. This also means that people do not have the freedom to act spontaneously and speak at will: “Look not at what is contrary to propriety; listen not what is contrary to propriety; speak no what is contrary to propriety; make no movement which is contrary to propriety…”419

In terms of duty to act, the highest duty in imperial China is that of “xiao” (filial piety) to one’s family and “zhong” (loyalty) to the emperor. Together, Confucianism requires unquestionable obedience to superiors.420 In daily application, people were asked to look towards to superior for guidance and approval:

“Confucius said,” There are three errors to which they who stand in the presence of a man of virtue and station are liable. They may speak when it does not come to them to speak; - this is called rashness. They may not speak when it comes to them to speak; - this is called concealment. They may speak without looking at the countenance of their superiors; - this is called blindness…” 421

418 Book XII, Ch. I (1), Yen Yuan. James Legg (Trans.), The Four Books (Hong Kong Wenhua tushu gongsi, 1993), (p. 278)
419 Id. Book XII, Ch. I (2), Yen Yuan. (p. 278-9)
421 Id. Book XVI. Ch. VI (368)
This means that people should avoid disrupting the relationship between senior and junior, authority and charges. This also means that people should not be a dissenter and protester. 422

As to how to exercise speech, people are admonished to be cautious: Sze-man Niu asked about perfect virtue. The Master said,” The man of perfect virtue is cautious and slow in his speech.” 423 They should also avoid outlandish, slandering or startling statements: “Tsze-chng asked what constituted intelligence. The Master said, “Ya, he with whom neither soaking slander, nor startling statements, are successful, may be called farseeing.” 424 The following such Confucius speech rules would likely to preclude people from “free” expression of idea, still less open demonstration and public protest.

This understanding of speech exercise while true is but one side the story.

While the public might not have a right or freedom of speech, the emperor has an affirmative duty, as part of heavenly mandate, 425 to listen to the people’s problems and concerns. In order to make sure the emperor was informed of public opinions, the emperors through the ages have set up imperial Censors to give them feedback. Failing to listen to the people and accept criticism that might bring ruins to the state:

The duke then said: “Is there a single sentence which can ruin a country?”

---

422 The idea of “xiao” or filial piety to family and “chung” or loyalty to state was deemed a one of the most important quality of a subordinate. Michael Nylan, ”Confucian Piety and Individualism in Han China,” *Journal of the American Oriental Society* Vol. 116 (1):1-27 (1966).

423 Book XII, Ch. II(2), Yen Yuan. James Legg (Trans.), *The Four Books* (Hong Kong Wenhua tushu gongsi, 1993), (p. 278).

424 Book XII, Ch. VI(2), Yen Yuan. (p. 283). James Legg (Trans.), *The Four Books* (Hong Kong Wenhua tushu gongsi, 1993).

425 Book of Songs, “Heaven hears as my people hear, heaven seas as my people see.”
Confucius relied,” Such an effect as that cannot be expected from one sentence. There is, however, the saying which people have -‘I have no pleasure in being a prince, but only in that no one can offer any opposition to what I say!”

“If a ruler’s word be good, is it also good that no one oppose them? But if they are no good, and no one opposes them, may there not be expected from one sentence the ruin of his country?”

There was also one other group of individuals in imperial China that was required to keep the government, state or employer advised and informed of observed problems and issues with the government. The intellectuals assumed a special role and unique relationship with the emperor, government and state. The intellectuals, as educated junzhi or shi was duty bound to tell the emperor what was going on as “establishment intellectuals.” In doing so, the junzhi, consistent with Confucius teachings, was asked to conduct himself as conscience of the people and monitor of the state.

To conclude, the right to free speech, association and assembly is new to China.

---

426 Book XII. Ch. XV. (4), Yen Yuan. (p. 305). James Legg (Trans.), The Four Books (Hong Kong Wenhua tushu gongsi, 1993),
427 Book XII. Ch. XV. (4), Yen Yuan. (p. 305). Id.
429 Teresa Wright, “State Repression and Student Protest in Contemporary China,” The China Quarterly, No. 157:142-172 (1999) (Through the ages, intellectuals serve the nation and emperor by using their moral and intellectual judgment and not act subserviently(p. 1144)
They were imported foreign ideas and borrowed Western ideal.\textsuperscript{430} In imperial China free speech and public protest was not welcomed. \textsuperscript{431} People were only allowed to speak their mind when invited to and even then at their peril, if they say the wrong thing.\textsuperscript{432}

\textbf{Social control}

Crime prevention and social control in traditional China was realized through indigenous groups – starting with the family which provides the education and discipline for character building, the neighbors which provide the supervision and sanction against deviance, and the community which set the moral tone and customary norms to guide conducts. Finally, the state acts as the social control agency of a last resort in providing punishment against crimes, economic maintenance to avert personal deviance and social

\textsuperscript{430} Sun Fo; Raymond Gram Swing, "Democracy in China," \textit{Far Eastern Survey} Vol. 13, No. 9 (May, 1944), pp. 76-77 (Dr. Sun Fu, son of Sun Yat-sen, made a speech before the Central Institute of Chingking wherein he observed that there was no democracy in China, freedom of speech was suppressed and opposition to the party is eliminated. While this was understandable given China’s war-time condition, this was not acceptable to China’s international friends, the likes of U.S.)

\textsuperscript{431} Zhu Chunyu, \textit{Treatise on early Qin, Tang, Song, Ming, Qing media enterprise} ("Xin Qin, Tang, Sung, Ming, Qing chuanpo shiye lunji") (Taipei: Taiwan shangwu yishu guan, 1989). (Confucius taught that sage emperors need to be solicitous of people’s welfare and responsive in addressing their concerns; a testimony to Chinese indigenous democratic tradition. As early as the Zhou dynasty, there was system and procedure in place to allow people to express their opinions from presenting petitioning to lodging complaints to filing appeals (p. 47.)

welfare to anticipate civil disorder. In this regard, the Chinese has taken a broad notion of control that includes the internalization of norms (by the individual), socialization and disciplinary regime (by the family); setting up custom and accountability system (in the community), removal of criminogenic conditions (by the administration) and defining the moral and social boundary (by the state) (Gibbs, 1982:9-11). The Chinese approach comes close to Edward A. Ross’ definition of social control - “the molding of the individual’s feelings and desires to suit the needs of the group” – including supernatural, ceremonies, public opinion, morals, art, education which formed the normative structure of a society. In a very real sense, Chinese social control is of a totalitarian gem (Wittogel 1957) and of a disciplining type (Dutton, 1992).

Discussion

In a report published by Pew Internet & American Life Project (March 27, 2008), a Senior Research Fellow describes Chinese Internet control practices and rationalization as follows:

“The Chinese government has long tried to control its internet in many ways. It censors or blocks politically-outspoken blogs. It has arrested citizens on charges of "inciting subversion" for posting articles in chat rooms critical of the Communist Party. It passes Internet traffic through a "Great Firewall" designed to deny access to such international websites as Wikipedia, Technorati, all blogs hosted by Blogspot, and many sites maintained by the BBC. It also censors content on Chinese-based sites dealing with a host of topics, including the religious group Falun Gong, the 1989 Tiananmen incident, corruption among government officials, the
independence movement in Taiwan, a free Tibet, various human rights issues, political incidents, or citizens' uprisings. The government justifies its control of the internet by arguing "that [unfettered Internet content] damages China's unity and sovereignty, harms ethnic solidarity, promotes superstition, portrays violence, pornography, gambling or terrorism, violates privacy, damages China's culture or traditions."  

The above excursion into Chinese history, philosophy and culture on speech, crime and control provides a much needed foundation to put Pew’s observation in a broader and deeper context. Specifically, instead of condemning Chinese government’s cyberspace governance strategy and Internet regulation policy instinctively as abusive of human rights, they should considered them as good faith efforts to avoid chaos in society, promote welfare of the people and uphold morality of the country (civilization).  

What we learned from the above excursion is that crime is more than just a legal wrong; it is an immoral act the perpetration of which disrupts the “cosmic order” and causes “luan” (chaos) in society. More generally, crime is something that should not have had happened, happened (“bu gai”). As such illegal, immoral, and disorderly conducts are cut out of the same cloth, i.e., being “inappropriate” (“no gia”) and “unreasonable” (“bu he qing – li fa”) as acting against good order and discipline of a perfect society. In a highly cultured society that is China, past and present, correct ideas matters more than proper conduct and inappropriate ideas (from unconventional to dissenting to

433 Deborah Fallows, Senior Research Fellow, “Few in China Complain About Internet Controls,” Pew Internet & American Life Project (March 27, 2008)
http://pewresearch.org/pubs/776/china-internet
unwholesome) promises to pollute the minds of millions. It is imperative to arrest ideas than punish people for deeds.

Thus observed, aberrational (thought) acts, however innocuous on its face or well intended in origination, must be prevented from happening. Failing that order has to be restored at all costs. Furthermore, the imperial emperors then and the Communist Party now has an affirmative duty to maintain a perfect “cosmic order” against all challenges large and small, in thought, speech or deeds.

View in this historical qua cultural perspective, it is easy to understand why the Communist Party build the Golden Shield – Great Firewall to shelter Chinese citizens from the corrosive culture of the West. It is also easy to understand why Internet censor is put in place to block “free” but “irresponsible” speech: pornography, violence, gambling, dissent, which is corrupting (e.g., rights without duty), destabilizing (e.g., Falun Gong), disorderly (e.g., inciting a riot) and inappropriate (e.g., casting aspersion on government).

A good – responsible emperor (government) is also one who carefully listens to and otherwise conscientiously seeks out opinion of the people. This is why the Chinese leaders have promoted the Internet as a feedback device from the people, witness the person of President Hu and Premier Wen in encouraging the Internet to conduct “public supervision” of the government.

The 2007 CASS survey report: “Surveying Internet Usage and its Impact in Seven Chinese Cities” provides us with detail scientific data in support of our cultural

---

434 Directed by Guo Liang, “Surveying Internet Usage and its Impact in Seven Chinese Cities.” Center for Social Development Chinese Academy of Social Sciences (November, 2007)
observations above.

First, Chinese leaders are very concerned about the run away, wide spread, unpredictable and lasting (negative) impact of Internet on the Chinese society. This is compatible with cultural teachings, i.e., Chinese emperors were the embodiment of virtues, morality, and benevolence. This is evident by public expectation of government to do something about Internet vice and corruption.

Second, there is no unrestricted freedom to free speech. More importantly, government should promote proper ideas on way to building a utopian society. This is evident by the fact that there are persistent and shared public expectations about purging the Internet of unwholesome influences, especially on young people, from “pornography” to “violence” to “gambling” to “gaming.” This is manifested in the public opinion that Internet (content) needs to be controlled. In 2008 over 80% of the respondents think that Internet should be controlled and managed.

Third, Chinese leaders and public agreed that speech and Internet must be controlled because they cause harm, especially to the young ones. There are also agreement as to what constitute harm to people (interests - slander), society (stability – cultural revolution), nation (sovereignty – Taiwan), and culture (morality – porn). But

435 Li Xing, “Freedom to blog is not license to slander” China Daily, April 12, 2007.
http://www.marbridgeconsulting.com/marbridedaily/2007-12-29/article/7063/sarft_mii_co_issue_online_video_regulation
437 “China's Internet Cafe Associations Publish Joint Declaration,” China Tech News, September 11, 2009 (In order to strengthen self-discipline and purify the industry, China's Internet cafe industry associations in 30 provinces and cities, including Beijing, Shanghai, Shaanxi, Dalian, Xiamen, and Guangzhou, have jointly published a self-discipline declaration on "Internet cafe industry purification".)
Chinese leaders and the public differs on what constitute actionable harm, e.g., whether Falun Gong is a cult or religion or health exercise that should be subject to control, or whether June 4, 1989 is a belligerent rebellion to be suppressed or a legitimate protest to be supported. There is also a disagreement as to whether public intellectuals, acting as voices of conscience, should be punished. Lastly, quiet apart from the merit of any speech, whether such speech should be suppressed if they are sponsored by the West (human rights) and have the potential of causing disruption (inciting riots).

Fourth, two groups of net users, i.e., young and uneducated, are particular vulnerable to unfettered Internet and speech. The Chinese government has an affirmative duty to care for the weak, young and vulnerable. For example, in 2006, Guo Tiejun, director of a Shanghai-based cyber addiction rectification center, reported that 15% of Shanghai youth is addicted to the computer. The report is based on a random survey of 2,125 students from 34 middle schools, with eight senior middle schools, eight vocational schools, and 18 junior middle schools.\textsuperscript{438} In 2007, Institute of Psychology of the Chinese Academy of Sciences research found that: (1) "Internet addicts in China are as many as 10 years younger than those in the West. They are more susceptible." In China most addicts are between 15 and 20 years. In the West, they are between 20-30. (2) In China, teen addicts are transfixed by online games. In the West they have a wider range of interests. (3) There are 18.3 million teen users. Over 2 million are addicts. The survey was launched by the Beijing municipal committee of the Communist Youth League of China in 2005.\textsuperscript{439} In 2008, China shut down 44,000 domestic websites and homepages.

\textsuperscript{438} "15% of Shanghai Teenagers Addicted to Computers," Xinhua News Agency February 10, 2006. \url{http://www.china.org.cn/english/Life/157610.htm}
\textsuperscript{439} "Boys Will Be Boys, But Net Addicts Younger Than in the West,“
removed 440,000 pornographic live-streaming videos and arrested 868 suspects in 524 criminal cases last year.440

**Impact of computer and internet on Chinese values**

The computer is a powerful processing machine. The Internet is a pervasive communication tool. China’s economy cannot prosper without such technologies. On the other hand, computer and Internet changes the way we communicate and associate with each other. Chinese leaders are rightfully concerned about the adverse impact and long term implications of such information technologies on Chinese society, from value orientation to social stability to political radicalization.

In 2000, a pair of researchers from City University of Hong Kong investigated into the impact of Internet on value orientations in China and discovered discernible differences between users and non-users. (Table 2 below):

“For example, compared with nonusers, Internet users are less likely to subscribe to Communism (by -3%) and Materialism (by -15%) but far more open to Post-materialism (by +18%). However, these differences vanished when other independent and control variables were included to share the impact on value orientations” such as cognitive sophistication (measured by education) and information access.”

The findings were based on a survey of 2,664 respondents in the sample, 27% of which (30% in Beijing and 24% in Guangzhou) have adopted the Internet. The users

---


spent 9 hours a week on the Internet, 80% with local Chinese websites. 46% of the users have used the net for online chat or discussions, from personal hobbies to personal relations, to government and politics, and investment.441

Table 2 Values differentiation between users and non-users

<table>
<thead>
<tr>
<th>Value Orientation</th>
<th>Users</th>
<th>Nonusers</th>
<th>Differences Users - Nonusers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communism</td>
<td>14%</td>
<td>17%</td>
<td>-3%</td>
</tr>
<tr>
<td>Materialism</td>
<td>48%</td>
<td>63%</td>
<td>-15%</td>
</tr>
<tr>
<td>Post Modernism</td>
<td>38%</td>
<td>20%</td>
<td>+18%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Number of cases</td>
<td>529</td>
<td>1405</td>
<td></td>
</tr>
</tbody>
</table>


This large-scale survey report clearly shows that the spread of Internet affects value orientations of users. The Chinese leaders are thus wise to take affirmative steps to insulate the public, especially the young and less educated, from adverse influences of the Internet. More importantly the Party leaders now and emperors then have a moral duty from heaven above to protect, preserve and promote the Chinese civilization, manifested as pervasive collective culture and ingrained as deeply held personal values, against all foreign sabotages and every domestic challenges, as a public trust. The failure to do so would have dire consequences. Chinese leaders would have failed their duties. Sabotage and challenge to established ideas and ideal is a never ending process. Concessions and compromises only embolden opponents and empowers detractors, and in time leading to wholesale rejection of existing ideology and paradigm. The challenge to ideology and

undermining of paradigm is ipso facto a challenge to the legitimacy and authority of the leaders. If such defiance is allowed to persist, the stability and order of society will suffer.442

**Internet censorship: A case study**

On May 19, 2009, the MII issued “Notification regarding requirements for pre-installing green filtering software on computers” requiring the installation of free “Green Dam Youth Escort” - Green Online Filtering Software on all newly sold computer in China:

“In order to build a green, healthy, and harmonious online environment, and to avoid the effects on and the poisoning of our youth's minds by harmful information on the internet, the Ministry of Industry and Information Technology (MIIT), Civilization Office of the Central Committee of the Communist Party of China (CPC), and Ministry of Finance, in accordance with the Government Procurement Law, have used CPC financial capital to purchase one-year exclusive rights to use “Green Dam Youth Escort” Green Online Filtering Software (hereinafter referred

442 “China's New Security State,” *Wall Street Journal*, Dec. 9, 2009. (According to Public Security Minister Meng Jianzhu, “The Internet has become a major vehicle through which anti-China forces are perpetrating their work of infiltration and sabotage” “Mr. Meng called upon police officers to boost cooperation with high-tech companies…Internet police units in provincial and municipal public security departments have since mid-2009 received more funding and resources to erect firewalls and to track down "subversive" Web sites.”)

http://online.wsj.com/article/SB10001424052748704240504574585120857399040.html?mod=googlenews_wsj
to as “Green Dam Youth Escort”) along with related services so that the whole society may use it free of charge. After comprehensive testing and pilot use, the software has been shown to effectively filter harmful content in text and graphics on the Internet and has already satisfied the conditions for pre-installation by computer manufacturers.”

Mr. Qin, spoke-person of Foreign Ministry made clear that the function of “Green Dam Youth Escort” is to keep the Internet clean from pornography and violence: "The purpose of this is to effectively manage harmful material for the public and prevent it from being spread …The Chinese government pushes forward the healthy development of the internet. But it lawfully manages the Internet." MII made clear that while the installation of the “Green Dam” software is mandatory, it is up to the parents/guardian/owners to impose control by adjusting the content filtering software. Amid growing controversy over the apparent underhand censorship, the state media are now downplaying the compulsory aspect of the software:

"PC makers are only required to save the set-up files of the program in the hard drives of the computers, or provide CD-Roms containing the program with their PC packages…The users have the final say on the installation of the Green Dam Youth Escort, so it is misleading to say the government

compels PC users to use the software … The government's role is limited to having the software developed and providing it free."

The MII first issued a solicitation for purchase of “Green Dam Youth Escort” software on August 4, 2008. The software was developed by the Jinhui Computer System Engineering Company with input from Beijing Dazheng Human Language Technology Academy Co. Since then the software “Golden Dam” has been installed in all high schools. As of May 2009, 106 web sites provide free download of “Green Dam” software, with a total of 7.1725 millions downloads. 20967 schools in 36 provinces, autonomous regions and directed municipalities have installed such software.

A survey of 1813 respondents shows that 92% approve of the government’s initiative, but only 70% are satisfied with the quality and services of such a program.

The reaction from the community, foreign and domestic was immediate, strong and disapproving, especially from the West. The heads of 22 foreign organizations, including the U.S. Chamber of Commerce, the European-American Coalition of Service Industries (CSI), Computing Technology Industry Association (CompTIA), Consumer Electronics Association (CEA), Emergency Committee for

---

445 “MII will purchase Green Online Filtering Software or web users free.” (“信息产业部将购绿上过滤软件供网民免费使用”) Aug. 4, 2008. it.sohu.com


448 American Chamber of Commerce in China (AmCham-China), Business Roundtable (BRT), Business Software Alliance (BSA), Canada China Business Council (CCBC) Coalition of Service Industries (CSI), Computing Technology Industry Association (CompTIA), Consumer Electronics Association (CEA), Emergency Committee for
Business Council, the IT Industry Council and other associations from North America, Europe, and Japan wrote to Premier Wen Jiabao to "reconsider implementing the Green Dam requirements…The Green Dam mandate raises significant questions of security, privacy, system reliability, the free flow of information and user choice."

Internationally, Ed Black, president of the Computer and Communications Industry Association, observed that:

"This is clearly an escalation of attempts to limit access and the freedom of the internet. It has economic and trade as well as cultural and social ramifications… [China] …not only control their own citizens access to the internet but to force everybody into being complicit and participate in a level of censorship…I hope the US Trade Representative, the State Department and other agencies of government will try to step up and reverse the decision."\textsuperscript{449}

The OpenNet Initiative published a report finding:\textsuperscript{450}

\textsuperscript{449} Ashey Moses, “China's Green Dam-Youth Escort net filter draws fire,” \textit{The Age} June 9, 2009.

\textsuperscript{450} “China's Green Dam: The Implications of Government Control Encroaching on the Home PC,” OpenNet Initiative Bulletin
First: “Green Dam exerts unprecedented control over users’ computing experience. The version of the Green Dam software that we tested … Not only does it block access to a wide range of web sites based on keywords and image processing, including porn, gaming, gay content, religious sites and political themes, it actively monitors individual computer behavior, such that a wide range of programs including word processing and email can be suddenly terminated if content algorithm detects inappropriate speech.”

Second, “The functionality of Green Dam goes far beyond that which is needed to protect children online and subjects users to security risks…With minor changes introduced through the auto-update feature, the architecture could be used for monitoring personal communications and Internet browsing behavior.”

Third: “The effective level of parental control over the software is poor. Technically, the software may be turned off or uninstalled and the filtering settings adjusted. In practice, a large number of users accept pre-installed software and never change default settings.”

Fourth: “Mandating the use of a specific software product is a questionable policy decision. Introducing a product standard by mandating the use of a particular software product made by a specific company for individual use at a national level is unprecedented. … A product mandate provides a strong measure of central control at the cost of consumer choice, security, and product quality,

http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc
with implications for personal computer performance.”

Finally, there is a technical problem. The Green Dam software is not well designed to serve the purposed intended and posed unnecessary security risk for users. According to analysis by the Computer Science and Engineering division of the University of Michigan:

“We examined the Green Dam software and found that it contains serious security vulnerabilities due to programming errors. Once Green Dam is installed, any web site the user visits can exploit these problems to take control of the computer. This could allow malicious sites to steal private data, send spam, or enlist the computer in a botnet. In addition, we found vulnerabilities in the way Green Dam processes blacklist updates that could allow the software makers or others to install malicious code during the update process…. We found these problems with less than 12 hours of testing, and we believe they may be only the tip of the iceberg. Green Dam makes frequent use of unsafe and outdated programming practices that likely introduce numerous other vulnerabilities. Correcting these problems will require extensive changes to the software and careful retesting. In the meantime, we recommend that users protect themselves by uninstalling Green Dam immediately.”

Domestically, a survey by China’s largest portal Sina found that more than 80%

451 Ibid.
respondents opposed to Green Dam in June 2009.453

On June 28, 2009 “The China 2009 Declaration of the Anonymous Netizens” was published, declaring cyberwar on China:

“To the Internet censors of China,

We are the Anonymous Netizens. We have seen your moves on the Internet. You have deprived your netizens of the freedom of speech. You have come to see technology as your mortal enemy. You have clouded and distorted the truth in collaboration with Party mouthpieces. You have hired commentators to create the “public opinion” you wanted to see. All these are etched into our collective memory. More recently, you forced the installation of Green Dam on the entire population and smothered Google with vicious slander. It is now clear as day: what you want is the complete control and censorship of the Internet. We hereby declare that we, the Anonymous Netizens, are going to launch our attack worldwide on your censorship system starting on July 1st, 2009…..”454

Two professors challenged the “Green Dam” installation as violation of laws.455

453 “China backs down over controversial censorship software: Green Dam, which blocks access to porn and politically sensitive, websites, will not be compulsory, state media reports,” Guardian June 16, 2009.
http://justrecently.wordpress.com/2009/06/14/academics-five-obstacles-for-green-dam/
Profs Zhou Ze, a lawyer with China Youth University for Political Sciences in Beijing, and Wei Yongzheng have applied to the MII a hearing over the legality of the “Green Dam” installation.

(1) The installation might have violated Art. 7 of Unfair Competition Law, in that:

“The government and its organ shall not abuse its authority to force the others to purchase the commodities from appointed seller or prohibit the fair competition from the others. The government and its organ shall not abuse its authority to prohibit outside commodities from going into home market, or prohibit domestic commodities from going to outside market.” The MII in requiring manufacturers of personal computers to install the Green Dam software from two licensors, i.e., Zhengzhou Jinhui Computer Systems Engineering Co Ltd. and Beijing Da Zheng Language and Knowledge Handling Technology Co. Ltd, has prohibited free and fair competition.

(2) The installation might have violated Art. 8 Anti-Monopoly Law, which stipulates: “No administrative organ or organization empowered by a law or administrative regulation to administer public affairs may abuse its administrative powers to eliminate or restrict competition.”

(3) The installation might have violated Art. 32 Anti-Monopoly Law, which stipulates: “Any administrative organ or organization empowered by a law or administrative regulation to administer public affairs may not abuse its administrative power, restrict or restrict in a disguised form entities and individuals to operate, purchase or use the commodities provided by business operators designated by it.”
(4) The installation might have violated Art. 37 Anti-Monopoly Law, which stipulates: “Any administrative organ may not abuse its administrative power to set down such provisions in respect of eliminating or restricting competition.”

(5) The installation might have violated Art. 9 Law of the People’s Republic of China on the Protection of Consumer Rights and Interests which stipulates:
“Consumers shall enjoy the right of free choice of commodities services.
Consumers shall have the right to make a free choice of business operates of supply of commodities services, freely among varieties of articles firms of services and decide independently to buy not to buy any kind of commodities, to accept not to accept any item of services. Consumers shall have the right to make comparisons, differentiations and ions when they make a free choice of commodities services.” In essence, consumer should have a free choice of what software if any that goes into pre-sale computer.”

(6) The installation might have violated Article 3 of the General principles of Civil Law states, which stipulates: “Parties to a civil activity shall have equal status” and Article 3 of Contract Law which stipulates that “The parties to contract shall have equal legal status. No party may impose its will on the other party.”

As of 30 June 2009, the mandatory pre-installation of the Green Dam software was delayed indefinitely. However, Asian brands Sony, Acer, Asus, BenQ and Lenovo etc. continued to ship computers with “Green Dam” software installed. Many

---

American computer manufacturers were willing to go along.\textsuperscript{458} Finally, on 14 August 2009, Li Yizhong, Minister of MII announced the discontinuance of pre-installation of “Green Dam” policy, except for schools, internet cafes and other public computers.

On June 23, 2009, editor of \textit{Caijing Magazine}, Hu Shuli weight in with an objective analysis and sensible compromise.\textsuperscript{459} Hu basically applauded the MII for finally coming up with a workable proposal to protect the interest of the kids. No one wants Chinese children to grow up in an unwholesome environment. Given this common goal, the question is how to secure the Internet to protect the youth. It is here, that MII has failed. First, it failed to consult widely before “secretly” issuing the directive for installation of Green Dam.\textsuperscript{460} Second, it failed to provide the computer companies and public sufficient time to debate and prepare for the installation. The order was released only 10 days before launch. Third, it did not sufficiently test the Green Dam software, or allowing experts in the field to comment on its functionality. This resulted in a leaking “dam”. Fourth, the public have a right to be (un) informed. But “Preventing the Internet's ability to spread violent and vulgar information that corrupts youths is beyond the ability of social organizations alone. In this arena, public rights need support from state authority.” However, this support must be rendered as a service, not through


coercion. It must be voluntary from the society. Otherwise, state authority exceeds its limits, and the effort is bound to fail for being incompatible with the long-range goal of fostering civil society's growth.

“Here, the crux is how government agencies define public rights. MII has a good intention to "build a green, healthy and harmonious Internet environment" and "prevent harmful information from reaching young people." But the way it defines public rights is inappropriate, overlooking the rights of citizens to collect information. Add to that the ministry's inept execution of the directive, a delayed announcement and imprecise procedures, and in the end, the MII's decision was rendered unacceptable to the public. At this writing, Green Dam is set for launch. MII, after a long period of silence, responded to public outcry by saying that the software is to be "included or saved on PCs," not with mandatory pre-installation. The deadline is approaching, and the original directive is likely to become basically null and void.

“To correct these missteps, we recommend what would be the most suitable measures. MII, strictly following legal procedures, should use fair, open and transparent administrative procedures to acquire the best filtering software through competitive bidding. The type of information filtered should be clearly described. Any PC buyer should be able to get this free software and decide independently whether or not to install it.”

Discussion

This case study on “Green Dam-Youth Escort” provides us with an in-depth look at the problems and promises of Internet censorship. The case also captures the plethora of

issues attending the “Great Firewall” debate.

First, it is clear that the Chinese government feels that it has the duty to make the Internet a safe and wholesome platform for the people to use. This “paternalistic” role of state, i.e., country as a big family with emperor as the titular head and officials as caring father and mother, has been with China since the beginning of time. The following passionate call for government control from a high Chinese official is now legendary:

"If you have any children or you are expecting some, you can understand the concern of the parents over the harmful Internet content. The Internet in China is open and the Chinese Government endeavors to promote sound development of the Internet. However, the Government also regulates the Internet according to law so as to safeguard the interests of the public and prevent the spread of harmful content."\(^{462}\)

Second, it is also clear that Westerners from journalists to human rights activists to business organizations are adamant in their objections. The issue is Internet censorship vs. free speech. The real debate is over cultural superiority and national sovereignty, or “clash of civilization.” The West claims that freedom of speech is universal. The Chinese wants responsible and constructive speech making.

Third, the Chinese government made clear that the government and the end users (parents for child) have divided responsibilities in making the Internet safe for use. The government provides the (screening) tool and the users use the (screening) tools. This conforms to age-old Chinese teachings that all discipline starts with self, then family,

then clan and nation last. In essence, the state can do little to keep the Internet safe if the user (parents) does not want to.

Fourth, the Western idea of free speech in and out of Internet runs counter to Chinese conception of “cosmic” order where every idea, thing and person has a place. Each person should act his role and only say and do what is right and proper. Beyond that, the state has the right to intervene to restore order and propriety.

Fifth, the government is most concerned about the corrupting influence of the Internet on the younger generation and will stop at nothing to hold them harmless in the Internet age. More than securing the young ones from moral endangerment, the government has an obligation to inculcate right thinking and proper behavior in the next generation. For the Chinese government not to assume the responsibility of conditioning perfecting the youth is being irresponsible and immoral.

Sixth, Green Dam represents a shift in Internet control strategy, consistent with a maturing citizenry in search of a harmonious society, from government control to household control, from external censorship to self-discipline, from macro-supervision to micro inspection, from categorical control to customized control, from direct control to indirect control, from government control to third part control

463 The case further reveals an ambivalent and complex relationship between government and Internet businesses. It shows that private businesses can be recruited for the control of the Internet. Indeed, many Chinese netizens see the Green Dam more as a sweet business deal for the software company than an effective control measure. This kind of outsourcing and privatization of control had long caused concern, and the Green Dam controversy brought the issue back into the public limelight, raised concerns about future state-market collusion. Guobin Yang, “Green Dam” as a Case of Online Activism in China,” Columbia University Press Blog. July 1, 2009.

http://www.cupblog.org/?p=663
Seventh, Green Dam fails because it fails to convince the people that it is necessary: The Green Dam policy indicates that there is still a surprising degree of bluntness in the exercise of state control over the Internet. In recent years, the Chinese government has demonstrated new levels of sophistication in affairs of Internet governance. One sign is the adoption since 2004 of a soft-management approach, which emphasizes self-discipline, civic responsibility, and the use of legal rather than administrative power to contain harmful contents. Part of the reason why the Green Dam policy met with such strong resistance is that it represented an unbearably heavy-handed approach to Internet control.464
Chapter Seven

Conclusion

Comprehensive approach is a dominant crime fighting strategy in China. The effectiveness of such a strategy in cyberspace control has yet to be empirically validated. There are good reasons to believe that the effectiveness of comprehensive control is a contingent one. Comprehensive cyberspace control works on some targets and not others, e.g., regulation works better with Internet bars than at home.

China is keen on protecting young people from many of the ill effects of the Internet, from gambling to pornography to corrupting influence (mostly from the West.) In fighting against corrupting influences on Internet, Chinese adopts multiple measures.

Education. One such measure is by promoting the “National Youth Civilized Use of the Internet Pact.” The Pact is a long-term strategy. It aims at educating the youth to the proper use of the Internet in a civilized and responsible manner. The campaign events, organized by the China Communist Youth League and local communities, conduct awareness training and enlist young people to help fight against Internet pollution, incivility and crime.\textsuperscript{465} One of the criticisms is that it curbs creative thinking of the youth. Interestingly, some U.S. officials also suggested the youngsters to learn "cyber-ethics"\textsuperscript{466}. The U.S. Department of Justice institute Cybercitizen Partnership,\textsuperscript{467} to


teach young people the right way to use the Internet. There is even a DOJ web page designated for cyber ethics information.\textsuperscript{468}

\textit{Law enforcement.} MPS conducts routine raids on Internet bars as it restricts their opening hours. This has a deterrence effect on youth who has to rely on Internet bars to be hooked up. The introduction of safe – clean Internet bars is yet another proactive measure to safeguard the youth from mixing with the wrong crowd or being exposed to criminal opportunity. Regrettably, the “Green Dam” project ailed to launched as a result of domestic resistant and foreign objections.

\textit{Administrative supervision/surveillance.} MPS inspects Internet bars for safety. Officers surf the net to rid youth of corrupting influences or victimization traps. In Shenzhen police created Jingjing and Chacha cartoon mascots of the Internet Police in China. The purpose of Jingjing and Chacha is “to let all Internet users know that the Internet is not a place beyond the law; the Internet Police will maintain order over all online behaviors.”\textsuperscript{469}

Comprehensive control is build upon Felson’s routine activity theory of crime prevention. Felson postulates that crime happens as a result of convergence of a motivated offender, an available opportunity and a lack of capable guardian. Education programs helps to shape young people’s attitude towards the Internet, making them use the Internet in a positive and healthy manner. By restricting the hours of the Internet bar, the police hope to stop youth from bad company and unwholesome influence at nights.

\begin{itemize}
\item \texttt{http://cybercrime.gov/AGCPPSL.htm.}
\item \textsuperscript{468} See “General Information – Cyber Ethics”, \textit{Computer Crime and Intellectual Property Section (CCIPS)} of the Criminal Division of the U.S. Department of Justice, at \texttt{http://cybercrime.gov/}.
\item \textsuperscript{469} “How much policing is needed on the Internet?,” \textit{The China Post}, Oct. 4, 2009.
\end{itemize}
Finally, the police inform the young people that their activities on the net are always watched. The young people are less likely to commit Internet crime if they know that their activities are being watched.  

In preventing people from being informed of online news and opinions disapproved by the Chinese government, such as human rights debate and Falun Gong, the Party is performing its traditional paternalistic role in safeguarding the welfare of the people and security of the nation. For examples, 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, breached Chinese system of censorship over the Internet by way of e-mails into China. The group distributed the pro-democracy magazine throughout China with mass e-mailing to about 250,000 addresses compiled from commercial and public lists. Unlike vice websites that contain pornographic 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 Falun Gong, are handled individually as they emerge. Of course, China

---

470 “Eight Ministries Joint Conference on Special Program to Keep the Internet Clean from Malevolent Information,” Xinhua News Agency, May 1, 2002.

471 Maggies Faggies, “Electronic guerrillas breach blocks set up by the government to keep citizens from seeing unorthodox news and opinions on the Internet,” LA Times 1999.

472 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.
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 for the Chinese government to curb all external websites that keep changing and increasing. China will keep watching and leave this problem area “as is”, 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 the 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 other aspect. More conscious efforts in making legislation for Internet are deem necessary.

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 tamed, 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.

Looking forward, 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 fill commercial needs.

From a technological perspective, China needs to speed up research and development on critical IT products, such as encryption, firewall, and router, to meet expanding security needs without depending on foreign security and communication technology. As long as China has to rely heavily on imported technology, China will not be able to avoid computer attacks from abroad, nor hope to be able to exercise comprehensive control over her domestic cyber security situation.

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

Internet is extra-territorial nature and knows no sovereign boundaries. Cybercrime 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, sharing information, exchanging intelligence, and enforcing law.

Through Internet, Chinese people are able to achieve effective government an improved their quality of life. Cyberspace governance id required to help achieve such
goals. 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.”

PART III

CYBERSPACE GOVERNANCE IN HONG KONG
Chapter One

Introduction

As an international finance centre, Hong Kong enjoys many of the benefits generated by CMC in the new Information Age. CMC is a much more cost-effective media relative to traditional communication channels. Internet allows people to communicate with each other on demand, in real time, anonymously, interactively, anywhere in the world. With a click of a mouse, people can share a large amount of information and process multiple business transactions, anywhere in the world. People are brought closer together in a virtual world surpassing geographical distance, time zone differences, social inhibitions, or cultural barriers. The cyberspace’s norms, culture and etiquette are much more causal, informal, and spontaneous than the conventional ones.

The Internet is also a much better way to do business and conduct commercial intercourse. In the words of a Hong Kong IT consultant:

“The promises held out by the Internet are at once compelling and confronting. The Internet promises to lower costs, streamline logistics, and shorten production cycles. The Internet holds out the promise of reaching new markets and new customers by eliminating the tyranny of distance. And the Internet promises to eliminate intermediaries. Those who move fast stand to gain a significant competitive advantage.”


The Hong Kong economy is increasingly and irreversibly relying upon CMC and Internet to operate. In 2002, “A Self Assessment of Hong Kong’s Readiness for E-Commerce” observes that PC penetration is growing fast. It has grown from 34% in 1998 to 50% in 2002. Between 2000 and 2009, PC connected to Internet grew from 36.4% in 2000 to 73.3% in 2009.

There were over 190 ISPs offering competitive price and services. Consumers in Hong Kong are making use of the Internet to send e-mail, surf the cyberspace, carry out research and conduct low value retail transactions. Consumers however do not as a rule rely on the Internet to purchase high value items. Hong Kong business executives are aggressive using the Internet to promote their ventures. 35% of the businesses are using Internet for their operations, including marketing, customer support, enhancing efficiency and conducting transactions electronically. Hong Kong government has taken the leadership in using the Internet to conduct business, e.g., electronic tendering and purchasing since April 2000. The above picture has not changed in 2003.

See also “Report on Internet Use by Hong Kong Industries,” Cyberspace Center, The Hong Kong University of Science and Technology, May 1997. (The Report describes and discusses the findings of three computer utilization surveys conducted in Hong Kong, namely Hong Kong Software Manufacturers survey, Hong Kong Computer Industry survey and Mini-survey of Hong Kong's General Industries. The findings show that between 97 – 98% of the computer industries are connected to the Internet. With the general industries, the connectivity varies, from a low of 28% for the Household industry to a high of 71% for the Electronics industry to 42% for the Women's Garments industry and 30% for the Piece goods, with Textiles industry in between.)

http://www.cyber.ust.hk/survey/index.html

Secretary of Commerce and Economic Development (CED) speech at Hong Kong International Computer Conference 2010 opening ceremony.

See “APEC E-Commerce Readiness Assessment Guide – A Self Assessment of Hong
Internet has also become a catalyst for Hong Kong economic reform, social development and political change.\textsuperscript{480} The amount of government, business, financial and personal communications and data transmitted by and stored in computers is beyond imagination. As Marjory Blumenthal, a perceptive scholar of the U.S. National Research Council observed: “As the next century [21\textsuperscript{st} century] begins, 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”.\textsuperscript{481}

The import, impact, influence and implications of Internet in Hong Kong go far beyond what has been contemplated, and promises more surprises ahead. The history and legacy of computer in Hong Kong is still being written.\textsuperscript{482}

\textsuperscript{479} See discussion in “Information Technology Usage and Penetration in Hong Kong” infra.

\textsuperscript{480} For the diffusion of Internet in Hong Kong, see William FOSTER, Seymour GOODMAN and Zixiang (Alex), “TAN, The Internet and E-Commerce in Greater South China (Taiwan, Hong Kong, Fujian, and Guangdong)” (September 28, 1999) \url{http://mosaic.unomaha.edu/schina.pdf}


\textsuperscript{482} Hong Kong has no National Information Infrastructure Project to speak of before 1995, though Hong Kong Information Technology Federation and Hong Kong Generation Chamber of Commerce has championed for its establishment. On December 6, 1996, the Hong Kong Legislative Council (Legco) Panel on Information Policy was formed to discuss the issues surround: “Development of Information Highway and Internet in Hong Kong.” Correspondingly the government established the Information
Information age raises new criminality concerns as it aggravates traditional criminal problems.\textsuperscript{483} Internet is vulnerable to attack by hackers and computers can be used to defraud millions of dollars. A tiny computer virus is capable of bringing down a huge multinational corporation.\textsuperscript{484}

Similar to many developed societies,\textsuperscript{485} the phenomenal growth in the usage of

\begin{flushright}
\textsuperscript{483} See Kam C. Wong and Georgiana Wong, Law and Order in Cyberspace: A Case Study of Cyberspace Governance and Internet Regulations in PRC,” Proceeding Papers, Third Annual Conference of the Asian Association of Police Studies (AAPS), (Hong Kong: AAPS, 2002).


\end{flushright}
computers, CMC and Internet in Hong Kong has been accompanied by an increase in computer related crime since the late 20th century. 486

Table 1: Total number of computer crime cases in Hong Kong – 2002 - 2008

<table>
<thead>
<tr>
<th>Year</th>
<th>Total No. of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>791</td>
</tr>
<tr>
<td>2007</td>
<td>634</td>
</tr>
<tr>
<td>2006</td>
<td>741</td>
</tr>
<tr>
<td>2005</td>
<td>653</td>
</tr>
<tr>
<td>2004</td>
<td>560</td>
</tr>
<tr>
<td>2003</td>
<td>588</td>
</tr>
<tr>
<td>2002</td>
<td>272</td>
</tr>
</tbody>
</table>

Source: Hong Kong Police Force

As observed by the UN:

“The burgeoning of the world of information technologies has, however, a negative side: it has opened the door to antisocial and criminal behavior in ways that would never have previously been possible. Computer systems offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of computer crime, society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service...

coordination and national security. Even a small glitch in the operation of these systems can put human lives in danger. Society's dependence on computer systems, therefore, has a profound human dimension. The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity for misuse or criminal activity. The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security.”

This has led to the call for critical review of cyberspace governance philosophy, law and practices.488

The study of cyberspace governance in Hong Kong is still at its early stage.489 As


489 The first comprehensive study of computer crime in a given industrial is conducted by the Hong Kong Monetary Authority (HKMA) in July 1997. SECURITY OF BANKING TRANSACTIONS OVER THE INTERNET (1997). (One of the missions of HKMA in the cyber era is Electronic Banking and Technology Risk Management: “As a bank regulator, the Hong Kong Monetary Authority (HKMA) aims to, among others, create a safe and sound environment for electronic banking (e-banking) development in Hong Kong without standing in the way of progress. In this connection, the HKMA has implemented a comprehensive e-banking and technology risk management supervisory framework for the banking industry in Hong Kong.”) The first comprehensive legal and policy study of computer crime and cyberspace governance in Hong Kong was conducted in March 2000 with the launching of the “INFORMATION INFRASTRUCTURE
yet there are few scholars or policy makers who have taken the challenge to conduct a defining, much less definitive, comprehensive study on the subject. Academic publications on cyberspace governance in Hong Kong are rare. This book is an

ADVISORY COMMITTEE - Establishment and Work of Inter-departmental Working Group on Computer Related Crime,” IIAC Paper No. 06/2000 Security Bureau. (The paper outlines the background, organization and charter of the Inter-departmental Working Group on Computer Related Crime.) The “Inter-departmental Working Group on Computer Related Crime Report” (HKSAR, 2000) (hereinafter “HKSAR Computer Crime Report(2000)”) was published in September 2000. The “Terms of Reference” for the Working Group are: “(a) identify the challenges to law enforcement, for example, in respect of evidence gathering and prosecution, arising from such developments; (b) review the adequacy of existing legislation and relevant administrative measures to deal with the challenges of identified in (a) above; (c) examine international developments and trends in this area, and draw lessons for Hong Kong as appropriate; and (d) make recommendations to address the inadequacies identified, taking into account the need to balance law enforcement facilitation on the one hand and the cost of compliance, financial or otherwise, on the other.” The first in-depth study of academic research into one aspect of computer crime, i.e., that of “dark figures” of computer crime in Hong Kong, is that of Chan, Hilton Kwok Hung, “Comparative study of reported and unreported computer crimes,” 2000. Ph.D. Thesis. Hong Kong University of Science and Technology. (hereinafter “Computer Crime Thesis(2000)”) (The study address three issues: “(a) What are the differences between reported and unreported computer crimes? (b) Why are computer crimes underreported? (c) What is the process leading to the reporting and non-reporting of computer crimes?.”)

http://lbxml.ust.hk/th_imgo/b672003.pdf

attempt to fill in the research gap.

This project investigates into computer related crime and control in Hong Kong; its philosophy, policy and practices. Particularly, the book will investigate the following questions: Is there a computer crime problem in Hong Kong? How did the people and government of Hong Kong “discover” computer crime, cyber risks and electronic privacy? What is the nature, incidences, prevalence and distribution of the computer crime problem? What are the causations of the computer crime problem? What are the control philosophy adopted and remedial actions taken by the Hong Kong government in addressing the issue? Are the control measures effective in providing for a safe and secure Internet environment in Hong Kong?

Part III on cyberspace governance in Hong Kong consists of eight chapters. After this brief “Introduction” (Chapter One), Chapter Two: “Researching into Hong Kong Cyberspace Governance” discusses the research difficulties and data sources availability in mounting such a study. Chapter Three: “Information Technology Usage and Penetration in Hong Kong” describes the current status and future trend of computer penetration, IT usage and Internet popularity in Hong Kong. Chapter Four: “The Discovery of Cyber Risk, Computer Crime and Electronic Privacy” investigates into the emergence of computer crime and electronic as a public concern and government problem since the mid-1990s. Chapter Five: “Nature, Prevalence and Distribution of Computer Crime” provides an overview of the background – nature, extent, distribution – of computer crimes in Hong Kong. Chapters Six: “Cyberspace Governance in Hong Kong” explores Hong Kong government’s approach to the control of computer crime and regulation of cyberspace. Chapter Seven: “Conclusion” summarizes the key findings of this research, ending with some recommendations in improving cyberspace governance
Chapter Two
Researching into Hong Kong Cyberspace Governance

Research Difficulties

There are four major problems and issues with researching into computer crime and cyberspace governance in Hong Kong. First, how to define computer crime. \(^\text{491}\) Second, how to ascertain the nature and extent of computer crimes in Hong Kong? Third, there is a lack of valid, reliable and accessible data bearing upon computer crime occurrence and cyberspace control policy in Hong Kong. Fourth, there is a lack of computer crime research in Hong Kong.\(^\text{492}\) As a result of the above observed issues and obstacles, research into computer related crime and policy on cyberspace governance in Hong Kong is not well developed, or not as well developed as it should be.

First, there is no commonly agreed upon definition of what computer crime

\(^{491}\) The need for and problem with defining computer crime are well recognized within computer crime literature. The issue has never been satisfactory resolved, much less approaching any consensus. There are basically two approaches – legislative and academic. The former defines computer crime with reference to harm and the later with regard to causation. See Section on “Definition of Computer Crime” in “Research Needs for Computer Crime Introduction” Computer Crime Research Center. [http://www.crime-research.org/eng/library/Introduction.htm](http://www.crime-research.org/eng/library/Introduction.htm)

entails in Hong Kong, a worldwide issue that equally afflicts Hong Kong government officials, IT professionals and academic researchers. There are two definitional issues, namely: What is the meaning of “computer”? What is a “computer crime?”

What is the meaning of “computer”? There are two concerns for legislation. First, is the term “computer” specifically defined enough to give notice to criminal violators to achieve deterrence purpose and serve due process function. Particularly, does the term “computer” includes other systematic application features, existing now or in the future, other than the stand alone computer set, i.e., monitor, keyboard and central processing unit. For example, does the term include Wireless Application Protocol? Second, is the term “computer” general enough to net all intended computer related crimes and anticipate future development and innovations in computer technology? After

493 The issue was first raised in 1992 by Hong Kong Chamber of Commerce. In 1992 the Hong Kong Chamber of Commerce’s Information Services Committee submitted a detailed response to the government’s proposed Computer Crimes Bill, see “Report on Inter-Departmental Working Group on Computer Related Crime Response by the Hong Kong General Chamber of Commerce,” Comments of Hong Kong General Chamber of Commerce (02/2001)


496 See HKSAR Computer Crime Report (2000), pp. 10 – 20, specifically 3.7 (“In the narrow sense, the term “computer” commonly conjures up the image of a stand-alone machine…However, in a broad sense…the term is increasingly taken to refer to a whole host of other items such as network computer systems and many mobile electronic communication device.”) The HKSAR Computer Crime Report (2000), intimated a due notice concerns without explicit discussion. See 3.8 “A legal definition leave “the matter entirely to the interpretation of the court …depending on the inclination of the judges in question.” It complete ignored the need to discuss issues presented by specificity of legislative definition and administrative of justice, e.g., deterrence, just desert, judicial
reviewing 35 Hong ordinances and examining 76 sections, the HKSAR Computer Crime Report (2000) recommends defining “computer” as “information system”, as defined in the Electronic Transactions Ordinance (Cap. 553). 

Electronic Transactions Ordinance does not define “computer” but use “information system” to mean: “a system which…

(a) processes information;
(b) records information;
(c) can be used to cause information to be recorded, stored or otherwise process in other information system (whatever situations); and
(d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated).

The HKSAR Computer Crime Report (2000) acknowledges that: “The terms “computer crime” and “computer related crime” are rather amorphous…” They can refer to crimes directed at the computer, e.g., hacking, crimes using computer as the medium, e.g., Internet gabling, and crimes where the computer play a minimal role, e.g., pornographic advertisement on the Internet.

The term computer crime generally refers to three kinds of crime, namely,


HKSAR Computer Crime Report (2000), p. 3.9 (“The definition should not be unnecessarily restructure lest it fails to cover new devices or technology.”).
computer crime in the strict sense, computer-related crime, and computer abuse. A pioneer and guru of computer security in the U.S., Donn B. Parker prefers a descriptive “definition” (of sort):

“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 are or are affected by computer and data communication systems, including people about whom data is stored and processed in computers.”

According to Parker, computer crime cases may involve computers playing in any one or more of the following roles:

1. Computer as object - such as destruction of computers or computer data or programs contained in a computer;
2. Computer as subject - such as fraud cases where financial data is being illegally changed;

---

501 For a historical development of computer crime, from computer being used as instrumentality of crime to computer being attacked as the object of crime. See Sam McQuade, “So-called “Cybercrime”: Its Nature and Manageability.” An Appendix Report Submitted for Inclusion in The President’s Commission Final Report on Critical Infrastructure Protection (August 1997). (The author argues for a change of paradigm (Kuhn 1970). He prefers the use of “cybercrime” over computer crime because digital technology allows crime to moves away and beyond the narrow confine of computer crime to other emerging fields of vulnerabilities, e.g., alternation of digital photography and stealing of digital images.)

3. Computer as 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. Computer as symbol - such as using non-existent computers for intimidation or deception.503

A more conceptual definition is supplied by Dennis Longley and Michael Shain:

“willful or negligent unauthorized activities that affect the availability, confidentiality and integrity of computer resources.”504 Availability of computer resources might be blocked in cases of denial of services attacks, such as spasm.505 Confidentiality of computer resources might be compromised by means of unauthorized intrusion such as hacking.506

503 Unless other specified, the terms, including ‘computer crime’, ‘computer-related crime’, ‘computer abuse’, and ‘Internet crime’, are used interchangeably throughout this paper.


505 “83% Of U.S. E-Mail Is Spam,” Security Pipeline, May 25, 2004 ((More than 97 percent of all spam is sent to the U.S., the U.K., Germany, Australia, and Hong Kong, with 84% for U.S., 52% for UK, 41% for Germany, 30% for Netherlands and 27% for Hong Kong.) For a technical paper on how denial of service attacks work, see Frank Jargl, Jorn Maier, Stefan Schlott, Michael Weber, “Protecting Web Servers from Distributed Denial of Service Attacks,” 10th International World Wide Web Conference (WWW10) Refereed Papers. For defense against DDSA, see David K. Y. Yau. John C. S. Lui. Feng Liang, “Defending Against Distributed Denial-of-service Attacks with Max-min Fair Server-centric Router Throttles,” Tenth IEEE International Workshop (2002) pp. 35 - 44

506 “Study: Israel, Hong Kong hotbeds for hacking attacks,” Silicon Valley.com, July 8, 2002 (“Overall, the United States generates by far the most cyber attacks, followed by
Integrity of compromises when hackers try to steal, alter, contaminate or destroy existing data base. 507

The difficulty with defining computer crime is much exacerbated when applied. In practice, it is difficult to apply a book definition of computer crime to a street setting. For example, if a computer is stolen for the proprietary data or operational software, it would not be classified as a computer crime. However, if knowledge of computer technology is used to commit such a crime, such as unauthorized access and illegal downloading of data from the same computer, it is. Yet both of them are understood conventionally as stealing by common law’s definition, i.e., “taking, carrying away, property of another, if intent to permanently deprive the owner thereof”. 508 There are also many new and emerging illegality and criminality that does not involve the use of computer but other digital technology, e.g., theft of software in a camera or illegal interception of telecommunication services. 509

Second, Hong Kong faces a challenge in understanding the true nature, extent and

Germany, South Korea, China and France, according to a report from Riptech Inc., a managed security service provider based in Alexandria, Virginia.”)


507 'ILOVEYOU' computer bug bites hard, spreads fast,” CNN. Com, May 4, 2002 (The “I LOVE YOU” viruses substituted existing Web development (including ".js" and ".css" files) and multimedia files (JPEGs and MP3s) with a VisualBasic file with a similar name. It started with an attack on Hong Kong and moved west.)


distribution of computer crime in the community.\textsuperscript{510} Without such understanding, controlling computer crime becomes very difficult.\textsuperscript{511}

It is well recognized in other countries that there are always “dark figures” in cyberspace crime,\textsuperscript{512} i.e., undetected, unreported and/or unrecorded crime cases.\textsuperscript{513} For

\textsuperscript{510} For an extensive discussion on the challenges in policing computer crime in Hong Kong, including “dark figures” of computer crime issue, see Kam C. Wong, “Introduction: Asian Policing in the 21st Century,” \textit{Proceeding Papers, Third Annual Conference of the Asian Association of Police Studies} (AAPS), (Hong Kong: AAPS, 2002).

\textsuperscript{511} See M. E. Kabay, “Understanding Studies and Surveys of Computer Crime,” (2001), particularly “1.1 Value of statistical knowledge base” (With out reliable data and statistics it is impossible to conduct risk management which requires consideration of security investment vs. computer risks.)


\textsuperscript{513} Dark figures of computer crime are not the only problem in understanding computer crime. Even if all the computer crimes are reported correctly they still need to be analyzed in a meaningful way. Here we suffer from not knowing everything we want to know about the computer hardware – processors, operating system, software – UNIX based intranet vs. Window NT based server and security structure – firewall - being used that contribute to possible security breach. Accounting for all these technical specifications will be difficult if not impossible when faced with millions of attacks a year, e.g., DOD got attacked 250,000 times in 1996. See M. E. Kabay, “1.3 Understanding Studies and Surveys of Computer Crime,” (2001), particularly “1.e Limitations on the applicability of computer crime statistics.” Ryan, Julie J.C.H. and Theresa I. Jefferson reviewed the methods and findings of 14 widely circulated computer security surveys conducted from 1995 to 2000 and found them to report widely different results on key issues: number of respondents (56 – 4300), having security policies (19\% to 83.4\%), reporting security breach (42\% to 73\%), unauthorized access – insider (44\% to 62.9\%), outsider (4\% & 8\% to 58\%), concern with connectivity (security) (8\% to 57\%),
examples, the FBI’s National Computer Crime Squad estimates that between 85 and 97 percent of computer intrusions in U.S. are not even detected, much less reported. With sponsorship from the U.S. Department of Defense, Richard Power experimented with attacking 8,932 computer systems. He discovered that only 390 (4.37%) systems managers were able to detect the attack. Only 19 (4.87%) the attacks were reported.

Hong Kong faces similar dark figures of computer crime problems. Computer crimes are highly technical in nature. Some are hidden within the computer architecture, and computer important or high priority (56% to 84%). (Not each of the 14 surveys was asked the same question). From the survey over survey the authors observed that there were substantial methodological issues and many data validity problems. They cautioned against using the survey results indiscriminately. e.g., making unwarranted generalization beyond the study sample itself. "The Use, Misuse and Abuse of Statistics in Information Security Research," Proceedings of the 2003 ASEM National Conference, St. Louis, MO.

M. E. Kabay, “Understanding Studies and Surveys of Computer Crime,” (2001), particularly “1.2.1 Detection” (There is no way to know how much computer crimes are not detected. The information security industry estimate the rate to be 10%. This figure is backed up by opinion and based on consensus, not as a result of empirical research.)

http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.pdf

M. E. Kabay, “Understanding Studies and Surveys of Computer Crime,” (2001), particularly “1.2.2 Reporting” (The information security industry estimate the rate of non-reporting to be 10%. This figure is based on professional experience supported by interviews with clients. DOD research showed that only 1/500 cases were ever reported, i.e., 0.002) http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.pdf


Computer Crime Thesis (2000) (The study addresses three issues: “(a) What are the differences between reported and unreported computer crimes? (b) Why are computer crimes underreported? (c) What is the process leading to the reporting and non-reporting of computer crimes.”) http://lbxml.ust.hk/th_imgo/b672003.pdf
e.g., “Trojan horse” viruses. Others are not even discernible until long after the fact. Thus, in most cases, the unsuspecting victims (lay computer users) are not even aware of the existence of computer virus embedded in their program. More often than not computer crimes happen under the nose of the computer owner without the person knowing it. Even when they are aware of the crime, e.g., illegal intrusion, they may not be immediately aware of the scope and extent of the damages, until months and years later. Finally, most computer crime victims just chose not to report computer crimes.

There are many reasons for victims not reporting computer crimes. Many corporations especially those in service sectors, such as finance and insurance industries, are reluctant to report a cyber-crime case, particularly with cases that reflect poorly on its internal security, e.g., embezzlement of funds by insider, or unsecured e-business platform, e.g., identity theft at ATM machines. Such crimes will jeopardize their corporate image, breach clients’ confidentiality, undermine customers’ trust, or simply dilute company’s good will. In the United States, annual FBI/CSI Computer Crime and Security Survey have asked respondents to provide reasons why they do not report intrusion to law enforcement. In 2002 the reasons given were: negative publicity (76%), competitors would use to advantage (67%), unaware that could report (57%), civic

518 See General Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, GAO/AIMD-96-84 (1996). (Defense Information Systems Agency (DISA) estimates that DOD is attacked about 250,000 times per year. Only about 1 in 500 attacks is detected and reported.)
519 2002 FBI/CSI Computer Crime and Security Survey. Methodology: 3,500 survey instruments were dispatched to information security professionals in the United States with 503 responses for a response rate of 14%. The low response rate and lack of follow up research for reasons for non-response make the findings not generalisable, but only suggestive of pattern, to the whole of United States.
remedies seemed better (51%).\textsuperscript{520}

There is also a legitimate concern about the effectiveness of the overworked and underpaid Hong Kong cyber cops in solving their techno-security problem. Whatever the Hong Kong Police is good for, they are not known for or excel in solving computer crimes. Finally, many Hong Kong business people or IT professionals believe that the most cost-effective way to deal with computer crimes is not to report to the police or prosecution by the criminal justice system, but through self-help and private policing. In sum, as of now, the private sector has little confidence in the Hong Kong government’s ability or capacity in dealing with their computer crime problem.\textsuperscript{521}

There is a need for valid and reliable data to support theoretical driven and empirically based computer crime and cyberspace governance research in Hong Kong. Computer crime data in Hong Kong is maintained and reported by Information Technology Services Department. Computer crime cases are also available at the HKP website but are not categorized. The Customs and Excise Department rarely report any of the cases they handle in a timely or meaningful way. In all, the official computer


\textsuperscript{521} From interviewing IT professionals, computer crime victims and HKP cyber crime investigators Chan, observed that the non-reporting of computer crime in Hong Kong resulted from a number of factors: ignorance of crime or harm; uncertainty of detection, prosecution or punishment, expensiveness of detection measures; fear of consequences: public image, reveal of weaknesses, exposure to civil liabilities; difficulty in assessing loss of information, such as customer data base or proprietary information; lack of motivation, e.g., data are not insured or insurable; corporate executives consider computer crime internal business problems not external criminal matter and finally when computer crime is discovered it might to too late to report. Computer Crime Thesis (2000), pp. 123 – 4.
crime data do not present us with a total or accurate picture of computer crime problems in Hong Kong as it should. Presently, they just show the tip of an iceberg. Questions abound: How many computer crimes are out there? How can computer crime be classified and categorized in a meaningful way? What are the nature and extent of computer crime in Hong Kong, and how might they be different from other comparable jurisdiction, e.g., Shanghai? How are computer crimes distributed in the social space, such as in terms the age, education, economic, social standing? More importantly, what are the causes, impact and implications of computer criminalities in Hong Kong? Answering of these questions require the collection and classification of data not currently made available in Hong Kong anywhere. Effective cyberspace governance awaits the development such a database.

Data Sources

The data used in this book come mainly from publications of the Census and Statistics Department, the Hong Kong Security Bureau, and the Hong Kong Police Force (HKP) of the Hong Kong Special Administrative Region (HKSAR). The HKSAR government information websites, its homepage at www.info.gov.hk, is open to the public.

The Security Bureau is one of the key players in the policy formation process of cyberspace governance in Hong Kong. In March 2000, the Security Bureau chaired an inter-departmental working group (the Working Group) “to examine existing legislation and related issues regarding computer crime” 522 in Hong Kong. The “Inter-

departmental Working Group on Computer Related Crime Report (September 2000)” was issued. In July 2001, the HKSAR government announced that it would adopt the suggestions recommended by the Working Group. In as much as the Report is used to develop computer crime control and cyberspace governance policy in Hong Kong, it is most useful for this study.

Computer crime statistics are quoted primarily from the HKP websites on “Information Security & Prevention of Computer Related Crime” at www.infosec.gov.hk. Crime cases are cited from HKP or local news media. Statutory Laws of Hong Kong are extracted from the Bilingual Laws Information Systems (BLIS), the database of the Laws of Hong Kong on Internet, serviced by the Department of Justice. Reference is also made to the proceeding papers of two distinct international conferences held in the territory: the First Asia Cyber Crime Summit523 and the Third Annual Conference of the Asian Association of Police Studies524. These conferences were hosted by two of the most prominent professional organizations in the field. Together they provide valuable secondary data and unique professional insights into this research effort.

523 The First Asia Cyber Crime Summit was hosted by the Centre for Criminology of The University of Hong Kong on 25-26 April, 2001 in Hong Kong.
524 The Third Annual Conference of the Asian Association of Police Studies (AAPS) was held on 29 July, 2002 in Hong Kong. The theme of this conference was: Asian Policing in the 21st Century.
Chapter Three

Information Technology Usage and Penetration in Hong Kong

In the 2001 Policy Address, the Chief Executive of HKSAR stated the urgent need for the community to transform rapidly from an industrial economy to a knowledge-based economy.

“Nevertheless, if we are to preserve our economic vitality, create greater prosperity, and maintain living standards, economic restructuring is the only way ... We are encouraging traditional industries to use technology and innovation to improve competitiveness ... The importance of electronic commerce is increasingly being recognized … we announced our revised ‘Digital 21’ IT strategy to promote the development of e-commerce under the theme ‘connecting the world’.” 525

In the 2003 Policy Address, the Chief Executive reiterated the importance to “enhance Hong Kong’s information connectivity, upgrade the necessary infrastructure ” in promoting economic restructuring. 526 The message is loud and clear: the deployment of IT is vital for Hong Kong’s economic development.

Before investigating into computer crime situation in Hong Kong, it is most necessary to put things in context, i.e., understand the information technology (IT) usage

526 Chief Executive Tung Chee Hwa, “The 2003 Policy Address: Capitalising on Our Advantages; Revitalising Our Economy (8 January, 2003)”, (HKSAR, 2003), paragraphs 14-17.
and Internet penetration in the community, and with it the emergence of computer criminality as a social, economic and legal problem.

According to Commissioner Tsang Yam-pui of the HKP, in 2000 there was an upsurge of computer crime from 34 cases in 1998 to 358 cases in 2000. He was quick to observe that the upsurge in computer crime corresponded with rapid growth in Internet usage in the community. “There are about 200 Internet Service Providers (ISP) as opposed to 56 in 1995, with 2.5 million as opposed to 600,000 users at the beginning of 1999.”

The message Commissioner Tsang conveyed was clear: advancement in IT technology breeds computer crime.

In 2003, there is a total of 3.2 million Internet users aged 10 and above. Since 2000, there are two major surveys on IT usage and penetration, one amongst household members and the other with the business sector. Both are conducted by the Census

529 The Thematic Household Survey conducted by the C&SD collects “information on IT usage and penetration in order to gain better understanding of the latest development of IT in the community.” The 2003 survey was conducted during May to August of 2003. Similar surveys were conducted yearly from 2000 to 2002. For survey methodology and more statistical analysis, see C&SD, “Thematic Household Survey Report No. 15: Information Technology Usage and Penetration” (HKSAR, 2003).
530 The 4th annual survey on Information Technology Usage and Penetration in the Business Sector was conducted by C&SD during May to August 2003, under the auspices of the Commerce, Industry and Technology Bureau. The objective is “to collect information relating to information (IT) usage and penetration in the business sector. The survey results would be useful for reference in the development of IT strategy in Hong Kong”. For survey methodology, see C&SD, “Report on 2003 Annual Survey on Information Technology Usage and Penetration in the Business Sector” (HKSAR, 2003).
and Statistics Department (C&SD).531 In 2003, the Household Survey reports a total of 1,479,000 households with personal computers (PC) at home. This represented 67.5% of the total households in Hong Kong. 60% of all computer households had their PCs connected to the Internet.

Table 1 below presents a yearly comparison of the IT usage and penetration between 2000 and 2003 amongst household members. It indicates increasing penetration of PC and Internet in the community; from 49.7% in 2000 of all houses to that of 67.5% in 2003. The rate of growth has slowed somewhat since the biggest jump in PC owner between 2000 to 2001 of 10.9%. The recent (2002 to 2003) increase is half that of 2000 to 2001, i.e., 5.4%. Of those households with PC, 88.8% were connected to the Internet.

People in Hong Kong start to use computer when they are young. The survey shows that persons age 10 or above having access to PC and use of Internet services in 2003 reaches 56.2% and 52.2% respective, an increase from 2000 of 43.2% and 30.1%. Amongst this age group, it is clear the Internet use rate grew faster, from 30.1% in 2000 to 52.2% in 2003 or net growth of 22.1%, than PC accessibility rate, from 43.3% in 2000 to 56.2% in 2003 or 13%.

Utilization of electronic business services is very high in Hong Kong. 93.6% of respondents 15 and over have used business services 12 months before the survey. The most commonly used e-business services include Octopus card for paying transportation

531 The other set of data is compiled by the annual “Internet Use in Hong Kong” survey from 2000 to current by City University of Hon Kong. The latest one being “Internet Use in Hong Kong: The 2008 Annual Survey Report (Jan. 2009)”. The survey report upon Internet penetration by population, sex, age, education, occupation, income, time, behavior, etc. newmedia.cityu.edu.hk/hkip/HKIP2007en.pdf
fare and purchasing, Automatic Teller Machine (ATM) for banking transactions, Interactive Voice Response System (IVRS) for purchasing, e-cash/Easy Pay System (EPS), Payment by Phone Service (PPS), online searching for information, and job searching, etc. Though the actual use of Internet for actual purchases were very low, i.e.,

Being a bi-lingual society, Hong Kong has 47.3% of the persons within the age group of 10 or above having knowledge of the use of Chinese input methods. The 2003 survey further reveals that the rates of using PC and Internet services are higher among younger, better-educated, and students. For example, 37.8% of the Internet users are aged 10 to 24 years old and 68.2% of the users have attained an educational level of Secondary school or with Matriculation. 66.7% of all Internet users are economically active, i.e., employed and unemployed person, whereas 26.7% of the total users are students.

| Table 1 – IT Usage and Penetration in Household (Years 2000 to 2003) |
|-------------------------|---------|---------|---------|---------|
| **Descriptions**          | **2003** | **2002** | **2001** | **2000** |
| a. Households with PC among all households in HK | 67.5%    | 62.1%    | 60.6%    | 49.7%    |
| b. Households with PC connected to Internet among (a) | 88.8%    | 84.6%    | 80.4%    | 73.3%    |
| c. Households with PC connected to Internet among all households in HK | 60.0%    | 52.5%    | 48.7%    | 36.4%    |
| d. Persons aged 10 or > using PC in 12-mths before survey within the age group | 56.2%    | 54.0%    | 50.3%    | 43.1%    |
| e. Persons aged 10 or > using Internet in 12-mths before survey within the age group | 52.2%    | 48.2%    | 43.3%    | 30.3%    |
| f. Persons aged 15 or > using e-business services for personal matters in 12-months before survey within the age group | 93.6%    | 92.6%    | 88.5%    | 84.9%    |
| g. Persons aged 15 or > using online purchasing services for personal matters in 12-months before survey within the age group | 7.0%     | 4.9%     | 5.6%     | n/a      |
| h. Persons aged 10 or > with knowledge of using Chinese input methods within the age group | 47.3%    | 42.8%    | 39.9%    | 29.8%    |
| i. Persons aged 15 or above aware of Electronic | 34.0%    | 39.7%    | 32.4%    | 28.7%    |
Table 2 below summarizes the key findings on IT usage and penetration in the business sector\(^5\) between years 2000 and 2003.

The survey reports that in 2003 55%, 48%, and 13% of all business establishments used PC, have Internet connection, and with Web page/Web site access, respectively. This is an increase from 2000, i.e., 51.5% (PC), 37.5% (Internet) and 7.3% (Web page). There are more establishments having Web page/Web site in 2003 (13%) than before, i.e., 12% in 2002, 11% in 2001 and 7.3% in 2000. The Web page provides an easy to use, interactive, global electronic platform to transact business, i.e., marketing products and services, or conduct administration, e.g., keeping personnel records or exhibiting corporate policy.

The 2003 survey indicates that 18.6% of the establishments have used the website for online delivery of goods, services and information, and 8.9% for online ordering of the firm’s products and services. Only 5.3% of the firms use their website for the purpose of online payment transactions.

\(^5\) For the 2002 survey, questionnaires were mailed to the 4,635 selected establishments of which 3,378 were successfully enumerated, representing an overall response rate of 95%. See C&SD Report. The response rate is consistent to that of the 2001 survey. “A total of 3,492 establishments selected in accordance with a scientifically designed sampling scheme were successfully enumerated in the survey, constituting a response rate of 96%. The fieldwork was carried out between April and June 2001 through mailed questionnaires followed by field officers’ visits/telephone calls to verify the information and provide assistance in completing the questionnaires.” See ITBB, “LegCo Panel on Information Technology and Broadcasting: 2001 Surveys on IT Usage and Penetration in the Household and Business Sectors (January, 2002)”, (HKSAR, 2002).
It is also reported that the most frequent usage of PCs is in the financing, insurance, real estate and business services sector, constituting 76.6% of all transactions in 2003. The same sectors have the highest percentage (68.9%) in the use of PCs with Internet connection. The lowest percentage of use is found in the transport, storage and communications sector; only 31.5% of such firms used PCs and barely 26.5% have Internet connection.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Establishments using PC</td>
<td>55.0%</td>
<td>54.5%</td>
<td>49.7%</td>
<td>51.5%</td>
</tr>
<tr>
<td>b. Establishment having Internet connection</td>
<td>48.0%</td>
<td>44.2%</td>
<td>37.2%</td>
<td>37.3%</td>
</tr>
<tr>
<td>c. Establishment having Web page/Web site</td>
<td>13.0%</td>
<td>11.8%</td>
<td>10.7%</td>
<td>7.3%</td>
</tr>
<tr>
<td>d. Establishment having acquired goods, services or info thru’ electronic means</td>
<td>9.6%</td>
<td>7.1%</td>
<td>6.2%</td>
<td>4.9%</td>
</tr>
<tr>
<td>e. Establishment having received goods, services or info thru’ electronic means</td>
<td>51.0%</td>
<td>45.2%</td>
<td>40.0%</td>
<td>35.3%</td>
</tr>
<tr>
<td>f. Establishment having sold goods, services or info thru’ electronic means</td>
<td>1.1%</td>
<td>1.5%</td>
<td>1.1%</td>
<td>0.3%</td>
</tr>
<tr>
<td>g. Establishment having delivered goods, services or info thru’ electronic means</td>
<td>13.6%</td>
<td>12.1%</td>
<td>12.4%</td>
<td>8.1%</td>
</tr>
</tbody>
</table>

(Source: Census and Statistics Department)

The above two annual surveys inform us of several computer usage development trends in Hong Kong, and their associate social problems:

1. Public awareness and usage of IT, including computers and Internet, has significantly increased, in business, public, as well as private sectors. The increase in awareness and use is attributable to a number of factors: educated population, good telecommunication infrastructure, and free government.533 The increase in popularity –

possession, connection, usage and access - leads to a proportional growth in motivation and opportunity for potential criminality to be committed in the virtual space.

2. The growing rate of PC users amongst the youths, students and better-educated present a new challenge to the government in its strategic planning for crime prevention and control. The ready availability and ease of access to computer promotes delinquencies and create computer criminals. With the youths, students and educated, public education and ethical indoctrination work better than punishment.

3. Electronic commerce is vital to the development of Hong Kong as a regional financial center and international business hub. A safe e-business environment is essential gain public confidence.

In the above chapter, we have discussed the importance of IT to Hong Kong economic development. We particular note the social crime concerns raised by such patterns of unbridled growth to the local government, i.e., increase in social deviance, compromise of computer ethics, violations of information ethics, and threatening of

(Basing on the work of Dutton, Rogers and Jun, the authors argued that Hong Kong is a “dream venue” for the Internet. It has a well-developed telecommunications infrastructure, a financially well off population, an educated people, a stable legal environment, and no government regulation of content.) Dutton, W. H., Rogers, E. M., & Jun, S. H. (1987). “Diffusion and social impacts of personal computers,” Communication Research, 14, pp. 219-250. (The authors argued that social status, personal attributes, social-cultural setting, technology level/features determines computer adaptation and use, and in time determines social impact of home computing.)
electronic commerce.

We now turn and investigate how the computer and Internet has been used for criminal purposes in Hong Kong, starting with how cyber risks, computer crimes and electronic piracy has gained public awareness and government attention in Hong Kong.
Chapter Four

The Discovery of Cyber Risk, Computer Crime and Electronic Privacy

Cyber risk is a psychology phenomenon. Computer crimes are an intangible entity. Electronic privacy is a moral concept. All of them are not real or material. That is to say, they have to gain public awareness – cognitive recognition and emotional resonance - before they become real, and of consequence to people.

Historically and culturally China has no conception of Intellectual rights.534 Historically, the best philosophy of governance was practices by Emperors Yao and Shun535 and prefect statehood found in the Zhou Dynasty. Culturally, the sage writings contain the secrets of Chinese civilization. Generations of students are taught to recite the classical literature of the old.536 Scores of intellectuals are expected to regurgitate sage writings of the past. All the officials were required to be conversant with and justify their action by historical materials, classical literature and sage sayings. It is not only not a crime to recite classical authorities without attribution, it is a sign of intellectual proneness to be able to recite at will passages after passages, sometimes verbatim, of learned treatises.537

534 Peter Yu, “The Second Coming of Intellectual Property Rights in China.” Occasional Papers in Intellectual Property, Benjamin N. Cardozo School of Law, Yeshiva University, No. 11 (Imperial China has no notion of property right) p. 4.
536 Confucian learning was canonized during Eastern Han Dynasty. The Emperor decreed the Five Confucian Classics to be the standard text for education: Book of Poetry, Book of Documents, Spring and Autumn Annals according to Mr. Tso (Zuo), Book of Zhou Rites, and Book of Changes. The Five Classics” provided external standard and internal bearings for self-cultivation and government rule.
537 Peter Yu, “The Second Coming of Intellectual Property Rights in China.” Sect II:
Hong Kong people are a pragmatic lot. They are known for making fast money than following established principles. They try hard to work around rules and making short cuts, instead of honoring the rights of others and respecting the rule of law.\textsuperscript{538} To them anything and everything in life is a “game” to be won at all costs.

Given this understanding of China historical approach to intellectual property and contemporary Hong Kong people’s mindset toward copyrights, it should come at no surprise that people do not take Intellectual property rights seriousness nor understand computer crime completely. It takes time for the Hong Kong people to be re-educated.

The “discovery” of cyber risk, computer crime and electronic privacy resulted from the convergence of a number of factors, including post 1997 privacy concerns, “Causes of Privacy and Counterfeiting Problems in China” pp. 16 – 18. (Unlike the west, imperial China did not consider copying the words and work of others to be morally apprehensible, socially inappropriate or legally wrong. It is consider “a noble” things to do.) See also William P. Alford, \textit{To Steal a Book Is an Elegant Offense: Intellectual Property Law in Chinese Civilization} (Stanford, CA: Stanford University Press, 1995) \textsuperscript{538} Fung Chi Pang, \textit{Singing against Hong Kong People} (Speedy rainbow publishing limited 1998) (The four defining personality traits of Hong Kong people are opportunism (zhisheng), use the brain (silao), struggle with everything (busaha) and to go all out(fen shen). Hong Kong people are pragmatists and utilitarian, more Machiavelli than Kant.) The personality of Hong Kong people is shaped by the unique history of Hong Kong Most of the people in Hong Kong came as “political” migrants escaping from Communist China trying to make a living on a barren rock ruled by the British as a colony. The Hong Kong people’s survival instincts make them impatient with rules and contemptuous of rights; pragmatism is the only ideology. Richard Hughes, \textit{Borrowed Place Borrowed Time} (London: Andre Deutsch, 1968). For a more detail analysis of Hong Kong people’s social psychology, or as the author put it games Hong Kong people play, George Adams, \textit{GAMES HONG KONG PEOPLE PLAY - A SOCIAL PSYCHOLOGY OF THE HONG KONG CHINESE} (GEORGE ADAMS 1991).
government IT security concerns, private e-banking security considerations, foreign anti-
privacy and anti-counterfeiting campaigns, domestic moral outrage with off shore
Internet gambling, and public awareness of sensational computer crime news.539

Post 1997 privacy concerns

One of the major driving forces behind making Internet safe and secure comes from a most unexpected quarter, pre and post 1997 politics. One of the major issues in the run up to the 1997 transfer of sovereignty of Hong Kong, from the British government to PRC, is that of human rights protection, including that of privacy.

As far back as 1984, the “Joint Declaration” paved the way for the return of Hong Kong to China on July 1, 1997.540 The Joint Declaration provided that the rights and freedoms enjoyed by the Hong Kong people will last for 50 years, to be secured by a Basic Law.541 Specifically, Article 3(5) of the Declaration provides:

“(5) The current social and economic systems in Hong Kong will remain unchanged, and so will the life-style. Rights and freedoms, including those of the person, of speech, of the press, of assembly, of association, of travel, of movement, of correspondence, of strike, of choice of occupation, of academic

541 The drafting of Basic Law begins in 1985 when the National People's Congress appointing a Basic Law Drafting Committee, comprising of more than 50 prominent China mainland and Hong Kong members.
research and of religious belief will be ensured by law in the Hong Kong Special Administrative Region. Private property, ownership of enterprises, legitimate right of inheritance and foreign investment will be protected by law. “

As a result, the Basic Laws of Hong Kong (1997)\textsuperscript{542} specially provide for the guarantee of basic human rights. Specifically, Article 29 provides that the "homes and other premises of Hong Kong residents shall be inviolable. Arbitrary or unlawful search of, or intrusion into, a resident's home or other premises shall be prohibited."

Article 30 further provides that the "freedom and privacy of communications of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communications of residents except that the relevant authorities may inspect communications in accordance with legal procedures to meet the needs of public security or of investigation into criminal offenses."

Rights provided under The Joint Declaration (1984) and Basic Law (1997) are not self executing. They need to be implemented by law, and actualized with executive actions. This fell on the shoulder of Christ Pattern (1992 to 1997), the last (28\textsuperscript{th}) Governor of Hong Kong. In this regard, the Governor made clear that: “The British role is to discharge our colonial responsibilities honourably and competently.”\textsuperscript{543} In practice that means pursuing a two prone strategies: introducing democratic institutions and


The work of Hong Kong Law Reform Commission on “Reform of the law relating to the protection of personal data” (1989 – 1994) (1994 Report) should be understood in this historical and political context. Hong Kong transition of sovereignty began long before 1997 and continued with Chris Patten democratization, liberalization and legalization policy.

The “Terms of reference” of the 1994 Report states: “On 11 October 1989 the Attorney General and the Chief Justice referred to the Law Reform Commission for consideration the subject of "privacy". The Commission's term of reference was: "To examine existing Hong Kong laws affecting privacy and to report on whether legislative or other measures are required to provide protection against, and to provide remedies in respect of, undue interference with the privacy of the individual with particular reference to the following matters:

(a) the acquisition, collection, recording and storage of information and opinions pertaining to individuals by any persons or bodies, including Government departments, public bodies, persons or corporations;

(b) the disclosure or communications of the information or opinions referred to in paragraph (a) to any person or body including any Government department, public body, person or corporation in or out of Hong Kong;

(c) intrusion (by electronic or other means) into private premises; and

(d) the interception of communications, whether oral or recorded…

Following on the heel of 1994 Report, The Law Reform Commission took another look at some of the more salient privacy issues raised by electronic data interception, interference and theft. This resulted in the issuance of: “REPORT ON PRIVACY: REGULATING THE INTERCEPTION OF COMMUNICATIONS"

“The rapid expansion of the Internet, and the resultant increase in the amount of personal information available on-line, has made the public more concerned about the privacy of their communications. Service companies are likely to use privacy as a competitive weapon in winning customers. … The growth in the use of electronic communications systems by industry has increased the need for security of those communications in such areas as banking and finance. Service carriers are aware that an inability to safeguard customer information will adversely affect customer relations and their business. Another concern is that of theft of proprietary information”

More ominously, the 1996 Report warned of the coming privacy crisis.

“The development of advanced communications networks is likely to be hindered unless service carriers can assure the public that there is adequate security for their communications. The President of the United States Telephone Association asserts that:

544 The 1996 Report “Terms of References” are anchored within that of Reform of the Law relating to the Protection of Personal Data and states: “The issues raised at items (a) and (b) in the terms of reference were addressed in the Law Reform Commission report on Reform of the Law relating to the Protection of Personal Data published in August 1994. Most of the recommendations of that report were adopted with the enactment of the Personal Data (Privacy) Ordinance (Cap. 486) on 3 August 1995. This report deals mainly with item (d).” See paragraph 5 to “Introduction” of 1996 Report.

545 See 10 (b) to “Introduction” of 1996 Report.

546 See 10 (c) to “Introduction” to 1996 Report.
“If the public becomes skittish about using the public network for fear either that it is full of ‘back doors’ designed so that their local sheriff will be developing a dossier on them based on call set-up information, that fear will translate into reduced use of the system. The result will be the loss of billions of dollars in potential revenue, and along with that many of the jobs, the taxes, and the benefits that we anticipate from the information age.”\textsuperscript{547}

While the 1996 Report mainly addressed government interception of electronic data and intrusion into computer domain, the warning applies to cyberspace interception and intrusion of all kinds.

This detour into 1997 politics and law of the Hong Kong government and Hong Kong Law Reform Commission on “privacy (1994 Report, 1996 Report) makes abundantly clear that the “discovery” of computer crime and electronic privacy in Hong Kong was driven by many forces and advanced along a number of paths. In the ultimate analysis, it matters less how computer crime, cyber security and electronic privacy issues are “discovered” as when the Hong Kong government and people finally come to terms with their emergence. The first step in dealing with any social – criminal problem is for it to be recognized cognitively and identified with emotionally. How cyber risk, computer crime and electronic privacy enter Hong Kong people’s psychic and ethos is the focus of this chapter. We will follow this line of approach in seeking to document how Hong Kong people come to “discover” computer crime.

\textit{Private e-banking security study}

\textsuperscript{547} See 10 (6) to “Introduction” to 1996 Report
In the mid-1990s, the Hong Kong government started to worry about e-security issues in conjunction with its desire to develop Information infrastructure to improve government efficiency, i.e., e-government, and business productivity, e.g., e-banking. This requires the government: “To instill confidence in the public … set up proper mechanisms to ensure the security and soundness of transactions made through the open communication networks.”  

In 1997, the Hong Kong Monetary Authority (HKMA), the quasi-government banking watchdog, launched one of the first computer crime and information security study in Hong Kong: “SECURITY OF BANKING TRANSACTIONS OVER THE INTERNET” (1997) (Hereinafter “1997 Study”). The study sought to identify the security risks associated with e-banking in Hong Kong. The study was conducted in part because the Seventh Schedule to the Banking Ordinance requires the banks in Hong Kong to maintain adequate accounting systems and effective systems of control ”to mitigate the risk of loss of confidentiality and the risk of unauthorized access to institutions' internal computer systems.” The HKMA has to play a leadership role in providing for a system and standard of risk management.

The major security risks identified by HKMA in the 1997 Study were false authentication, interception of information on route, unauthorized access to accounts of

548 SECRETARY FOR INFORMATION TECHNOLOGY AND BROADCASTING Testimony. Legco Proceedings. Wednesday, 4 November 1998 (“Furthermore, we plan to introduce an enabling bill on electronic commence to the Legislative Council next year. The bill will make specific provisions for digital information, legal endorsement for electronic signatures, the establishment of a certification authority and such like matters.”)

549 The study was conducted by “Study Group on Electronic Banking” established by the HKMA in July 1997. SECURITY OF BANKING TRANSACTIONS OVER THE INTERNET http://www.info.gov.hk/hkma/eng/guide/guide_no/guide_1511xb.htm
The HKMA concluded with this observation:

“The use of sophisticated cryptographic techniques, firewalls and other security tools can provide security that is comparable to that offered in physical transactions. However, similar to a physical transaction, the effectiveness of such measures would be largely dependent on their proper implementation and the establishment of a set of comprehensive policies and procedures that are rigorously enforced.”

For the first time in Hong Kong government policy circles, the 1997 Study placed the issues of computer malfeasants and electronic transactional risks squarely on the table, first as a private e-business obstacle to overcome in launching e-banking and later as a public IT policy debate to be resolved in developing Hong Kong “Cyberport”.

On hindsight, the importance of the 1997 Study goes far beyond merely highlighting e-banking risks in an electronic age. The 1997 Study helped to raise public consciousness over the emergence of computer crimes and cyber risks. In so doing, the HKMA study set the stage, laid the agenda and defined the issues for future debate over the shape and contour of cyberspace governance.

**Government IT security concerns**

In 1999, the Hong Kong government formally launched the Cyberport project to promote Hong Kong’s future economic development. The vision of Cyberport states:

“The Cyberport aims to provide an important Information Technology (IT) flagship infrastructure to attract, and thus create, a strategic cluster of local and overseas companies and professional talents specialising in Information Technology (IT) applications, information services (IS) and
multi-media content creation.” 550

The success of the Cyberspace project ultimately depends on the Hong Kong
government’s ability to secure the information highway and hold IT infrastructure
harmless against potential cyber barons, Internet pirates and computer criminals. As a
result, around this time, i.e., late 1990s and early 2000s, there was much discussion in
and out of government as to how the cyberspace could (should) be regulated and made
safe, e.g., who are responsible for cyber security in Hong Kong?

Unlike in the United States,551 the issue of whether to govern or not to govern in
the cyberspace was never an issue. From the beginning, the question has always been
how and how much to regulate the cyberspace. 552 In June of 2001 the Deputy Secretary

551 See John Perry Barlow, “A Declaration of the Independence of Cyberspace”
(February 8, 1996) <barlow@eff.org> (“Governments of the Industrial World, you weary
giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of
the future, I ask you of the past to leave us alone. You are not welcome among us. You
have no sovereignty where we gather. We have no elected government, nor are we likely
to have one, so I address you with no greater authority than that with which liberty itself
always speaks. I declare the global social space we are building to be naturally
independent of the tyrannies you seek to impose on us. You have no moral right to rule us
nor do you possess any methods of enforcement we have true reason to fear.”)
552 Some scholars argue that there is no such thing as non-regulated cyberspace, i.e.,
order in cyberspace implies passive coordination if not assertive governance. The debate
is not able whether to regulate but with delineating what is the purpose of regulation, i.e.,
coordination vs. control, determining who is regulating, e.g., cyber users vs. big
government vs. powerful cooperation, and deciding upon how to regulate, e.g., grass
roots regulation or imposed order. David Johnson and David Post, “Law and Borders--
The Rise of Law in Cyberspace,” 48 Stanford Law Review 1367 (1996) (Cyberspace has
real boundary and requirements of law. But the legal regime must be adjusted to the
characteristics of the cyberspace, not transferring from the conventional material world.)
Milton Muller, “The "Governance" Debacle: How the Ideal of Internetworking Got
for Security, Cheung Siu-hin announced the government’s cyberspace governance philosophy and computer security strategy. As the Secretary put it, the issue on hand is between having an Orwellian Big Brother “watching our every move” or having some basic rules for the information highway to avoid abusive drivers. The government’s “approach has been to treat regulation as the means to establish minimum ground rules to secure fair play.” The Secretary was quick to add that government regulations cannot be the sole solution to cyberspace security. They are also not the most efficiency and effective solution to computer crime and information security problems. The best strategy is to educate the public to secure themselves, e.g., guard against online identity theft, and work with the private sector (IPS) to reduce security risks, e.g., adoption of best practice or preservation of computer forensic evidence. The approach was

---

553 The Hong Kong government’s position thought clear on its face raises more questions than it solve. First, what is “minimum” vs. “maximum” is not ascertainable in the abstract. Second, the question of “minimum” to whom needs to be resolved? Ultimately, the issue of reasonableness of cyberspace regulation cannot be disposed of by simplistic and jingoistic “minimum” vs. ”maximum” rule. The essence of the debate is never how much to rule, a legal question, it is for what ends the regulations should be directed, a philosophical issue.

554 Again, when the Hong Kong government looks toward the public and community to help to secure the cyberspace, it was less a move to promote political accountability but a strategy to enhance efficiency and cost effectiveness.

towards cyberspace community policing.  

The Hong Kong government public education effort was instrumental in educating the public to computer crime problems and IT security issues

**Foreign anti-piracy campaign**  

In the 1990s Hong Kong was the piracy capital of the Asia, if not even the world. A cursory inspection of the British colony (known then as a dependent territory) economic history shows that in 1996, software piracy was a growth business. Pirated software could be bought openly, cheaply and safely everywhere. For example at Golden Shopping Arcade (GSA) and Computer 33 Plaza

---

556 For discussion of history and philosophy of community policing, as applied to China context, see Kam C. Wong,” Community Policing in Comparative context: P.R.C. vs. U.S.A.” (November 11, 2001). (On file with author).

557 Gregor Urbas, “Cybercrime Legislation in the Asia Pacific Region” Cybercrime Summit, Centre for Criminology, University of Hong Kong, April 25 – 26, 2001. (Over the last two years, Microsoft Corporation has launched campaign against privacy and counterfeit of proprietary computer software. It closed down 88,000 Internet sites offering counterfeit software and conduct hundreds of raids on counterfeiting sites in China (including Hong Kong and Macau), Malaysia, Philippines, Singapore, Taiwan and Thailand.)

558 “Piracy in Hong Kong: IGN64 goes undercover in Sham Shui Po and looks at piracy devices and their impact on the N64 scene.” April 8, 1999. [http://ign64.ign.com/articles/067/067652p1.html](http://ign64.ign.com/articles/067/067652p1.html)

559 For a tourist first person account of software piracy shopping, see “Exploring the Internet: Round One, Hong Kong” (Microsoft Word for Windows in the U.S. costs U.S. $129, after special discount. In the Golden Shopping Center it fetched. U.S. $12.50. AUTOCAD (15 high-density disks) or even a full distribution of SCO's Open Desktop sold for U.S. $138 and the U.S. it was priced U.S. $1,000. ) [http://www.museum.media.org/eti/RoundOne06.html](http://www.museum.media.org/eti/RoundOne06.html)

560 “Piracy in Hong Kong: IGN64 goes undercover in Sham Shui Po and looks at piracy
in Shumshuipo, "Internet Zone" at Whampoa Gardens, and Sinoplaza in the Mong Kok section of Kowloon.

A 1996 IIRA 301 Country Report takes note of the prevalent and seriousness of the problem:

“CD-ROMs containing pirated computer software, both business applications and entertainment titles, are flooding the market in Hong Kong. Seizures of these pirate CD-ROMs skyrocketed from 5400 in 1994 to 176,872 in the first nine months of 1995, a 44-fold increase on a monthly basis. This contraband often takes the form of compilations, in which the massive storage capabilities of the CD-ROM format are used to package dozens of unrelated computer programs from a variety of sources, with a legitimate market value of tens of thousands of US dollars, for sale in Hong Kong at a minuscule percentage of the legitimate price. For instance, the latest versions of Autodesk's AutoCAD Release 13 (retail price US$4,250), Novell's NetWare 4.1 (retail price $2,845) and Lotus's Smartsuite were packaged with over 100 other programs owned by different companies and sold openly in Hong Kong in October 1995 for HK$50 (US$6.50). Pirated versions of Microsoft's Windows 95 were on sale at the Golden Shopping Arcade within a week of the operating system's launch on August 24, 1995.”

Hong Kong retail computer software piracy was also found in the cyberspace. In devices and their impact on the N64 scene.” April 8, 1999.

http://ign64.ign.com/articles/067/067652p1.html

August of 1996, the Business Software Alliance (BSA) working closely with the Alliance Against CD-ROM Theft (AACT) closed down an Internet site, called Sammy Game Center, which offered illegal CD-ROM products for sale and export to the United States, the Netherlands, Sweden and Canada, via the net.562

To the (foreign) intellectual property industry, the adverse economic impact of Hong Kong privacy and counterfeiting is great. According to International Intellectual Property Alliance (IIPA) data, the level of piracy in computer programs for business application and entertainment software from 1995 to 1998 in Hong Kong were: 1995 (business 62%, entertainment 75%), 1996 (65%, 73%), 1997 (67%, 70%), 1998 (59%, 72%). (Table 1)

Table 1: ESTIMATED TRADE LOSSES DUE TO PIRACY and LEVELS OF PIRACY: 1995 – 1998 in Hong Kong (in millions of U.S. dollars)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Motion Pictures</td>
<td>30.0</td>
<td>20%</td>
<td>20.0</td>
<td>20%</td>
<td>15.0</td>
<td>15%</td>
<td>10.0</td>
<td>4%</td>
</tr>
<tr>
<td>Sound Recordings/Musical</td>
<td>30.0</td>
<td>60%</td>
<td>20.0</td>
<td>20%</td>
<td>18.0</td>
<td>20%</td>
<td>5.0</td>
<td>13%</td>
</tr>
<tr>
<td>Compositions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Programs:</td>
<td>69.2</td>
<td>59%</td>
<td>92.9</td>
<td>67%</td>
<td>89.0</td>
<td>65%</td>
<td>88.7</td>
<td>62%</td>
</tr>
<tr>
<td>Business Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Programs:</td>
<td>112.3</td>
<td>72%</td>
<td>110.9</td>
<td>70%</td>
<td>115.7</td>
<td>73%</td>
<td>112.2</td>
<td>74%</td>
</tr>
<tr>
<td>Entertainment Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Books</td>
<td>2.0</td>
<td>NA</td>
<td>2.0</td>
<td>NA</td>
<td>2.0</td>
<td>NA</td>
<td>2.0</td>
<td>NA</td>
</tr>
<tr>
<td>TOTALS</td>
<td>243.5</td>
<td></td>
<td>245.8</td>
<td></td>
<td>239.7</td>
<td></td>
<td>217.9</td>
<td></td>
</tr>
</tbody>
</table>

The foreign intellectual property commercial interests - movie, music, theater, software, retailing, broadcasting and information technology industries - the likes of ATV, Blockbuster, BSA has adopted a two prone strategies to dampen the floodgate of pirated software in Hong Kong. First, they conduct education program and launch awareness campaign to inform the public as to the magnitude and seriousness of the piracy problem in Hong Kong. Second, they apply political pressure on the Hong Kong government to clamp down on piracy and counterfeiting; demanding more law enforcements, stricter legislation and heavier punishment.

In order to mobilize the Hong Kong public, the foreign and domestic intellectual property coalition staged mass rallies, e.g., an anti-piracy march in Hong Kong on March 17, 1999, to heighten public awareness about over the grave consequences and negative impact of piracy on Hong Kong.


564 “Hong Kong Anti-Piracy March.” GrayZone Quarterly Digest March 17, 1999, [http://www.grayzone.com/hkmarch99.htm](http://www.grayzone.com/hkmarch99.htm) (The message is that piracy hurts Hong Kong economy, jobs and image. People should not buy pirated goods and should report counterfeiters. The Anti-Piracy March was supported by Asia Television Ltd., Blockbuster, Business Software Alliance (BSA), Cable and Satellite Broadcasting Association of Asia (CASBAA), Composers and Authors Society of Hong Kong Ltd. (CASH), Hong Kong Cable Television Ltd. Hong Kong Cinema & Theatrical Enterprises Association, Hong Kong Cinematography and Television Lighting Association, Hong Kong Fine Arts Association, Hong Kong Film Awards Association, Hong Kong Film Directors' Guild, Hong Kong Internet Service Provider Association Hong Kong, Kowloon & New Territories Motion Picture Industry Association Ltd. (MPIA), Hong Kong Optical Disc Manufacturers Association (HKODMA), Hong Kong Performance Artists Guild Hong Kong Record Merchants Association Ltd., Hong Kong Screenwriters' Guild, Hong Kong Small & Medium Business Association, The Hong Kong Stuntman
message is as clear as it is dire: Copyright piracy is causing serious losses to Hong Kong economy and grave harm to Hong Kong's reputation as an international trading center. Piracy of intellectual property is a crime. Hong Kong people should not buy pirated goods. Hong Kong government should take resolute actions against counterfeiters. The public was urged to appeal to the Hong Kong Government to take resolute measures to fight the crime of piracy. 565

Beyond public education and political actions, the intellectual property coalition threatened the Hong Kong government with possible USTR 301 trade sanction, if it did not take immediate and effective measures to put intellectual property piracy under control. For example in 1995, IIPA's Special 301 recommended to place Hong Kong on Special Mention status (equivalent to USTR's Other Observations category) as a result of increased flow of pirate materials from China into Hong Kong. 566

In 1996 IIPA

Association Hong Kong Theater Association, Hong Kong Video Industry Association, HMV, International Federation of the Phonographic Industry (IFPI), Motion Picture Association (MPA), Motion Picture Production Executive (HK) Association, Movie Producers & Distributors Association of Hong Kong, Movieland, Music Publishers Association of Hong Kong Ltd., Society of Cinematographers (Hong Kong), Society of Film Editors (Hong Kong), Software Publishers Association (SPA), South China Film Industry Workers Union, Television Broadcast Ltd. (TVB).

565 “Hong Kong Anti-Piracy Day a Major Success,” IFPI Press Release March 17, 1999

566 On January 1, 1996, the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) went into effect. In general terms, TRIPS requires an enforcement system that: permits effective action against infringements; provides expeditious remedies which constitute a deterrent; is fair and equitable; is not unnecessarily complicated or costly; and does not entail any unreasonable time limits or unwarranted delays. TRIPS requires that member countries must apply their criminal laws in cases of commercial piracy; it is not enough to merely have laws on the books unless those laws are used effectively. Failing that USTR can impose trade sanctions. "Copyright Enforcement Under the TRIPS Agreement""
recommended placing China on Watch List to encourage Hong Kong to devote more resources to copyright enforcement and. In 1997 IIPA wanted to place Hong Kong on Priority Watch List. Because of the perceived worsening digital piracy problem, Ambassador Barshefsky placed Hong Kong on the Watch List on April 30, 1997. In 1998 USTR agreed with IIPA’s recommendation to keep Hong Kong on the Watch List.567

Through public pressure and trade sanctions, IIPS was able to compel the Hong Kong government to take resolute actions against piracy, including more effective legal measures, e.g., licensing of CD copying machines, and take more aggressive enforcement actions, e.g., more raids against privacy and counterfeiters.568

On December 16, 1998 Ms, Selina Chow, Legco members for the retail industry, moved the following motion:

"That, in view of the recent proliferation of pirated compact discs in various districts, this Council urges the Government to immediately review the existing policies and strengthen the co-ordination of various law enforcement authorities, so as to combat more effectively the manufacture, importation and sale of pirated video, music and software compact discs; furthermore, the Government should strengthen its publicity and education programmes with a view to making the public aware that the infringement of intellectual property rights is immoral; this Council also urges the Government to actively consider amending the

International Intellectual Property Alliance (IIPA)

568 Legco proceeding, OFFICIAL RECORD OF PROCEEDINGS, Wednesday, 16 December 1998
relevant legislation in order to empower the law enforcement authorities to prosecute those engaged in the pirated recording of movies in cinemas and consider the imposition of fines on purchasers of pirated compact discs, thereby achieving deterrent effects."

In February 1999, the Hong Kong Government published a consultation paper entitled "Combating Intellectual Property Rights Infringement in the Hong Kong Special Administrative Region: Possible Additional Legal Tools". The paper proposed a number of measures to fight piracy and counterfeiting, including:

i. including piracy and counterfeiting offences under the Organised and Serious Crimes Ordinance;

ii. amending the Copyright Ordinance and the Trade Descriptions Ordinance to provide for the confiscation of criminal proceeds from intellectual property infringement offences;

iii. introduction of mandatory or standard sentences for copyright and trade mark offences;

iv. closure orders against premises used repeatedly for piracy or counterfeiting activities;

v. immediate closure orders for premises used for piracy or counterfeiting activities;

vi. banning unauthorized video recording in cinemas;

vii. banning video equipment in cinemas; and

569 For a response see “Hong Kong Software Industry Comments on June 1999 Trade and Industry Bureau Submission to The Legislative Council Panel on Trade and Industry” CB(1)1457/98-99(02) (June 3, 1999)
viii. imposing consumer liability, including

- imposing a fixed penalty for possession of infringing articles;
- creating a smuggling offence in respect of the import or export of infringing articles;
- recasting the offence of possession of infringing articles.

As a result of the consultation process, the Legislative Council passed an amendment to Organized and Serious Crimes Ordinance to include piracy and counterfeiting offences. On January 12, 2000 Legco also proposed to criminalize the possession of an infringing article other than for personal, domestic use.

On the law enforcement end, the government also took more aggressive actions against piracy in 2000 to pacify the foreign concerns. For example on June 22, 2000, the Internet Task Force of Hong Kong Customs conducted the first raid in Hong Kong against an Internet site selling pirate software, where Microsoft Windows 2000, Microsoft Project 2000 and Symantec pcAnywhere were sold at HK$20 per copy. Two suspects were arrested and three computer servers, two computers, 76 pirated discs and other computer equipment worth approximately HK$50,000 were sized.570

The foreign anti-piracy movement has the net effect of educating the Hong Kong public to respect intellectual property rights. It also compelled the Hong Kong government to be more solicitous of intellectual property rights. In the process, it was successful in making one kind of computer crime, that of stealing of intellectual property electronically, tangible and real, and enforceable by criminal law in Hong Kong.

570 Microsoft Licensing: Hong Kong Copyright Law, “Hong Kong Customs First Crackdown on Online Sale of Pirate Software (L) June 28, 2000
http://www.microsoft.com/hk/licenses/cases.htm (visit 11/08/04)
Moral outrage and economic pressure against Internet gambling

Gambling is a favorite pastime in Hong Kong.\textsuperscript{571} Take soccer gambling as an example. The Hong Kong government Home Administration Bureau survey shows that in May 2001, 2.4\% or 120,000 people in Hong Kong have betted in soccer gambling.\textsuperscript{572} An independent Chinese University of Hong Kong gambling survey conducted at the same time actually shows more gamblers, i.e., 6.2\%\textsuperscript{573} or 340,000 people. The conservative estimate was that soccer gambling annual turnover amounted to $200 billion a year.\textsuperscript{574}

With the introduction of off shore and Internet gambling\textsuperscript{575} the situation got worse. The growth of offshore gambling is further evident by a ten folds increase in

\begin{footnotesize}
\begin{enumerate}
\item For a first person account of gambling in Hong Kong. MICHELLE LEVANDER “Log On Your Bets,” \textit{Times (Asia)} Nov. 5, 2001. (“Living in Hong Kong, it's hard not to get caught up in playing the odds. Gambling fever is woven into its history:..”)
\item Home Affair Bureau, \textit{Public Consultation on Gambling Review: Consultation Report} (HKSAR March 22, 2002), “Chapter 3: The Proliferation of Soccer Betting Activities” 3.6 The figure is underestimated because of respondents’ unwillingness to admit to illegal gambling to government surveyors and the survey did not include people who bet with friends.
\item The difference in finding is likely to be the result of a more reliable methodology used by CUHK. CUHK is not a government agency and has no law enforcement responsibility. As a result, respondents were likely to be more forthcoming and honest with their answers.
\item See \textit{ld}. “Betting with Offshore Bookmakers”, esp. 3.14. Internet gambling offers a number of advantages: full time availability, ease, cheap, choices, worldwide access, comfort and secrecy at home
\end{enumerate}
\end{footnotesize}
telecommunication volume between gambling Country X (widely suspect to be U.K.) and Hong Kong (see Table 2)

Table 2: Telecommunication to off shore gambling site (country x) and other countries: 1993, 1994, 2000

<table>
<thead>
<tr>
<th>Countries</th>
<th>Year</th>
<th>Minutes (000)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All other countries</td>
<td>1993</td>
<td>1376858</td>
</tr>
<tr>
<td>All other countries</td>
<td>1994</td>
<td>1578442</td>
</tr>
<tr>
<td>All other countries</td>
<td>1995</td>
<td>3074885</td>
</tr>
<tr>
<td>Gambling site (country x)</td>
<td>1993</td>
<td>32</td>
</tr>
<tr>
<td>Gambling site (country x)</td>
<td>1994</td>
<td>34</td>
</tr>
<tr>
<td>Gambling site (country x)</td>
<td>1995</td>
<td>332</td>
</tr>
</tbody>
</table>

Source: Adapted from Table 3.1: Home Affair Bureau, *Public Consultation on Gambling Review: Consultation Report* (HKSAR March 22, 2002), “Chapter 3: The Proliferation of Soccer Gambling Activities”

The Hong Kong government’s policy towards gambling is one of: “restrict gambling opportunities to limited and authorized gambling outlets only.” More simply, controlled gambling. The reason for such a permissive but restrictive gambling policy is a realization that gambling cannot be altogether prohibited, because of history (institutionalized house racing), culture (Chinese love gambling) and politics (Jockey club clout). Thus, it is better to authorize, regulate and limit gambling to a bare minimum in order to satisfy existing demands. This policy concedes that unregulated gambling would only contribute to unlimited gambling, underage gambling, criminal connections, gambling fraud, and loss of revenue for charity.

---

577 *Id.* 2.3.
578 *Id.* 2.4.
579 Home Affair Bureau, *Public Consultation on Gambling Review: Consultation Report*
Gambling in Hong Kong is regulated by the Gambling Ordinance (Cap 148) and Betting Ordinance (Cap 108). Hong Kong government derived substantial and continual tax revenue from gambling activities, i.e., from about 7.21% (HKD 11,051 millions) of government revenue in 1995 to that of 5.12% (HKD 11,930) in 1999. (Table 3)

<table>
<thead>
<tr>
<th>Financial Year</th>
<th>Betting Duty (HKD millions)</th>
<th>Percentage of Government Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>19995/1996</td>
<td>11,051</td>
<td>7.21%</td>
</tr>
<tr>
<td>1996/1997</td>
<td>12,191</td>
<td>7.01%</td>
</tr>
<tr>
<td>1997/1998</td>
<td>13,453</td>
<td>4.89%</td>
</tr>
<tr>
<td>1998/1999</td>
<td>12,228</td>
<td>5.66%</td>
</tr>
<tr>
<td>1999/2000</td>
<td>11,930</td>
<td>5.12%</td>
</tr>
</tbody>
</table>


In the 1990s, offshore (Internet) gambling challenged the monopoly of Hong Kong Jockey Club, the only authorized gambling house in Hong Kong. With the discovery of information highway, Internet gambling becomes more prominent and the betting avenue of choice. Survey conducted in 1999 by the international Internet usage measurement firm, NetValue, found that the number of Hong Kong residents visiting gambling sites almost doubled between October and December of 1999 to 41 percent of the population, from 22 percent before. According to the NGISC (1999) report on Internet gambling, it is estimated that the number of online gamblers more than doubled from 1997 to 1998, an increase from 6.9 million to 14.5 million.580

The Jockey Club and other officials have requested the Hong Kong government to

pass legislation to outlaw offshore bookmaking altogether. But, Andrew Cheng, Chairman of the Bills Committee on Gambling refused the overture. In March 31, 1999, the Hong Kong Legco took up the issue of Internet gambling and its impact on Hong Kong’s economy and morality. In February 2000, Hong Kong government contemplated stopping the use of credit card for Internet gambling. But this proposal was jettisoned when Hong Kong Jockey Club declared that it would accept credit card for its own Internet gambling starting September 2000.

Finally, in May 2002 Legco passed the Gambling (Amendment) Ordinance and ban off shore gambling, with maximum of 7 years in jail and $5 million in penalty for brokers and 9 months and HK$30,000 for gamblers.

The legislative victory against off shore gambling was a result of two potent forces at work, i.e., one economic and the other moral. They joined hand as a powerful political force in pressuring the government to act.

Economically, the Hong Kong government and Hong Kong Jockey Club stand to lose billions every year if off shore – Internet gambling is not regulated.

Morally, there was great public outcry that increase gambling would lead to

581 “Offshore Internet Gambling Leaves Hong Kong Out Of Pocket, Inside China,” Reuters February 22, 2001 (Jockey Club (JC) estimates it is losing HK$50 billion ($6.4 billion) a year to high-tech and illegal bookmakers. JC pays 11% of its income to the government as betting duties, a major source of income for the government. In Lunar New Year 2001, the Jockey Club collected eight percent less than last year, due to economic downturn and as a result of Internet competition.)


585 Those who fight against gambling is being called: “Moral person” “Moral person”
more individual destructions, family tragedies, youth problems, and social inequities.


Yee Ah, “Gambler story (1) Leaving the Police” (賭仔故事（一） 離職警察) (Ah Ke learned to gamble when he was young. He had a good paying job as a police officer. When he was in the Marine Division, he emerged himself gambling and borrowed large sum of money. He finally has to escape to China to avoid the debt.) January 31, 2000 The Society for Truth and Light http://www.truth-light.org.hk/article_v1/jsp/a0000129.jsp

Yee Ah, “Gambler story (2) A father who was transfixed with gambling” (賭仔故事（一） 一個沉迷賭博的父親) (Ah Ping was an illegal immigrant from China. He took a job as barber. Because he was hooked onto gambling he has constant arguments with his wife. This affected his daughter who has no confidence with the father and still less hope with the family.) The Society for Truth and Light June 30, 2001.

For a collection of newspaper cases of individual and family tragedies as a result of gambling, from March 2001 to May 2001, see Chan Yin Ping “Horrifying tragic gambling cases” (賭博慘案驚心動魄) (There were 14 cases of suicides or illegal activities by desperate gamblers and 13 cases affecting family members or friends, leading to 14 deaths.) The Society for Truth and Light July 30, 2001 http://www.truth-light.org.hk/article_v1/jsp/a0000227.jsp

Leung Lan Tien Wei, “Gambling culture spread, poising of youth” (賭風蔓延 茶毒青少年) Hong Kong Economic Journal, July 13, 2000. (Gambling culture is spreading in Hong Kong, especially amongst the youth. The Jockey Club encouraged families to bring their young ones on “Jubilee Day” to have a taste of horse raising. The media encouraged gabling mentality by speculating on stock, e.g., Tom.com, and promoting soccer betting with gambling tips and league tables in mainstream sports page.) http://www.truth-light.org.hk/article_v1/jsp/a0000021.jsp See also Professor Chung Kim Wah, “Do not underestimate the negative impact of gambling activities on youth” (不要低估賭博活動對青少年的負面影響) (Research shows that early exposure to gambling legitimate gambling in the eyes of the children and have long term impact on youth healthy moral development.) January 31, 2000. Society of True and Light http://www.truth-light.org.hk/article_v1/jsp/a0000127.jsp.

Choi Chi Sum, “The legalization of gambling, taxing the poor people in disguise”
The Christian and religious organizations in Hong Kong has a long history of fighting gambling. They mobilize their followers to petition the government, e.g., submitting anti-gambling petitions to the Home Affairs Bureau on Sept. 11, 2001, or demonstrated in the street, e.g., mass rally on September 15, 2001. They engaged in legislative research, public policy study and opinion survey on issues of anti-gambling.\textsuperscript{590} They also called upon the members to pressure the legislators in voting against any gambling friendly legislation.\textsuperscript{591}

The Society of Truth and Light, a grass roots social work organization, epitomize the grass roots movement in fighting gambling in general and Internet gambling in particular. It has called for the studying of the harmful effect of gambling on youth, family and society before moving ahead with legalizing of off shore soccer gambling.\textsuperscript{592}

\textsuperscript{590}Those who fight against gambling is being called: “Moral person” “Moral person” hardworking in the background: (「道德佬」背後的實幹) \textit{The Society for Truth and Light}, March 31, 2002. \url{http://www.truth-light.org.hk/article_v1/jsp/a0000278.jsp}

\textsuperscript{591}“Influencing the legislative councilors, the electors have responsibility’ (影響議員 選民有責) \textit{Society of True and Light}, January 16, 2003 (The article listed all the names of all 13 legislative councilors who supported gambling, and others who have not made up their mind. The article also supplied a form letter for petitioning the legislative councilors against legalization of soccer betting.) \url{http://www.truthlight.org.hk/article_v1/jsp/a0000356.jsp}

\textsuperscript{592}“Society of True and Light response to Public Consultation on Gambling Review) (明光社就賭博問題諮詢文件的回應) (The Society offers eight recommendations, the first two called for more study of the problem, and the last asked the government to delay the legalization proposal. The other five recommendations asked the government to educate the public and do whatever is necessary to alleviate the ill effects of gambling on the
In 2000, concerned citizens – churches, social work organizations, parents – organized an anti-gambling watchdog organization called: “Coalition to supervise gambling culture.”

The charter of the Coalition is to see whether the government follows through with its anti-gambling policy; to keep in touch with gambling organization (Jockey Club) over its gambling methods; to keep account of the mediation to see whether they have mixed sports gambling with sports activities; to engage universities to conduct gambling survey and to generate social pressure against gambling.

In 2000, the “Coalition of concern with spreading of gambling culture” was established. The Legco passed a resolution “against legalizing football”. The Society of True and Light asked City University of Hong Kong to research into “The impact of gambling on Hong Kong Youth.” The study finds that young people who are affected by gambling show little energy at work and harbor negative ideas about the law.

The concerted effort of Christian organizations or anti-gambling coalitions to people, especially with the youth. The specific recommendations were:

Recommendations: (1) The government should not act without a comprehensive investigation of the current status and future impact of citizens involvement in gambling. (2) The government should collect cases from social service agencies to ascertain the nature and extent of gambling problems in the society, and (8) The government should suspend any proposition to legalize more gambling until comprehensive and long term observation of the impact of gambling on the society can be made.)


593 「監察賭風聯盟」


595 「關注賭風蔓延聯盟」

596 Soccer gambling legalization journal (賭波合法化事件簿) Candle Web July 1, 2003. 「賭博對香港青少年的影響」
fight overseas gambling resulted in increased police gambling enforcement. Table 4 shows that enforcement actions against gambling rose from 1221 cases in 1997 to that of 2080 cases in 2000, an increase of 784.  

Table 4: Gambling enforcement Statistics: 1995 - 2000

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total raids</td>
<td>1570</td>
<td>1263</td>
<td>1221</td>
<td>1332</td>
<td>1818</td>
<td>2080</td>
</tr>
<tr>
<td>Total successful Raids</td>
<td>1223</td>
<td>1095</td>
<td>1082</td>
<td>1075</td>
<td>1200</td>
<td>877</td>
</tr>
<tr>
<td>Persons arrested</td>
<td>7857</td>
<td>7857</td>
<td>7534</td>
<td>7816</td>
<td>7737</td>
<td>5251</td>
</tr>
<tr>
<td>Money, Slips, Betting slips seized</td>
<td>47829 (000)</td>
<td>47820</td>
<td>42180</td>
<td>89874</td>
<td>36354</td>
<td>582236</td>
</tr>
</tbody>
</table>

Source: Adapted from Table 3.1: *Home Affair Bureau, Public Consultation on Gambling Review: Consultation Report* (HKSAR March 22, 2002), “Chapter 3: The Proliferation of Soccer Gambling Activities”

In 2001 the “Big Coalition against legalization of gambling” and “Big Christian coalition against the legalization of gambling” was established. In April the “Industrial gospel group” established a “Problematic Gamblers rehabilitation center.”

On September 15, 2001 a “Just say no to gambling” public demonstration was

---

598 Given the large amount and huge volume of gambling going on, the enforcement efforts must be considered as symbolic not real. HKP police know that being raided is part of doing business, but no sufficient to bankrupt the gambling organizers.

599 「反對賭波合法化大聯盟」

600 「基督教反對賭波合法化大聯盟」

601 「問題賭徒復康中心」

602 「向賭博說不」
organized with 1500 participants. The government has asked the Polytechnic University to study “The status of Hong Kong people participating in gambling”. In March 2002, the Department of Civil Affairs issued a “Gambling question consultation document.” It showed that 86% of the respondents were against soccer gambling. The government ignored the consultation document and relied on its own 1500 telephone survey to endorse soccer gambling.

In January of 2003, the Hong Kong government decided to legalize soccer betting, though not off-shore gambling. The Christian Church anti-soccer gambling Coalition organized the “Concern with the next generation, resolutely against soccer gambling” demonstration with 3,600 members participating. In May of 2003, the Legco organized public hearing on soccer gambling. 94 organizations or individuals participated and only one supported the football gambling bill. 603

Notwithstanding public objections, the Internet has been used to side step legal prohibition against promotion of gambling in the media. The Internet has been used to promote and facilitate football gambling, e.g., 「g-win」 allows for direct betting on the net, which runs against the “Gambling [Amendment] Ordinance. September 19, 2003. 604 Resourceful gambling organizers also have been using Internet to promote gambling to the youth. 605

Finally, on July 10, 2003, the Legco passed the “Betting Tax (Amended)

---


604 Chan Yin Ping, “Gambling media without regulation, the true nature of promotion by various major media” (賭波資訊無王管: 各大傳媒宣傳賭波實況) http://www.truth-light.org.hk/article_v1/jsp/a0000402.jsp

"Ordinance" and legalized soccer betting.

Reacting to such public displeasure and legislative development, City Polytechnic University of Hong Kong conducted a random sampled, phone survey to ascertain the impact of the law on Hong Kong community. The survey was conducted between August 1 and 2, 2003. The surveyors successfully called 1025 people, age 15 and above with a response rate of 48.5%.

The survey finds that people were still very much divided over legalization of soccer gambling, with 44.8% in support and 32.1% against. Asked about the impact of legalize gambling 60.3% thinks that it would lead to more gambling and 40.6% thinks that restrictive gambling will have a negative impact on youth as compared with legalized gambling. More telling, increasingly, soccer betting is looked upon as gambling, i.e., 55.9% as compared with 1.5% before legalization (Table 5)

Table 5: Do you have interesting in soccer gambling – by age

<table>
<thead>
<tr>
<th></th>
<th>Age(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>15 – 17</td>
</tr>
<tr>
<td>Very interested</td>
<td>2.8</td>
</tr>
<tr>
<td>Interested</td>
<td>8.3</td>
</tr>
<tr>
<td>Very little interest</td>
<td>37.5</td>
</tr>
<tr>
<td>No interest at all</td>
<td>51.4</td>
</tr>
<tr>
<td>Do not know</td>
<td>-</td>
</tr>
<tr>
<td>總計</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The above recitation of the fight against the legalization of soccer gambling and off shore betting shows that it is a contentious issue implicating many diverse interests and affecting some very basic values in the Hong Kong community. As a result, the fight against off shore soccer gambling, led by amongst others the Society of Truth and light, turned out to be the most potent common cause to unit the Hong Kong people against cyber crime. The Jockey Club of Hong Kong is against off shore betting because it wants to maintain its monopoly over gambling, for economic, status and power reasons. The religious and social services groups are against off shore gambling because they are concerned with its corrupting influences on the young and destructive tendency on individuals and families. The government is against Internet off shore gambling because this erodes its tax base and challenges its legal authority. All three joined hands to condemn Internet gambling as being harmful to the youth, risky to gamblers and beneficial to off shore brokers; the same kinds of shortcomings and risks afflicting all e-transactions. In the end, the anti-off shore gambling movement acted as a mass education forum and natural public awareness campaign in instructing the Hong Kong people of all persuasions about the ill effects and criminogenic potentials of the Internet. The public was able to see for themselves, for the first time, in a close and personal way, what an uninhibited Internet can do to their economy, morality, youth and family.

Overnight, cyber-harm, experienced in the form of off shore gambling, becomes

Source: Adapted from Table 6 in Chung Kim Wah, “After legalization of soccer gambling” (賭波合法化後) Society of True and Light 607

Pearson R = 26.991, p<0.05

http://www.truth-light.org.hk/article_v1/jsp/a0000400.jsp
recognizable, tangible, material, consequential, and more importantly visceral. Cyber criminality is no longer conceived of as distant commercial risks in Central District, to be discussed in abstract terms, 608 or received as personal software “deals” in Shamshuipo or Wanchai, to be appreciated in positive ways, but something that is destructive of careers, harmful with kids, damage to family and corrupting in the community.

Cyber harm has arrived, and here to stay. All it takes now is for the public’s perception of cyber ills and harms be validated and reinforced. For this the public turns to the media for the portrayal of a moral and legal crisis in the making.

Public awareness of computer crime and privacy.

Three high profile cases, one in 1995 and the two others in 1999, sensitized the Hong Kong public to the kinds of law enforcement and piracy issues that are raised in an cyber era.

One of the earliest cases drawing the public’s attention is the need for better or more competent computer crime law enforcement in Hong Kong. The realization surfaced as a result of a fumbled computer raids by the HKP and Telecommunications Authority (OFTA) in 1995, causing public outcry.

On March 4, 1995, the HKP and OFTA conducted a raid to shut-down seven ISPs for "commercial crimes involving computer hacking". The IPSs were suspected of providing telecommunication services without a license. The unannounced raids have the

608 In 2003 only 7% of Hong Kong public 15 years old and above used the Internet for “online purchasing services for personal matters” and barely 1% of Hong Kong business establishment “having sold goods, services or info thru’ electronic means” in 12-months before the survey.
unintended effect of shutting down Internet and E-mail links of 10,000 accounts.

The raid raised a number of controversial and embarrassing issues, including:

“What does this signal for the future of freedom of information and freedom of speech in Hong Kong? What does this do to Hong Kong’s International business reputation regarding competition and free trade?” Last, but not least, whether the HKP and or OFTA were cognizant of, sensitive to or otherwise concern about these issues before, or even after, they carried out the raids.609 The competency of HK government in handling police raid related privacy concerns bring the cyber crime law enforcements agencies into dispute locally and internationally.610 This case pointed to the fact that Hong Kong law enforcement agencies are not ready for the cyber age.

In 1999, another high profile case HKSAR v. Tsun Shui Lun [1999]611 raised another interesting issue about privacy. The case happened in April 1998. It involved the privacy right of then Secretary for Justice. Tsu Shui Lun was a technical assistant to a radiologist at Queen Mary Hospital. Tsu used his computer access at the hospital to retrieve medical records of the Secretary for Justice, a patient of the Hospital. He shared the records with his wife, friends and two local newspapers. He was arrested and prosecuted under Section 161 (1) (C) of the Crime Ordinance (Cap.200), i.e., theft of

610 Michael W. Kim, “How counties handle computer crime?” Ethics and Law on Electronic Frontier (Fall 1997) (There was a lack of coordination between Hong Kong Police Commercial Crime Bureau and Office of the Telecommunications Authority, leading to a duplication of investigative effort and resulted in offenders avoiding criminal punishment altogether with payment of HK$700 administrative license fees.)
computer data for personal benefits.

Tsu defended himself by saying that he released the information to the newspapers not for personal gain, a legal requirement, but “because the public have the right to know the truth”, i.e., that the government has lied about the medical conditions of the Secretary of Justice requiring her hospitalization. The case raised a furor in Hong Kong over the public’s right to know, a government employee’s ethical duty to keep a secret and ultimately a patient’s right to privacy. In a still larger context, the case raised the broader issue of computer security. Tsu was convicted. For the first time in Hong Kong the privacy right of an individual is vindicated, criminally.

The third case raised the issue of government power of search and seizure for confidential computer data held by the press (media). In November of 1999, a leading anti-establishment newspaper, *Apple Daily* was searched by the Independent Commission Against Corruption (ICAC) in connection with a corruption investigation. It was alleged that the paper’s journalists were bribing police officers to supply police information. Later two police communications officers and one reporter were sent to jail for selling and purchasing of police information. During the ICAC search for evidence at *Apple Daily* computers were seized and database were searched for evidence, with little protection for the confidentiality and privacy of unrelated parties in the case.

The Newspaper appealed to the Court of Appeals and argued that the Interpretation and General Clauses Ordinance, which made provisions for search and seizure of journalistic materials, were too broad. Otherwise, the search and seizure of information in newspapers’ computers placed the confidentiality between the media and informants at risk and the privacy of innocent third party in jeopardy. The case caused an
uproar in Hong Kong and was very much the talk of the town.\textsuperscript{612}

The issues and debate over the impact and implications of the case on confidentiality and privacy concerns was best captured by my commentary of the case in the \textit{South China Morning Post}, reproduced below:


At issue, as the counsel for Apple Daily Limited Gladys Li argued, is whether the warrant authorizing the search and search of journalistic material “which is likely to be relevant to the investigation for the purpose for which this search warrant is issues” is too wide and parasitic. The CFA ruled in favor of the ICAC.

The determination and reasoning of the CFA, notwithstanding its brevity, was a most measured and reasonable one, and focused entirely on the points of law raised.

While I respect the CFA and readily defer to its determination on legal grounds, I am however, much troubled by the implication and impact of the case on future computer-electronic data privacy protection as a matter of public policy.

I start this policy debate by observing that the Apple case is unique; it involves the search and seizure of computer stored electronic data of a major

\textsuperscript{612} “Hong Kong's media face to face with the Taiwan factor,” 2000 ANNUAL REPORT JOINT REPORT OF THE HONG KONG JOURNALISTS ASSOCIATION AND ARTICLE 19 © HKJA and ARTICLE 19 (JULY 2000)
newspaper.

It is my contention that computer searches and seizures of electronic data (computer search) is a unique kind of search and seizure deserving of special treatment and requiring different consideration than a regular search and seizure of premises and materials (traditional search).

I further argue that computer search calls for extra-ordinary legal protection that is more solicitous of the privacy rights of computer users, than is currently provided for by the law. My basic premise is that a computer search is more intrusive of privacy in scope, manner and degree than a traditional search.

In a traditional search, there is less an expectation of privacy. Notwithstanding people’s claim of privacy, they realize that in real life their premises are often open to friendly invitees, e.g., colleagues, and occasional subjected to uninvited strangers, e.g., postman. In spite of due care, materials and things (including documents) are often found in plain view, exposing our inner most secrets to all. That is to say, while people want to enjoy privacy in places and things, oftentimes their expectation is compromised and intruded upon as a result of “expected” unexpected events, e.g., friendly colleagues who walk past our office or plying strangers who see through our windows. More simply, we are accustomed to surprise visits.

In the case of computer-electronic data, there is a much more heightened and legitimate expectation of privacy. It is commonly believed that the computer is a secured place; a private domain off limits to all others (access code) and exclusively unto ourselves (“P.C.”). People use the computer to talk to close friends, share intimate ideas, conduct sensitive business and store personal
information. The clear example is that when people exchange e-mail, not to speak of ICQ, they are more relaxed, informal and candid. Assured of privacy (e-mail) and emboldened by anonymity (ICQ), people drop their guard and speak their mind freely and uninhibitedly. When such information are readily available to law enforcement officials, they reveal our most inner thoughts and private self!

A computer has a long, long memory. It “remembers” things when most people have forgotten. Whereas things and documents can be misplaced or destroyed, there is no such possibility with electronic data storage. For example, when we delete a data file it does not really mean that the file is destroyed. It just means that the file space is made available for a new entry. The deleted data can be recovered through the use of undelete or salvage commands. Even if the deleted file space is overwritten, residual “file fragments” remain. There is of course the possibility that, unbeknown to ourselves or just having forgotten, the deleted file could have been automatically stored in a backup storage area, ready to be inspected by vigilant law enforcement officials.

Computer also keeps track of our daily routines. For example, the audit trails and computer logs contain information about who have accessed the computer and when, where and for how long. They record who has modified a file and what modification was made. It also indicates when and by whom files were downloaded to a particular location, copied, printed or purged. In essence, the computer logs offer a minute by minute account of what we are doing, every time we engage the computer. It tells law enforcement officers who we talk to, what we watch and even how we think, and in time who we are through transactional and pattern analysis!
Indeed, it is not too far fetch to say that the computer offers inquisitive law enforcement officials an instant and intimate profile of who we are. This is due to the convergence of two factors. First, before the days of the computer, there is no one central depository of all our routine activities (e-commerce) and communications (e-mail). Now there is. Whereas before we share our thoughts only with a selected few and our activities can only be observed by many unrelated causal observers, now the computer gathers all the information about us in one place. Before, especially in a big city, people know us by bits and pieces, never as a comprehensive whole. Now the computer bares all. Second, as e-commerce becomes more common (from shopping to schooling) and e-mail becomes more indispensable (replacing phone, fax and mail), increasingly our life centers around the computer. As we live a world of carefree virtual reality, with everything at our fingertips, the computer is diligently building a personal profile on us. The computer becomes a diary of a sort to be shared by the first law enforcement officer who want to know and find out about our inner most secrets – our identity.

A computer is capable of storing an enormous amount of information. It offers a most economic and efficient way to process, store and exchange information with the push of a button. This capability creates dependency (between person and computer) as well as inter-dependency of use (between persons linked by computer). People are increasingly relying on the computer to conduct ones business and personal affairs. As more and more people use it, the computer becomes more and more essential, and indispensable. The success of Microsoft Windows platform attests to this technologically driven and socially
supported dependency movement on a global scale. Simply, modern man cannot live without electronic data processing. Graphically, without electronic data processing there is no business and association. If that should be the case, indiscriminate seizure of computer will deprive a business or individual of its life support capacity (recording, processing and communication too); in acute cases resulting in business failure and personal maladjustment. Should the law enforcement officials be held accountable for the interruption of business and disturbance of personal life?

The computer has changed our life. Our criminal procedures, particular with respect to searches and seizures, should change along with it.

The three (selected) high profile cases reported here are important milestones to Hong Kong’s journey of computer crime “discovery”. They are important milestones because, viewed individually in point of time and together as a time series, they tell us how far we have come in recognizing computer crime and electronic privacy issues. The fact that the cases were able to precipitate a debate over privacy of patience (case 2), authority of search and seizure (case 3) and competence of cyber investigation (case 1) is the clearest indication that computer crime as an existential entity has penetrated Hong Kong people’s psychic and invaded their hearts and mind. It is too early to tell whether the Hong Kong people would give in to intellectual thieves and privacy intruders, but the battle of order has been drawn. The cyber criminals are coming.

The arrival of computer crimes

The first reported computer related crime case was in 1995.

In 1995, Hong Kong law enforcement officials cracked a major credit card fraud
ring in Hong Kong and Shenzhen, seizing equipments and computer data. The computer criminals identity thieves sold each fake credit card account for US$250. 613 In November of 1996, a disgruntle computer technician brought down Reuter’s trading net in Hong Kong. In November 10 of 1997 the drgaonserve.com was hacked in Hong Kong. In February 9 of 1998 SunSITE was hacked in Hong Kong. 614

Major computer related crimes cases started to appear in 1999 with some degree of frequency.

One of the more colorful hacking stories in the 1999s was that of “Hong Kong Blondes.” 615 The Hong Kong Blondes was a self organized anti-establishment group that used their IT proneness to subvert communist China’s dictatorial regime and international corporations’ exploitative practices. Starting with 1998, Hong Kong Blondes launched a series of cyber attacks against the PLA's computer systems through DoS or "Denial of Service" – by overloading PLA web sites with millions of hits. They further hacked into PLA’s site and started to corrupt its database through erasing, altering or falsifying information. As time progress, the group began actually to install codes within the PLA computer mainframes to monitor the electromagnetic signals emitted by

615 Anthony C. LoBaido “Hong Kong Blondes Build Techno Army Against Communist Chinese Government” <smongol-I> 24 Mar 2000 (The author conducted the only seven weeks long interview with the leadership of Hong Kong Blondes.) See also “Thai hackers claim responsibility: Hong Kong Blondes satellite group says it made cyber-attacks,” WorldNetDaily FEBRUARY 15, 2000
PLA computers with remote means. Hong Kong Blondes even managed to place “social engineers” (cyber mole to work in PLA) to obtain access codes. The MPS acknowledged such illegal attacks and unauthorized access on their web (72,000 cyber-attacks launched against the PLA between January to September in 2000) with 165 successful penetrations in 2000 alone.

On May 20 of 1999, the HKP, after prolonged investigation (five months) successfully broke up an organized hacking syndicate, seizing computers and CD-ROMS. A total of 10 people between the age of 16 – 21 were arrested; three hackers, a middleman and six buyers of passwords. This is the first organized hacking case investigated and prosecuted in Hong Kong. The case started with IPS filing a complaint of hacking with Computer Crime Section of the Commercial Crime Bureau (CCB) which launched an investigations in January f 1999.

According to police, the hackers hacked into 200 legitimate accounts to get their passwords. The passwords were sold at HK$350 (US$45.13) for a month's access. The buyers would use the illegal access codes to rack up Internet times worth between HK$2,000 and HK$3,000 a month. The going rate for Internet access was HK$150 ($19.34) and HK$1.98 ($0.26) per hour for Public Non-Exclusive Telecommunications (PNETS) license fee. The hackers were also guilty of setting up a Web site to sell illegally download music at HK$88 ($11.35) each or HK$160 ($20.63) for two CD copies.

In June of 1999 seven Hong Kong teenagers were arrested for using stolen credit card numbers on the Internet to purchase computer products worth more than HK$1

616 “Hong Kong Computer Hacking Syndicate Smashed.” IT Daily 1999 MAY 30 (Newsbytes)
On April 4, 2000, Magistrate Ian Candy imposed custodian sentence on three hackers (Po Yiu-ming, 19, Tam Hei-lun, 19, and Mak King-lam, 18), sending them to jail and detention center for 49 computer related offences, such as illegally hacking into Internet accounts. Po stole a total of 127 login names and passwords through the Internet and resold them. Mak admitted to establishing a web to sell illegally down loaded MP3-format songs for $88 each (US $11) for a total of $15,000 (US $1,900). According to the investigators: "It is ... the first case brought to the court involving an Internet user selling stolen data to reap unlawful profits." 618

In 2000, a Hong Kong IPS discovered unauthorised alterations to its web page. It subsequently received a message demanding several thousand US dollars be deposited in a Russian Bank account in order for the attacks to cease. 619

Finally, the Department of Public Prosecution in Hong Kong mounted a number of successful prosecutions in Hong Kong in 2001 – 2002. (Table 6)

Table 6: Selected successful prosecutions of computer crimes in Hong Kong: 2001 - 2002

<table>
<thead>
<tr>
<th>Cases</th>
<th>Nature of Offense</th>
<th>Facts</th>
<th>Disposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKSAR v. KUNG Hang-ming</td>
<td>Obtaining access to a computer with</td>
<td>In April of 2002 Ms. Kung, the defendant,</td>
<td>Convicted on October 2002 of</td>
</tr>
</tbody>
</table>

618 “Singapore, Hong Kong crack down on teen hackers,” *CNN* March 23, 2000
<table>
<thead>
<tr>
<th>Case Details</th>
<th>Offence</th>
<th>Description</th>
<th>Punishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESCC 2832/2002</td>
<td>Section 161 Crimes Ordinance, Cap. (Cap. 200)</td>
<td>stole the login name and password from her supervisor and transmitted trade secrets to her new employer, a competitor. She did so by remotely controlling a Singapore computer.</td>
<td>30 offences under Section 161 Crimes Ordinances (Cap. 200)</td>
</tr>
<tr>
<td>HKSAR v. LEE Shiu-keun DCCC 1134/2001</td>
<td>Conspiracy to Defraud under Section 19 of the Theft Ordinance (Cap 210)</td>
<td>Between June 1, 1998 and March 6, 2000, the two defendants established 6 sham companies and bank accounts to conduct overseas trading. The defendants netted a total of US$1.02 million before being arrested.</td>
<td>Convicted on April 29, 2002 of 6 offences under Section 19 of Theft Ordinance (Cap. 210)</td>
</tr>
<tr>
<td>Not disclosed</td>
<td>Obtaining access to a computer with dishonest intent Section 161 Crimes Ordinance (Cap. 200)</td>
<td>In November of 2000, the defendant, a police officer, access police organized crime data to obtain information on particular vehicles and drivers so that his girl friend could track down her ex-husband’s where about.</td>
<td>Convicted on September 17 2001 under Section 161 Crimes Ordinances (Cap. 200). Sentenced to 6 months.</td>
</tr>
<tr>
<td>HKSAR v. CHAN Kwok-hung and 5 others ESCC 527/2002</td>
<td>Dealings with proceeds of indictable offences</td>
<td>The victim of this case has HK$520,000 in his bank account. Defendant Chan Kwok-hung and 5 others forged his signature to obtain a new PIN number from the bank, with it new chequebooks and an ATM account. With these, the defendants were able to transfer the victim funds electronically to their accounts.</td>
<td>Convicted on March 2, 2002 of dealings with proceeds of indictable offences</td>
</tr>
<tr>
<td>HKSAR v. CHEUNG Wing-</td>
<td>Obtaining access to a computer with dishonest intent</td>
<td>Defendant Cheung transferred money from</td>
<td>Convicted on November 13,</td>
</tr>
<tr>
<td>Hang ESCC 3532/2001</td>
<td>Dishonest intent Section 161 Crimes Ordinance (Cap. 200) and theft under Theft Ordinance (Cap. 210)</td>
<td>His girl friends’ account into his own E-banking account through another girl friend’s account.</td>
<td>2001 of 9 counts under the Theft Ordinance (Cap. 210) and 15 counts under Section 161 of Crimes Ordinance (Cap. 200)</td>
</tr>
<tr>
<td>HKSAR v. FUNG Chi-kwan, ESCC 268/2002</td>
<td>Criminal damage</td>
<td>On November 25, 2001, defendant Fung, a disgruntled dismissed employee, hacked into his ex-employer’s computer through the Internet and deleted the employer’s business records with substantial damages.</td>
<td>Convicted of one count of criminal damage.</td>
</tr>
<tr>
<td>HKSAR v. LI Tai-chung ESCC 1899/2002</td>
<td>Living off the earnings of prostitution</td>
<td>In June of 2002, defendant offered sexual services by young girls over the ICQ for HK$3000.</td>
<td>Convicted on October 11 2002 of living off the earnings of prostitution</td>
</tr>
<tr>
<td>HKSAR v. CHUNG Yee-yung, NKCC 5804/2002</td>
<td>Publishing an obscene article under section 21 of Control of Obscene and Indecent Articles Ordinance (Cap. 390)</td>
<td>The defendant, uploaded child pornographic materials (oral sex between 12-14 year old boy and a masked man) in Hong Kong onto the net and was viewed in New Jersey. In May of 2002, defendant was arrested as a result of a joint operations (“Operation Web Sweep”) between New Jersey police and HKP.</td>
<td>Convicted on September 30, 2004 for violating Section 21 of Control of Obscene and Indecent Articles Ordinance (Cap. 390) and sentenced to 14 months.</td>
</tr>
</tbody>
</table>

Source: Lo Hing Cheung, “Cyber Crime: The Challenges & Way Forward.” Paper presented at 16th International Conference, Technology and Its Criminal Responsibility, Security and Criminal Justice, Charleston, South Carolina, December 6 – 10, 2002. Lo was the Senior Assistant Director of Prosecution, Department of Justice, Hong Kong SAR.  

620 [http://www.isrcl.org/Papers/Lo.pdf](http://www.isrcl.org/Papers/Lo.pdf)
The whole purpose of this section on recitation of computer criminal cases from 1995 to 2002 is to show that by 2002 computer crime is accepted very much as part of the landscape and scenery of information highway in Hong Kong. The other point to note is that most of the computer crimes were prosecuted for the underlying criminality, from prostitution to theft to child pornography, more so than as pure Internet crime.

The challenge is now to devise effect measures to prevent their occurrence and ameliorate their impact. To do so effectively we need to understand more about the nature, prevalence, distribution and causation of computer crimes. To this subject matter we now turn.
Nature, Prevalence and Distribution of Computer Crime

As observed, the increasing widespread usage of IT and ever deepening penetration of Internet in Hong Kong has facilitated economic growth, promoted social interaction, speeded up cultural change and otherwise changed lifestyle of the people. As in other part of the computerized world, and without exception, computers and Internet brought along various kinds of computer-mediated criminality and network-related social deviance to Hong Kong. In this chapter, we will investigate into the nature, incidence, prevalence and distribution of computer crime in Hong Kong.

The emergence of computer criminality

In 1996, there were only 21 cases of computer crime in Hong Kong, being 4 hacking, 6 publication of obscene articles and 7 others for a total of 21 (Table 1). This was increased to 34 cases in 1998, and 317 in 1999 (238 hacking, 32 publication of obscene articles, 4 damages of data, 18 Internet fraud and 25 others). The jump in official computer crimes during this time did not register a precipitous rise in computer crime as much as it showed growing public awareness and increase government attention in pursing computer crime and control. 621

Table 1: Hong Kong Legislative Council: Reported Computer Related Crimes: 1996 - 1999

<table>
<thead>
<tr>
<th>Case Name</th>
<th>1996</th>
<th>1997</th>
<th>1998</th>
<th>1999</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking</td>
<td>4</td>
<td>7</td>
<td>13</td>
<td>238</td>
</tr>
<tr>
<td>Publication of obscene</td>
<td>6</td>
<td>6</td>
<td>13</td>
<td>32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal damage of data</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Internet shopping fraud</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>Others</td>
<td>7</td>
<td>2</td>
<td>4</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td>21</td>
<td>20</td>
<td>34</td>
<td>317</td>
</tr>
</tbody>
</table>


Table 1 shows computer related crime as reported by the Legislative Council Panel on Security from 1996 to 1999. Table 2 shows computer related crime as reported by the Department of Justice from 1993 – 2000. There are two instructive observations we can make in comparing these two sets of official computer crime data from 2000. First to observe is that the Legislative Council data does not include PABX Fraud as a computer crime. This could not have been an oversight, because later Legislative Council reports use the same table. The other more reasonable explanation pointed to a definition dispute, i.e., a difference in understanding of what computer related crime entails. Second, the Department of Justice data reached back to 1993 and the Legislative Council data started with 1995. The disparity reveals that there were difference assessments within the Hong Kong government as to when computer crime becomes a problem in Hong Kong. The Department of Justice apparently thinks that computer problem starts two years earlier than the Legislative Council.

Both of these observations pointed to a larger truth, i.e., there was a lack of

---

622 A PABX is a computerised system that manages an internal telephone extensions network. By manipulating the PABX system electronically one can get calls billed to owner of PABS.
coordinated approach to and common perspective on the control of computer crime and regulation of cyberspace during this time. This is evidenced by the lack of inter-departmental exchange and leadership void in this area. The Hong Kong Legco, the Law Reform Commission, the HKMA, the Hong Kong SFC, the HK Security Bureau, the HKP and HK Custom and Exercise all look at cyber risks and computer crime through their own prism – jurisdiction and priority - and approach them in their own ways. 623

Table 2: Department of Justice: Reported Computer Related Crimes: 1993 – 2000

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hacking</strong></td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>7</td>
<td>13</td>
<td>238</td>
<td>38</td>
</tr>
<tr>
<td><strong>PABX Fraud</strong></td>
<td>0</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Publication Obscene Articles</strong></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>6</td>
<td>13</td>
<td>32</td>
<td>0</td>
</tr>
<tr>
<td><strong>Criminal Damage</strong></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td><strong>Internet Shopping Fraud</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td><strong>Others</strong></td>
<td>3</td>
<td>3</td>
<td>7</td>
<td>7</td>
<td>2</td>
<td>4</td>
<td>25</td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>4</td>
<td>12</td>
<td>18</td>
<td>26</td>
<td>25</td>
<td>38</td>
<td>317</td>
<td>49</td>
</tr>
</tbody>
</table>

Source: Mr. Grenville Cross, “Symposium of ‘e-Management: Challenges and Opportunities.” Organized by Institution of Electronic Engineers Hong Kong (May 26, 2000).

1999 recorded the highest computer related crime reported in the history and certainly since records were kept since 1993. Computer crime increased from 4 in 1993 to 317 in 1999. This is a jump of 7825%. Compared with a year before (1998 ) this is still an increase of 734%.

623 The case in point was the fumbled raid conducted by the HKP and OFTA on March 4, 1995 discussed above.
Senior superintendent Raymond Lau Chi-keung of the HKP Commercial Crime Bureau observed that the computer crime rate increased as a result of increased computer ownership and use. Superintendent Raymond Lau also observed an increase in the sophistication and complexity in the computer cases. Many of the cases were perpetrated by youngster under peer pressure to how off.624

### Table 3: – IT Usage and Penetration in Household (Years 2000 to 2003)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Households with PC among all households in HK</td>
<td>67.5%</td>
<td>62.1%</td>
<td>60.6%</td>
<td>49.7%</td>
</tr>
<tr>
<td>b. Households with PC connected to Internet among (a)</td>
<td>88.8%</td>
<td>84.6%</td>
<td>80.4%</td>
<td>73.3%</td>
</tr>
<tr>
<td>c. Households with PC connected to Internet among all households in HK</td>
<td>60.0%</td>
<td>52.5%</td>
<td>48.7%</td>
<td>36.4%</td>
</tr>
</tbody>
</table>

In 2001, there was a slight decrease of computer crime cases to 235 cases. The drop may have been due to the burst of dot.com bubble and the slow-down of IT industry during the period.

In the reporting of the 2001 crime situation, the HKP attributed the decrease in computer crime in Hong Kong to heightened public’s computer security awareness and effective self-help, and the successful effort of HKP to detect, arrest, prosecute and convict computer criminals in four major cases. However, the HKP never offered any evidence, much less empirical research, to support such a contention.

In 2002, the HKP recorded a total of 272 computer crime cases, an increase of 37 cases. In addition, the Newspapers Registration Section (NRS)625 received a total of 99

---


625 Newspaper Registration Section (NRS) is one of the enforcement agencies of the
public complaints on pornographic materials against Internet between July 2001 and June 2001.

A further analysis of the computer crime statistics reveals that over 75% of the cases in 1999 and 2000 were ‘hacking’ cases. The rest were pornography cases (38% in 1998). In the recent years, the number of hacking drops while crimes in electronic commerce, such as e-banking theft and e-fraud cases increases. In 2001, 65 cases of electronic deceptions were recorded, including using stolen identity to obtain goods or services via the Internet, such as fraudulent e-shopping and e-auction. There were also 8 e-banking theft cases in 2001 involving HK$4.4 million. The HKP is much concerned with e-banking thefts because they pose significant threat to Hong Kong as a major international finance centre.626

The patterns and trend of computer crime

Table 4 summarizes the computer crime cases between 1996 and 2003 according to the types of offences currently categorized by the HKP. The total number of computer crime in 2003 climbs to 588 cases, doubling the 272 cases reported in 2002, and 21 times more than those reports in 1996. In 1993, a majority of those computer crime cases, 60.5% (356/588), involved illegal access to computer with criminal or dishonest intent. If we were to add unauthorized access to computer generally, the percentage goes up to

Control of Obscene and Indecent Articles Ordinance, Cap. 390. All the complaints received against Internet crime are in relation to the publication of obscene or indecent articles through the Internet.

68.5% (403/588). This is an up-surge of 158%, from 138 cases in 2002 to 356 cases in 2003, and 4.4 times that of 2001.

The second most prevalent computer crime is “obtaining property and service by deception” via Internet. In 2003, there were 103 such cases, constituting 17.5% of all computer crime cases. The interesting thing to note is that while obtaining property by deception has shown a steady growth pattern, from 2 cases in 1997 and 10% of all cases during that year, to 29 cases in 2000 and 7.9% of all cases during that year, to 86 cases in 2003 and 14.6% of all the cases during that year. On the other hand, obtaining services by deception has dropped, from 33 cases in 2002, and 7.12% of all the computer crime cases processed, to 17 cases in 2003, and 3% of all the cases.

The third largest crime in 2003, after unauthorized access and obtaining property by fraud, is publishing obscene materials on the net. At 58 cases this is 9.9% of all the cases. All told in 2003, three kinds of computer crime swamped enforcement: unauthorized access, computer fraud and publication of obscene material.

Table 4 – Computer Crime Cases in Hong Kong by Various Offences (1996-2003)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Yearly Total)</td>
<td>588</td>
<td>272</td>
<td>235</td>
<td>368</td>
<td>318</td>
<td>34</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>A Unauthorized access to computer by telecommunication</td>
<td>47</td>
<td>26</td>
<td>33</td>
<td>53</td>
<td>238</td>
<td>13</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>B Access to computer with criminal or dishonest intent</td>
<td>356</td>
<td>138</td>
<td>81</td>
<td>222</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C Criminal damage (computer related)</td>
<td>16</td>
<td>16</td>
<td>27</td>
<td>15</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>D Obtaining property by deception (on-line shopping)</td>
<td>86</td>
<td>45</td>
<td>32</td>
<td>29</td>
<td>18</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>E Obtaining services by deception (computer related)</td>
<td>17</td>
<td>19</td>
<td>33</td>
<td></td>
<td>49</td>
<td>26</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>
While unauthorized access and publication of obscene materials need no further elaboration, obtaining property and services by deception is worth demonstration by an example. In December of 2003, that Hong Kong Monetary Authority (HKMA) has issued an alert on dubious bank website in December 2003. Since 2003, fraudulent bank websites operated from overseas have been increasingly uncovered. Victims include prominent financial institutions in Hong Kong such as Citibank (August 2003), East Asia Credit (September 2003), and HSBC (December 2003).

*Computer crime and corporations*

How are companies in Hong Kong affected by computer crime? In 2003 Computer Emergency Response Team Coordination Centre (HKCERT), Technology Crime Division of Commercial Crime Bureau of Hong Kong Police Force (HKP), and Information

---


Technology Services Department (ITSD) of HKSAR conducted a survey of Hong Kong registered company to ascertain their experience with computer crime. The survey investigates companies’ experience with computer attacks; awareness of information security levels; extent of, technologies adoption, kinds of security strategy employed and outlay for information security expenses. The 2003 survey shows that over half of the respondents (56.2%) have installed servers and/or web sites, of which 23.3% have experienced computer attacks within the last 12 months (2003) before the survey. Computer virus attack remains to be the most dominant mode of unauthorized computer attacks at 94.5%. This is followed by hacking (13.5%) and denial of service attack (5.6%). Unauthorized computer attack impact smaller companies more than big ones. Attack on small companies resulted in a higher percentage of PCs being affected.

The survey shows that computer attacks are getting more and more sophisticated. Only about 12.2% of unauthorized attacks are traceable to local origin. The remaining 43.4% is still unaccounted for. Finally, since Hong Kong is an international business, commercial and financial center, 44.4% of the attacks are found to be originating from overseas.

In 2003, the total financial loss resulted from computer attacks is about HK$1.22 million as compared to HK$1.84 million in 2002, and HK$1.52 million in 2001. The decline in 2003 of computer related financial loss might be due to a drop in the reporting ratio by the respondents, in responding to financial impact interviews.

In 2002, only 32.6% of the victims have reported financial losses resulted from

---

computer attacks. Possible reasons for such a decline may be due to a higher awareness in information security, or under-estimation of loss due to a failure to quantify the intangible costs, such as manpower for fixing the damage and providing for recovery. Key figures of this survey summarized in Table 5 supplements the computer crime statistics released by the HKP in understanding the crime situation in the business sector.


<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Total no. of computer crime incidents</td>
<td>943</td>
<td>1,095</td>
<td>1,387</td>
<td>1,510</td>
</tr>
<tr>
<td>b. Change in percentage as compared to previous year (+/-)</td>
<td>-13.9%</td>
<td>-21.1%</td>
<td>-8.1%</td>
<td>n/a</td>
</tr>
<tr>
<td>c. Average no. of attacks per victimized company</td>
<td>2.4</td>
<td>3.4</td>
<td>3.5</td>
<td>2.6</td>
</tr>
<tr>
<td>d. Change in percentage as compared to previous year (+/-)</td>
<td>-29.4%</td>
<td>-4%</td>
<td>+34.6%</td>
<td>n/a</td>
</tr>
<tr>
<td>e. Total no. of PCs affected</td>
<td>4,098</td>
<td>5,460</td>
<td>5,366</td>
<td>4,733</td>
</tr>
<tr>
<td>f. Change in percentage as compared to previous year (+/-)</td>
<td>-24.9%</td>
<td>+1.8%</td>
<td>+13.4%</td>
<td>n/a</td>
</tr>
<tr>
<td>g. Average no. of PCs affected per incident</td>
<td>4.3</td>
<td>5</td>
<td>3.9</td>
<td>3.1</td>
</tr>
<tr>
<td>h. Change in percentage as compared to previous year (+/-)</td>
<td>-14%</td>
<td>+28.2%</td>
<td>+25.8%</td>
<td>n/a</td>
</tr>
<tr>
<td>i. Total financial loss estimated (HK$)</td>
<td>$1.22M</td>
<td>$1.84M</td>
<td>$1.52M</td>
<td>$1.38M</td>
</tr>
<tr>
<td>j. Change in percentage as compared to previous year (+/-)</td>
<td>-33.5%</td>
<td>+20.5%</td>
<td>+10.8%</td>
<td>n/a</td>
</tr>
<tr>
<td>k. Average financial loss per victimized company (HK$)</td>
<td>$3,116</td>
<td>$5,632</td>
<td>$3,888</td>
<td>$2,461</td>
</tr>
<tr>
<td>l. Change in percentage as compared to previous year (+/-)</td>
<td>-44.7%</td>
<td>+44.9%</td>
<td>+58%</td>
<td>n/a</td>
</tr>
</tbody>
</table>

(Source: HKCERT, HKP, and ITSD)

The above statistical survey data (from three most respected surveys) allows for a comprehensive analysis of the current status of computer crime in Hong Kong, in the early 2000s.

Finally, between 2000 and 2002, four major concerns prompted the Hong Kong
government to take aggressive actions to regulate cyberspace, i.e., increased in computer related deviance, increased in breach of computer ethics, violations of information privacy, and threats to electronic commerce. From available government statistics, there was also a phenomenal growth in computer crime since late 20th century.

In the following sections, we will investigate into various aspects of computer crime control and cyberspace governance policy and practice in Hong Kong.
View on Computer crime legislation

In providing for law and order in the cyberspace, the Hong Kong government has pursued strategies consistent with Hong Kong’s traditional Chinese values and established governing philosophy, i.e., small government, positive – non-interventionism, individual communitarianism and voluntarism, community empowerment and activism, and utilitarianism and pragmatism. In 2000, Legislative Councilor Sin Chung Kai–Information Technology articulated four basic principles of cyberspace legislation in Hong Kong: First, apply current law to cyberspace. Second, avoid unnecessary legislation. Third, support and promote predictable, consistent and minimum legislative regime. Fourth, introduce laws only when found necessary.

Consistent with above governing philosophy and legislative principles, the Hong Kong government recognizes a long term need to reduce the “artificial” barrier between computer crime vs. street crime legislation. The thinking within the government, as reflecting the community’s point of view, is that a crime is a crime, no matter how it is perpetrated and where it occurred:

“Our law should ideally be able to cater to the requirements of the information age without regard to whether an act is done via traditional means or in the cyber world ... [N]ew legislation or amendments to existing legislation should be drawn with an eye to the requirements of the


information age. As far as possible, legislation should be technology- and medium-neutral. Given the constantly evolving nature of the cyber world, we cannot afford to stand still in our effort to curb computer crime.”

This view about inseparability between street vs. virtual (computer) crime is based on the venerable Chinese understanding that crime is a challenge to heavenly order (tianming). Specifically, crimes are disturbances (“luan”) of “heavenly order” – embodied and personified in the Emperor’s rule - to be suppressed at all costs.634 People perpetrating crime and causing chaos were “bad” elements. Local officials who failed to maintain order within their jurisdiction were disciplined. Finally, emperors who experienced civil disorders were deemed to be unfit to rule and deprive of their legitimacy from heaven.

Cyberspace Policy

Hong Kong is considered one of the most dynamic economies in the world. In terms of economic development, e-business is a mean to enable Hong Kong to compete in a knowledge-based economy. The Digital 21 Strategy entitled ‘Hong Kong:

634 Kang Shuhua, Criminology (Fen Zui Xue (Beijing: Zhunzong chubanse 1998) (Crime is a violation of God’s will (tianyi), p. 37. Crime and disorder as challenge of Emperor’s personalized power (from heaven above) is not unique to China. See Foucault, Michel Foucault, Discipline and Punish: The Birth of the Prison. (New York: Vintage Books, 1977) (In the 17th century France, punishment must not only be done but have to be seen to be done. It must be inflicted upon the condemned, and damned, in a slow, methodical, painful, and above all spectacular way, to demonstrate the absolute power of sovereignty, to give and deliver from pain.)
Connecting the World’ promulgated in May 2001 has articulated five key objectives to improve Hong Kong’s competitive advantages, including enhancing Hong Kong’s world-class e-business environment.635

Computer security is a real concern, especially in the earlier days when the HK government has yet to refine its regulatory regime. For example, as recent as 2000, flagship companies based in Hong Kong were debating whether to run their business online. Cathay Pacific Airways was one of the first to convert to online service model to improve upon cash flow management, information interactivity, decision-making, just in time operations and system maintenance. This allowed Cathay Pacific to operate between five continents, across 20 different locations and with 28 revenue – currencies cost centers. However, HK & Shanghai Hotels with 70 subsidiaries overseas preferred to rely on their traditional cash management system. Likewise the Mass Transit Railway Corp (MTRC) was concerned enough about cyber risks and information security, especially the authorisation features, to delay embarking on e-commerce.636

The Hong Kong government, realizing the vulnerabilities of information highway for multinationals and global trade, has taken an active role in keeping the information highway free and safe.637 In the words of Paul Lovelace, an Internet and e-commerce

637 Peter Lovelock, “Telecoms Infotechnology Forum: Hong Kong as an Internet Financial Hub.” Telecommunications Research Project. October 29, 1999. (Hong Kong has to compete with other financial centers on line for transaction volumes, investor assets, listings, and offering is increasing.”)
security expert from Hong Kong University:

“Hence our position … e-commerce in Hong Kong will continue to lag until the government becomes more involved in providing the necessary ‘soft’ infrastructural development for commerce by cyberspace. By this we mean the legal framework for e-commerce, the regulatory framework for banking and securities trading, the security framework for merchants, and for copyright and data protection, and a new, more appropriate, emphasis upon education, training, research and development.” 638

Accordingly, the Hong Kong Security Bureau has established a strategy to enhance the capable Hong Kong government’s capacity to deal with emerging computer crimes and vulnerable cyber security; pledging “to strengthen present monitoring of and response to computer crime trends and developments.” 639 The Hong Kong Police (HKP) was charged with the implementation of such a strategy in making Hong Kong one of the safest and most stable, business friendly societies in the world.

The private sectors and various business associations, not satisfied with the governments conservative approach, have called for a more aggressive approach and assertive presence by the Hong Kong government. 640 For example, Hong Kong

640 The private sectors and various business associations have called more for a more aggressive and pro-active approach by the Hong Kong Government. “Response to the Digital 21 consultation document,” Hong Kong Coalition of Service Industries and Hong Kong General Chamber of Commerce (December 2003). (The government should
Coalition of Service Industries and Hong Kong General Chamber of Commerce in response to the “Digital 21 consultation document” has called for a more robust and focused IT development plan, including: increasing IT education and training, strengthening intellectual property rights protection, upgrading of communications infrastructure in the Pearl River Delta region, conducting structural review of the regulatory framework for broadcasting and telecommunications, appointing a champion to coordinate regulatory policies and industrial involvement across the information industries. 641

Cyberspace policy in action

Unlike the motherland of China, 642 Hong Kong government does not monitor and regulate the flow of information on the Internet. The right of free speech is firmly secured by Article 27 of the Basic Law: “Hong Kong residents shall have freedom of speech, of the press and of publication; freedom of association, of assembly, of procession and of demonstration; and the right and freedom to form and join trade unions, and to strike.” 643

Hong Kong people enjoyed unimpeded free expression and privacy rights on the

641 “Response to the Digital 21 consultation document” (December 2003)
643 The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (Adopted on 4 April 1990 by the Seventh National People's Congress of the People's Republic of China at its Third Session.)
This yearning for freedom clashes head on with an emergent concern for the protection of intellectual property rights, computer security and fair competition in cyberspace. It also challenges entrenched traditional Chinese values of proper moral education for the younger generation in a cyberspace age.

Just as in mainland China, Hong Kong government has placed much effort in promoting healthy, ethical and moral use of Internet. The approach in Hong Kong however is more de-centralized and communalized. Education efforts are not centrally coordinated and much depends on community voluntarism and individual self help, e.g., having computer association to led security awareness and information ethics efforts.

Hong Kong government takes an aggressive leadership role in spearheading the

644 Kam C. Wong and Georgiana Wong, “Law and Order in Cyberspace: A Case Study of Cyberspace Governance and Internet Regulations in PRC” supra.

645 Hong Kong Computer Association has argued for a bottoms up, instead on top down approach in providing for IT education and training. “Information Technologies & Education Quality Our Investment into the Future.” (“Encourage private sector participation from the outset - We believe this Program will have a better chance to succeed when it is not engineered as a top-down, purely government-funded initiative. Social re-engineering programs which are too public-sector focused or government-centric, lacking private sector and commercial sector participation from the outset can become ineffective and slow in implementation.”) See samples of Hong Kong professional association’s effort at security education, see “eFinance Security Seminar Hong Kong 2002,” January 25, 2002, Hong Kong Convention & Exhibition Center. Organized by Computer Associates (CA), Supporting Organizations: Hong Kong Computer Society (HKCS), Information Security and Forensics Society (ISFS), Professional Information Security Association (PISA); Technical Workshop: Phishing Exposed, Nov. 6, 2004, City University of Hong Kong Professional Information Security Association; “Incident Response and Forensics Workshop,” Mar 21, 2004, Hong Kong Convention & Exhibition Centre, Organized by: HKPC and HKCERT.
teaching of computer ethics.\textsuperscript{646} The Inter-departmental Working Group has recommended joint efforts of the public and private sectors in promoting public education in computer security awareness and information ethics.\textsuperscript{647} Such call to arms has resulted in many joint ventures. For example, on August 15, 2003, The Hong Kong Police, Education and Manpower Bureau, Television and Entertainment Licensing Authority, with the active participation of Information Systems Audit and Control Association (Hong Kong Chapter), jointly organized a computer ethics promotion program for the youth.

In this regard, the Hong Kong government’s approach to computer ethics education resembles that of the United States.\textsuperscript{648} For example, the U.S. Department of Justice

\textsuperscript{646} For Hong Kong government and related departments’ effort to educate the public on computer security and ethics, see “Publicity and Education Efforts,” 2001 Computer Crime Report. Annex 9, pp. 106 – 116. Various departments who are involved with publicity and education efforts, include: Hong Kong Police Force – Crime Prevention Bureau – Computer Crime Section; Information Technology and Broadcasting Bureau and Information Technology Services Department; Office of the Telecommunication Authority; Office of Privacy for Personal Data; Commerce and Industrial Bureau/Intellectual Property Department; Hong Kong Productivity Council; Consumer Council; Fight Crime Committee. Conspicuously missing are the HKMA and HKSFC, both while being quasi-public institutions are sufficiently involved with implementation of public policy that there efforts in IT security education and training must be coordinated and integrated.

\textsuperscript{647} “Leveraging Information Technology – Ethics Perspectives for Managers Forum 2001” The Hong Kong Ethics Development Centre (HKEDC), ICAC, 2001/11/27.

(DOJ) encourages the young people to use the Internet correctly through the sponsorship of educational programs, e.g., the Cybercitizen Partnership.

The Hong Kong government also takes a pro-active approach in fighting computer crime. In this regard ICAC takes the lead to work with 13 local businesses associates to developing good ethical guidelines to prevent computer crime, unethical, corrupt and criminal activities from happening. The guide includes case illustrations from the ICAC’s investigation files illustrating common patterns of computer crime in business organization and provide an ethical management model with practical tips of how to prevent work place computer crime from happening. Likewise, The HKMA routinely sends security circulars and guidelines to alert bank management and operatives to structural security problems or emerging security risks.


650 “ethics@work - a guide for business managers in the use of IT” The ISACA, the ICAC and 13 professional organizations/chambers of commerce have collaborated to produce the captioned Guide.

651 Id.


653 “Precautionary measures against fake e-mails or websiter.” (Fraudsters send e-mails to the public in the guise of Authorized Institution (AI) requesting the bank customers to make connection to a fake bank website and devolve sensitive information.) HKMA Guidelines and Circulars. Ref. B1/15C, B9/29C, September 30, 2004
Computer Crime Legislation

The Computer Crimes Ordinance in Hong Kong was enacted in 1993 through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210), with some new offences created and the coverage of existing offences extended.

Table 1 below summarizes the relevant provisions of Hong Kong law being used to combat computer related crimes and their maximum penalty.654 The Inter-departmental Working Group once considered an option to capture all legislative changes regarding computer crime in one ordinance, but finally decided to leave the discretion to the law draftsman for an appropriate vehicle.

Table 1 – Provisions of Computer Crimes Ordinance in Hong Kong

<table>
<thead>
<tr>
<th>Law</th>
<th>Provisions</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cap. 106, S.27A</td>
<td>Prohibiting unauthorized access to computer by telecommunication</td>
<td>Fine of $20,000</td>
</tr>
<tr>
<td>Cap. 200, S.59</td>
<td>Extending the meaning of property to include any program or data held in a computer or in computer storage medium</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Cap. 200, S.59 &amp; 60</td>
<td>Extending the meaning of criminal damage to property to misuse of a computer program or data</td>
<td>10 years’ imprisonment</td>
</tr>
<tr>
<td>Cap. 200, S.85</td>
<td>Extending the meaning of making false entry in bank book to falsification of the books of account kept at any bank in electronic means</td>
<td>Life imprisonment</td>
</tr>
<tr>
<td>Cap. 200, S.161</td>
<td>Prohibiting access to computer criminal or dishonest intent</td>
<td>5 years’ imprisonment</td>
</tr>
<tr>
<td>Cap. 210, S.11</td>
<td>Extending the meaning of burglary to include unlawfully causing a computer to function other than as it has been established and altering, erasing or adding any computer program data</td>
<td>14 years’ imprisonment</td>
</tr>
<tr>
<td>Cap. 210, S.19</td>
<td>Extending the meaning of false accounting to include destroying, defacing, concealing or</td>
<td>10 years’ imprisonment</td>
</tr>
</tbody>
</table>

Given the trans-border nature of computer crime, the Working Group had completed a comparison study of our existing legislation with reference to the “Draft Convention on Cyber-Crime” of the Council of Europe (COE). The COE has identified four major categories of offences and recommended they be incorporated into the substantive criminal law of participating countries. The four categories of computer crimes are: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and ancillary liability and sanctions.

Table 2 below presents an analysis of computer-related offence provisions, based on the COE classification of offences as defined in the Draft Convention. Altogether, the Working Group has presented a framework with 57 recommendations of legislative and administrative measures to improve the Hong Kong regime in tackling computer crime.

Table 2 – Analysis of Computer-Related Offence Provisions in Hong Kong Based on the Council of Europe Classification of Offences

<table>
<thead>
<tr>
<th>COE Classification of Offences</th>
<th>Hong Kong Ordinance</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Illegal access</td>
<td>Crimes Ordinance</td>
</tr>
<tr>
<td>Cap.200, s161 (5 yrs max.)</td>
<td></td>
</tr>
</tbody>
</table>

655 The Council of Europe (COE) is an international organization with 41 member states. It seeks to, inter alia, strengthen the rule of law throughout its member states by encouraging the adoption of common practices and standards. COE website at http://www.coe.int.

The HKSAR Computer Crime Report (2000), while far from perfect,\textsuperscript{657} is more

\textsuperscript{657} There are many problems and issues afflicting the conduct and findings HKSAR Computer Crime Report (2000), including: First, the Working Group failed to include essential parties, such as representatives from HKMA or HKSFC. Both parties are pioneers to the cyberspace risk management and computer crime control field, i.e., since 1996. These parties also have important vested interest, long experience and substantial expertise in the dealing with computer crime to share. Second, the Working Group has no valid and reliable computer crime data to work from. Third, the Working Group has failed to conduct comprehensive empirical study on the magnitude and impact of computer crime on Hong Kong society in general, and upon specific commercial segments in particular, e.g., banking industry or global trade. A comprehensive critique...
than adequate to “identify the challenges to law enforcement” and “review the adequacy of existing legislation and relevant administrative measures” to deal with enforcement challenges. It “examine international developments …and draw lessons” and make “recommendations to address the inadequacies identified”. In so doing, the Working Group takes a balancing cost-benefit approach to policy formation, taking into consideration law enforcement needs and compliance costs in recommending actions.658

The HKSAR Computer Crime Report (2000) legislative proposals were well received659 but not without contentious debate, from law society, 660 business
associations, computer professionals and cyberspace academics.

The Criminal Law and Procedure Committee of the Hong Kong Law Society has raised a number of concerns. For example, the Working Group has called for legislation in enhancing the investigative power of law enforcement agencies, particularly recommending that officials should be provided “with decryption tools or the decrypted text of encoded computer records where necessary and justified.”

The Hong Kong Law Society in their submission finds the HKSAR Computer Crime Technology Federation - submission to follow; Hong Kong Society of Accountants and Information Systems Audit and Control Association (Hong Kong Chapter) LC Paper No. CB(2)828/00-01(02) - joint submission; Hong Kong Institution of Engineers (Information Technology Division) LC Paper No. CB(2)828/00-01(03) – submission; Webmasters (Hong Kong) Association LC Paper No. CB(2)811/00-01(04) - submission (issued on 6.2.2001); Mr Wanbil LEE - submission to follow. http://www.legco.gov.hk/yr00-01/english/panels/se/agenda/seag1002.htm


661 For example, see “Report on Inter-Departmental Working Group on Computer Related Crime Response by the Hong Kong General Chamber of Commerce” Hong Kong General Chamber of Commerce (02/2001) (“This Report on Computer Related Crime is a very timely, in light of the increasing concern for crimes related to the use of the computer and the Internet. We are pleased that many of today’s issues have been taken up in this report”)


Report (2000) objectionable on privacy and other grounds. Specifically, the Law Society submission raised the following concerns:

“(a) implications of the proposed legislation on the development of e-commerce;
(b) potential infringements of privacy;
(c) implications for the disclosure of encrypted information, which may include legally privileged information;
(d) the right of individuals against self-incrimination,
(e) the need for disclosure of keys when access to plain text would be sufficient; and
(f) the need for the empowered agencies to be fully accountable to democratic institutions and subject to public scrutiny.” 665

Professor Samuel Chanson of Department of Computer Science, Hong Kong University of Science and Technology and Chairman to Information Security and Forensics Society (ISFS) finds the HKSAR Computer Report (2000) “a step in the right direction”. 666 However the Report needs to balance the conflicting considerations of investigation, privacy, and cost to provider and public. 667 Professor Chan cautioned against placing too much emphasis on legal issues, e.g., definition of computer crime, and enforcement problems, e.g., investigative powers. It is as important if not more important

667 Id. Slide 5 of 15.
to put effort into the prevention of computer crime. Finally ISFS made the following recommendations in improving the HKSAR Computer Report (2000):

1. **On Privacy.** In order to develop Internet to its fullest potential, privacy is a major concern, especially while the data is in transit or on storage. Thus data flow should be protected by Personal Data Ordinance. Any future computer law should only be adopted after in-depth study of its impact on privacy.

2. **On fighting computer crime.** The government should work with the IT community to fight computer crime, e.g., engaging the IT community in defining, identifying, preventing, detecting and investigating computer crime. This includes seeking assistance and cooperation from ISPs and web hosting companies in investigating computer crimes, e.g., helping to preserve forensic evidence, maintaining security adopting standards and procedure to prevent computer crime.

---

668 *Id.* Slide 7 of 15.
669 *Id.* Slide 8 of 15.
670 “Information Security Practices for Banks and Financial Institution.” Hong Kong Computer Security, Information Security Specialists Group, Special Industrial Form. 16th August 2003. (The forum addresses “Incidence Response and Investigation”. It addresses issues on how to response to incident, contain damage, trace evidence, take remedial actions and find resources. The panel speakers came from Head of Compliance, DBS Bank, Head - Banking Development Department Hong Kong Monetary Authority, HKP, Technology Crime Division, Commercial Crime Bureau, Secretary HKISPA, Center Manager, Hong Kong Computer Emergency Response Team Coordination Center, Senior Manager, Regional IT Security, Hong Kong Shanghai Bank.)

671 “Comments on Government’s Report on Computer Related Crime”. Power-point presentation by Professor Samuel Chanson, Slide 9 of 15. See e.g., “Hong Kong Internet
(3) *On setting best industrial standards.* Police, academics and IT professionals should collaborate to come up with best industrial standard on issues affecting computer security that will be acceptable in court. 672

(4) *On computer crime prevention.* The government, should promote computer security awareness to the public and SMEs. 673

(5) *On computer security experts.* There is a gross shortage of computer security and forensic experts. The government should work with the university to develop computer security, investigation and forensic courses. 674

The Hong Kong Internet Service Providers Association (HKISPA) was very much encouraged by the government’s attention to computer crime. Overall, it supports the government’s effort to improve cyberspace governance and considers many of its recommendations positive ones. HKISPA is however opposes to a number of the HKSAR Computer Report (2000)’s recommendations, including:

---

(1) The Report called law enforcement agency being given: “uninhibited access to the decryption key or decrypted text.” HKISPA considered disclosure of encryption code or text for investigation purposes as both necessary and reasonable. However in order to protect public expectation of privacy and safeguard against possible police abuse, the disclose such keys should only be done with judicial oversight and according to stringent guidelines.

(2) The HKSAR Computer Report (2000) called for the punishment of unauthorized access to computer data: “As long as the unauthorized access is done by telecommunication, criminal or dishonest intent does not have to be proved.” HKISPA objected to punishing people who accidentally or inadvertently entered others’ computer domain or data set. It suggested punishing unauthorized access to computer or data only when intent can be positively demonstrated.

(3) To deal with “defection of computers” future legislation should prohibits “intentional scanning and sending false data to a system which caused serious malfunction or damages.”

(4) It recommends that the request for assistance to ISPs by law enforcement officials should be reasonable and not prohibitive in costs or efforts.

---

676 Report 6.18, p. 32.
The Hong Kong Police Force (HKP) has taken active steps to deal with computer related crime as early as 1993 when legislation was first amended to address computer crime. 678

New offences such as 'Unauthorised Access to Computer by Telecommunication', 'Access to Computer with Criminal or Dishonest Intent', and 'Criminal Damage' to computer data have been created…In those days, the cloning of a mobile telephone was a typical computer crime where the computer was a tool in making unauthorised duplicate telephones to be used at the expense of the owner of the victimised telephone account. Other incidences of computer involvement in crime include the use of computers to store data pertaining to illegal enterprises and to publish obscene articles.” 679

Three characteristics define the nature of computer crime during this time. First, computer crimes were local crimes. They were yet to be globalized, e.g., facing worldwide hacking or virus attacks on a daily basis. The criminal act, victim and offender remained in Hong Kong police jurisdiction. 680 Second, computer crimes were convention crimes conducted with computers, e.g., fraud. Third, computer was used an as instrumentality of a crime, e.g., storing betting

680 Id.
and payout information. It is not essential elements of the crime itself, e.g.,
spamming or hacking.

The HKP was ill prepared to confront computer crimes in the earlier years, cir.
early 1990s. Chief Superintendent Victor Lo in charge of Commercial Crime Bureau
which has jurisdiction over computer crime at the time observed that there were many
difficulties and issues in investigating computer crime, tracing digital evidence, and
tracking cyber criminals, specifically: (1) Computer crime happens in a split second; (2)
computer crime hurts multiple victims and occasions wide ranging damages; (3)
computer crime causes many small damages adding up to big loss; (4) computer crime
has no face-to-face contact, making identification impossible; (5) computer crime makes
fraud easy to perpetrate but difficult to recover; (6) computer crime trail can be easily
mediated and concealed; (6) computer crime evidence collection is difficult with multiple
jurisdictions; (7) computer crime investigation across jurisdiction is made difficult as a
result of lack of uniformity between criminal justice jurisdictions; (8) computer criminal
identification is time consuming and labor intensive; (9) computer crime electronic
investigation and surveillance might conflict with human rights and personal privacy; (10)
computer crime investigation requires ISPs to keep data and records which could be
cumbersome and costly; (11) computer crime investigation need to link criminals and
crime; (12) computer crime might be conducted by insiders. 681

Altogether, the criminal investigation structure, process, culture, staffing, training,
experience and expertise of the HKP were not suited for the effective investigation of
computer crime.682

681 Id.
682 According to academic research into organization and practice of criminal
During this time, HKP was not ready for the onslaught of computer. The HKP itself has few computers, much less computer expertise, IT professionals, cyber investigators and forensic experts. In 1993, The HKP finally established its first ever Computer Crime Section within the Commercial Crime Bureau with 17 officers. One of the key challenges from the outset is the ability to recruit and train a cadre of officers with good computer knowledge and skills. The HKP lack of basic computer technical knowledge and investigative skills came to forefront when police was not able to bring cyber criminals successfully to justice, e.g., in 1995, a police raid on a “hacker’s” premise was bungled when the suspect was able to flip the fuse-box switch and turned off the computer system, destroying all the evidence necessary for prosecution in the process.

The strategy then was to sent officers overseas for training. Such trainings while essential in upgrading HKP officers technical computer crime knowledge, did not adequately equip them to conduct computer law enforcement or cyberspace investigation in Hong Kong:

“Of paramount importance was the need for accredited training, which would enable our officers to withstand challenges when giving evidence in court. In addition, overseas training courses did not address such crux investigation in the United States, traditional criminal investigators are generalists, not specialists. They are selected for making street arrests and cracking conventional crimes. Few of them received training as detectives, much less computer forensics and investigation. Most local and smaller police departments do not have dedicated forensic resources readily available to them in the timely manner. Very few worked with community to prevent or detect crime. The picture likewise reflect Hong Kong situation.

issues as local legislation, procedural matters which conform to current
Hong Kong Police standards, and importantly, the language issue of
searching and retrieving data written in character sets."684

Because of the lack of resources, competence and size of the Computer
Crime Section, much of the work done during this period is one of computer
security education and advisement, typical of the work style of the Crime
Prevention Bureau. For example the Computer Crime Section, working with well
connected public agencies, e.g., Department of Education, or more knowledgeable
private partners, e.g., KGMP Peat Marwick (Computer Audit Department), to
publish accessible computer security manual, 685 holds public computer security
awareness and ethics seminars and provide on site visits to inform small business
owners on how to protect against computer crime. 686

Into the 2000s, HKP cyber crime law enforcement resources were devoted mainly to
three areas: policing computer crime; developing computer investigative skills and
forensics capability, and promoting public awareness in computer security.

In order to improve computer crime investigation and prosecution, the HKP set up
TCD was supported by a computer forensics laboratory. TDC was augmented by a

684 Mr. Victor Lo, “Police Training for Cyber Transformation.” Paper Presented at
Transnational Organized Crime Conference, Hong Kong (March 18 – 21, 2002), p. 3.
685 See “Computer Crime for users of small computer systems,” Crime Prevention
Bureau, HKP (1997)
686 See “Publicity and Education Efforts – Hong Kong Police”. In Inter-departmental
Computer Crime Investigation Cadre (currently known as Technology Crime Initial Response Team (TCIRC) of 80 computer proficient officers assigned to different regions to handle minor computer investigation and forensic examinations. TDC was left with handling more serious and complex cases.687

In July of 2001, the HKP established a Computer Security Unit (CSU) within the Crime Prevention Bureau to educate the public about the nature and extent of computer crime risks and to assist businesses to adopt measures to avoid from becoming victims of computer crime.

In light of HKP effort to deal with computer crime and on occasion of the Commission of Police Hui Ki-on’s alarm over the growth of computer related crimes, I have written the following Op-ed essay raising issues and challenging the approach taken by the HKP in tackling computer crime:688

On 2 January 2000, the Commissioner of Police, Hui Ki-on, sounded the much anticipated but belated alarm – computer crime is coming. Computer related offences have surged from 34 in 1998 to 266 in 1999, an almost eight-fold increase. A majority of these cases, 71% or 189 cases, concern hacking; a citizens reported crime. The crime surge is for real.

The Hong Kong Police has promptly taken four steps to address the incipient problem: (1) establishing a task force of 80 officers to crack down on computer crimes; (2) thinking about improving upon the current legislation on

688 Kam C. Wong, “Policing Computer Crimes,” Department of Government and Public Administration, Chinese University of Hong Kong. (On file with the author.)
police investigative powers on computer offenses; (3) educating its officers on computer forensic science; (4) educating the public on the prevention of computer crimes.

What are the difficulties with policing computer crimes? How can the situation be improved?

The biggest challenge to the Hong Kong Police is in fully understanding and properly reacting to computer crimes in the society.

The Hong Kong Police have a problem with understanding the magnitude (totality) and appreciating the significance (impact) of the problem on hand. More graphically, the Hong Kong Police have a difficult time in knowing its enemy lurking in the dark - mapping out the contour and tracing the relief of computer crime territory in Hong Kong. In real terms, what are the total incidences and relative distribution of computer crimes in the SAR.

How many computer crimes are out there? How are they distributed in the social space, e.g., do computer crime happens more to rich people? educated people? young people? What is the typical profile of a computer criminal? More significantly, what causes computer crimes?

No one knows for sure, since not everyone report on computer crimes in Hong Kong, e.g., being hacked. However, one thing seems certain - the Hong Kong Police are looking only at the tip of a submerged iceberg.

The reasons for not reporting computer crimes are many. They are not unlike why crime victims do not report traditional crime, e.g., they do not think a crime has been committed; do not think it is too serious to report; do not think the police can do anything about the crime, it is too much trouble to report. In this
regard, there is big obstacle in crime reporting and recording, there is as yet no commonly agreed definition of what computer crime entails, world wide.

Take the case of banks. It is a common practice of banks in Hong Kong (and world-wide) to deal with commercial and computer crimes in-house. With computer crimes, the banks rather pay the hackers and learn from the experience than seeking the help of the police. Some banks even hire hackers as a security consultant in order to improve upon its system-security performance.

Police investigation disturbs business, compromises bank-client confidentiality and tarnishes good-will. Banks also believe that they have the resources and expertise to handle the investigation better than the police. Banks can hire computer security firms to prevent and detect computer crimes. The consultants are more solicitous of the banks’ business interests, more protective of their trade secrets, and more proficient in tracking down computer criminals.

Without knowing the full extent of the totality and impact of computer crimes, the Hong Kong Police will not be effective in fighting them, e.g., police resource deployment is a function of the seriousness (magnitude and significance) of a given crime problem. The more serious the problem, the more attention is given by the police. Currently, the Hong Kong Police are at a loss at to how to classify the seriousness of the computer crime problem. This resulted in an inability to properly prioritize, rationally, the deployment of necessary police resources dedicated to dealing with computer crimes. Rhetorically, is 80 officers too little? too many?

Problem with reacting to computer crimes. There are four issues here.

First, calling it a computer “crime” does not make it a crime.
Second, calling it a computer “crime” does not make it a police business. The Hong Kong Police is not the only law enforcement agency in town, e.g., ICAC, Immigration Department, Fire Department all have law enforcement powers and investigative responsibilities in their own respective jurisdiction. More practically, the Hong Kong Police possess no accumulated experience, special resources or professional expertise in fighting computer crimes. As a matter of fact, Hong Kong Police is experienced in fighting street level crimes and a novice in combating cyber crimes.

Asking the Hong Kong Police to investigate computer crime is justified only on grounds of tradition and as a result of convenience, i.e., through incremental adhesion of policing functions (same as ICAC taking on non-corruption investigation), and not as a result of rational allocation of functional responsibilities based on objective criteria, e.g., based on demonstrated expertise or proven competence. More to the point, should a specific agency – Hong Kong Computer Crime Control Agency - be set up to deal with computer crimes?

Third, there is the issue of how police should prioritize the deployment of its resources. Police resource is an expensive commodity. They must be deployed as against needs. Though it is said that the role of the police is to fight crime and maintain order, its day to day activities is more concerned with providing services (70% of the time). How many police officers should the Hong Kong Police allot to the “cyber beat”? Should this determination be based on the number of criminals, on the viciousness of the criminals, on the number of crimes, the number of victims or social, economical or personal impact of the crime. One thing we know about computer crime is the fact that one relative innocent teenager could cause billions dollars of damages to thousands of people,
worldwide!

Fourth, there is a question of whether Hong Kong Police will ever be effective in fighting or dealing with computer crimes. There are two problems. First, computer crimes know no state boundary. This poses problem of cross-border law enforcement. It is more difficulty in terms of time and effort to investigate cross-border crime. There are complicated problems with legality (criminal law jurisdiction), difficult problems with bureaucracy (international cooperation), insurmountable problems with resource limitations, and uncertain prospect of deterrence (across border). For example, should a country which exports computer crimes, say U.S.A., be required to pay for law enforcement costs of a countries affected by a computer crime, say Hong Kong. Presumably, the computer crime exporting country will have an incentive and is in a better position to track down the computer criminals at large. Second, police law enforcement resources and efforts are no match with the ingenuity, skills and dedication of computer criminals. By making this observation, I surmise that computer crimes, as “automated information system” crimes, is mostly committed by young people who take on computer criminality for fun or as a challenge. These people are computer addicts and have a lot of time on their hand. Multiply this criminal profile by the millions and millions of young people all over the world who have time and a computer at their disposal, this is the criminal population the Hong Kong Police has to deal with. Are they ready or able to take on this world-wide challenge?

The invention of the computer as an “automated information system” has complicated the investigation of crimes and punishment of criminals by many
folds. Whether the Hong Kong Police will ever have sufficient resource or capacity to be able to deal with such kind of crimes remain to be seen.

My timely critique fairly sum up some of the difficulties confronted by the HKP in dealing with computer crime in the 2000s

HKP is not the only law enforcement agency with computer crime jurisdiction. The Hong Kong Custom and Excise Department also acquire cyberspace jurisdiction on account of Intellectual property rights infringements, e.g., piracy of movies or duplication of copyrighted CDs. Just like the HKP, until very recently (1990s), custom officers suffered from a lack of interest in and knowledge about computer technology, and related computer crime investigation techniques.\textsuperscript{689} In response, the Custom and Excise Department established an all volunteer Computer Forensic Special Interest Group to build up basic skills and keep abreast of development in cybercrimes. Of the 75 members in the Interest Group, 20 of them were specially trained to conduct cybercrime investigation as a member of a Computer Analysis and Response Team.\textsuperscript{690}

In January of 2000, the Custom and Excise Department established its first ever Intellectual Property Investigation Bureau (IPIB) with 7 officers in charge of investigating intellectual property rights infringement activities on the Internet.\textsuperscript{691} As a result of such re-organization, the investigation into and prosecution of infringement of copyright cases jumped from 1 in 1999 to 43 in 2000 (Jan-June). Since then the

\textsuperscript{689} Mr. Vincent Poon, “Challenges to Enforcement of IPR.” Paper Presented at Transnational Organized Crime Conference, Hong Kong (March 18 – 21, 2002), p. 2.
\textsuperscript{690} Mr. Vincent Poon, “Challenges to Enforcement of IPR.” Paper Presented at Transnational Organized Crime Conference, Hong Kong (March 18 – 21, 2002), p. 3.
\textsuperscript{691} “Inter-departmental Working Group on Computer Related Crime (September 2000)”, (HKSAR, 2000), p. 78.
enforcement effort has increased to that of 1149 cases, 106 arrests and 27.9 millions property seized in 4/2002 to 4/2003.692 Data from the Department (1-4/2004) shows that Copyrights arrests constituted 12.1% of the Department’s activities in 2004.693

Finally, the difficulties is investigating cybercrime is best summarized by a HKP turned computer expert, Hilton Chan: (1) Computer crimes can be remotely perpetrated; (2) Computer crime creates insurmountable jurisdiction issues, from trying to determine where the crime is committed to which country possess original jurisdiction, to how warrants are to be executed; (3) Computer crimes can be perpetrated with low costs and high yield; (4) Computer crimes can be committed with high speed; (5) Computer crimes are low risks activities due to difficulty in tracing offenders in real time; (6) Computer crimes involve stealing of information which has no easily ascertainable value; (7) Computer crimes involve “stealing” of information which is considered by most people to be unethical conduct and not criminal behavior; (8) Solving computer crimes requires the collection of electronic evidence spread across the world; (9) Computer crimes avoid detection because of low awareness; (10) Computer crimes mean different things in different culture; (11) Computer crimes are new concepts yet to be totally understood and completely accepted; (12) Computer crimes are facilitated by more users friend computer design and readily available criminal tools, e.g., hacking program on net; (13) Investigation of computer crimes is obstructed by different hardware and software in

692 The figures provided by the Custom and Exercise Department do not draw a distinction between Internet related, e.g., download of Copyrights materials and convention Copyrights violation, e.g., seizure of CD at border. See “Statistics on Cases and Seizures under Selected Ordinances” Custom and Exercise Departments. http://www.info.gov.hk/customs/eng/statistics/s_case_e.html (Visited November 5, 2004).
Computer systems; (14) Computer criminals emboldened by lack of reports; (15) Computer crimes live in a permissive and free for all computer culture. 694

Thus observed there are three obstacles standing in the way of effect computer crime investigation and prosecution:

First, there is a need to overhaul the current computer legislations to give law enforcement agencies more power to investigate cross-border computer crime.

Second, there need to be international protocols or rules governing, retrieval, preservation and authentication of computer forensic evidence such that can be used in criminal proceedings across national boundary.

Third, there is a dire need to provide for structured and relevant computer training such that the officers appreciate the concepts and theory about cybercrime 695

**Computer Crime Prevention through Education**

Prevention is a proactive measure in combating crime. In view of the penetration of PCs and Internet usage at home and in business, public education plays a key role in raising security awareness and cultivating information ethics. There are plenty of initiatives, such as exhibitions and seminars, by various government agencies and the private sector in promoting the importance of information security. Unfortunately, these individual efforts need a closer coordination in yielding better results.

The government departments, such as ITBB/ITSD and HKP, each offers their own


publicity programs. They sometimes overlap. The NGOs and quasi-government agencies are also playing a very active role. Broadly speaking, the current education efforts tend to address three major groups of target audience: the banking and finance industry, the business community (particularly SME), and the mass public.

Among the private sectors, the banking and finance industry are the most active in providing for training and education on a continued, and sometimes commercial basis. Many of the larger commercial establishments have engaged in-house profession security staff to handling information security breach and risk management training.

The Hong Kong Monetary Authority (HKMA) takes a high profile leadership position in working with banking members to formulate finance/banking guidelines and best practices for adoption. Besides publishing the guideline for the industry members, HKMA does not take an active role in customer education programs.

The Hong Kong Productivity Council (HKPC) is primarily responsible for computer security educating and publicity campaign for the SMES. For example, working together with the Consumer Council and the Office of Privacy Commission for Personal Data (PCO), HKPC and PCI jointly published and distributed an education leaflet: ‘Guide to Personal Data Privacy and Consumer Protection on the Internet’ to the SMEs.

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) of HKPC acts as an information clearance centre to share and exchange security information, such as news on virus and vulnerability on system software. HKCERT also conducts surveys, provide consultancy and render assistance to prepare SME against cyber attacks.

In coping with the increasing need for public awareness and education programs on computer security issues, the Crime Prevention Bureau (CPB) of HKP established the
Computer Security Unit (CSU) in July 2001, a specialized unit dedicated to provide services to the Hong Kong public in advising on all aspects of computer security and promoting public education on computer security awareness.

The HKSAR Computer Crime Report (2000) informs us that the government has made a conscious decision to engage the private sectors in taking a larger and more active role in computer security education and publicity. This approach is based upon a philosophy that “every user has a responsibility to protect his own computer system and data … we cannot rely on the Government alone”.696

Regrettably, HKSAR Computer Crime Report (2000) fail to discuss the role of the Education Department or universities in preparing the Hong Kong community or helping the Hong Kong people in meeting computer security needs, either through education or research. These organizations should have a prominent role to play in helping the young people to become better cyber citizens, legally and morally.

Chapter Seven

Conclusion

The Internet has fundamentally changed our way of life. Internet contributes to our personal enrichment, government efficiency and business productivity. Computer technological development also gives rise to new criminality as it aggregates old ones.

The Hong Kong government wants to build an information rich and knowledge-based economy for the 21st century and beyond. In constructing the information highway, Hong Kong government is very much concerned with deviance and disorder in the cyberspace. Under the leadership of the Security Bureau, an Inter-departmental Working Group was established to study the technology problems and legal issues in making the cyberspace safe. The HKSAR Computer Crime Report (2000) proposed a framework for improving the existing cyberspace security regiments by July 2001.

Consistent with tradition philosophy and contemporary policy, the Hong Kong government has adopted a passive, reactive, minimalist and piece meal approach in confronting computer crimes. The Hong Kong government also does not have an overarching philosophy, long time vision and integrated sets of policy in bringing about law and order in cyberspace that is compatible with Hong Kong ethos, values and interests. The government talked much about consulting the public and deferring to the professionals, in order to map a course for computer security development. But the public, by and large, is still not aware of the significance of computer security or the necessity for information ethics. The professionals, knowing too much, are more solicitous of their own welfare and interests, than that of the public.

The Hong Kong government should adopt a comprehensive approach in formulating and implementing a computer crime policy. With this in mind, governance in cyberspace
is a matter of managing the combinations of laws, norms, the market, the architecture (or code), and ethics to achieve order in the cyberspace. Comprehensive approach to computer crime fighting also calls for co-operations from all those people who have a vested interest and those can make a difference. In this regard, the government should take a stronger leading role in promoting public awareness and mobilizing public support for computer security.

Cyber-crime is an emerging problem in Hong Kong. Internet recognizes no border. Fighting computer crime very often needs a joint effort from various governing regimes and assistance from different legal jurisdictions. The Hong Kong government should continue to work with international institutions and overseas regulators in sharing information, developing best practices, and adopting uniform legislation in to facilitate cyberspace governance. It is crucial for the government to act proactively before computer crime develops into a burning issue – a price too high for Hong Kong citizens to pay. Finally, the study of cyberspace governance in Hong Kong is still at an immature stage. There are much to be discovered by scholars, researchers and professionals in the field.
APPENDIX I

The Internet Timeline of China Series, CNNIC: 1987 to 2004

1. In September 1987, with the support from a scientific research group led by Professor Werner Zorn of Karlsruhe University in Germany, a working group led by Professor Wang Yunfeng and Doctor Li Chengjiong built up an Email node in ICA, and successfully sent out an Email to Germany on Sep 20th. The Email title was "Across the Great Wall we can reach every corner in the world."

2. From November 9th to 11th, 1987, a Chinese delegation was invited to participate in the sixth International Academic Networkshop held in Princeton, U.S. During the conference, the local organizer forwarded congratulatory letter of the National Science Foundation (NSF) to Chinese representative - Mr. Yang Chuquan, welcoming the extension of BITNET and CSNET electronic mail to China.

3. In early 1988, China's first X.25 PAC – CNPAC has been established. Major cities including Beijing, Shanghai, Guangzhou, Shenyang, Xi’an, Wuhan, Chengdu, Nanjing, and Shenzhen had been covered.

http://www.cnnic.cn/en/index/0O/06/index.htm
4. In March 1988, the China Academic Net (CANET) project was launched with the objective of organizing universities and research institutes to connect their vast computers to the global computer networks.

5. In July, 1988, through satellite lines of Radio Austria, the Institute of High Energy Physics of Chinese Academy of Sciences adopted X.25 protocol, making a VAX785 computer as one of descendant nodes of European Organization for Nuclear Research (CERN) in Geneva, Switzerland.

6. In December 1988, the college network of Tsinghua University was connected to Canada's University of British Columbia (UBC) through X.25 network and initiated the E-mail applications by adopting X400 protocol E-mail software pack, which was introduced by Professor Hu Daoyuan from UBC.

7. In May 1989, the Chinese Research Network (CRN) was connected to the German Research Network through the pilot X.25 net. Members of CRN include: the No. 15 Institute of Electronic Science of the Ministry of Electronic (located in Beijing), the No. 30 Institute of the Ministry of Electronic (located in Chengdu), the No. 54 Institute of the Ministry of Electronic (located in Shijiazhuang), Fudan University, Shanghai Jiao Tong University (located in Shanghai) and Southeast University (located in Nanjing), etc. Services that CRN can provide include Email (X.400 [MHS] standard), file transmission (FTAM standard), catalogue (X.500 standard) and so on. People may also access the Internet through the gateway of DFN in Germany.
8. In October 1989, one of credit projects of the World Bank -- the Demonstration Network for Education and Scientific Research in Zhongguancun Area (named by the State Development Planning Commission), or National Computing and Networking Facility of China (NCFC, named by the World Bank) prepared for initiation. It was then formally launched in November. NCFC is a high-tech information infrastructure project of the "Key Subject Development Project" of the World Bank, and was invested and supported by the State Development Planning Commission, CAS, the National Natural Science Funds and the State Development Planning Commission. The project was charged by CAS, and was jointly implemented by Peking University and Tsinghua University. The chief goal of the project was to consummate the construction of the NCFC backbone network and the college networks through technical cooperation with Peking University, Tsinghua University and CAS.

9. On November 28th, 1990, with Professor Wang Yunfeng and Professor Werner Zorn's efforts, the registration of China's country code top-level domain - .CN was completed with Mr. Qian Tianbai as the administrative contact. From then on, China has its own Internet identity. Since China had not yet achieved full functional connection to the Internet at the time, the .CN ccTLD name server was temporarily set in Karlsruhe University in Germany.

11. In June 1992, '92 INET Conference held in Kobe, Japan. Prof. Qian Hualin made an appointment with the principal of International Network Department; National Sciences Foundation discussed the issue of official connection between China and the Internet. However, he was informed there were political obstacles since so many U.S. governments had connected to the Internet.

12. In later December 1992, Tsinghua University Network (TUNET) was set up and went into service. TUNET is the first college network that adopts TCP/IP structure in China. The backbone was successfully adopted FDDI technique for the first time, which leaded many aspects within China such as the scale, the technique level and the application of networks.

13. In later 1992, the College Network (i.e., CASNET, which connects over 30 research institutes in Zhong Guan Cun area and CAS headquarter in San Li He) of Project NCFC, TUNET (Tsinghua University Net) and PUNET (Peking University Net) completed the construction.

14. On March 2nd, 1993, a 64KDECnet fixed line to the Stanford Linear Accelerator Center (SLAC) was officially opened. Built by the Institute of High Energy Physics of Chinese Academy of Sciences, the fixed line was operated by renting international satellite channels of AT&T. With great support from the National Natural Science Foundation of China, Principals of key research projects in various subjects were enabled to use this fixed line through dial-up connections. An Email system was available to hundreds of domestic scientists.
15. On March 12, 1993, deputy premier Zhu Rongji proposed and deployed the establishment of National Public Economic Information Network (i.e., Golden Bridge Project).

16. In April 1993, Computer Network Information Center, Chinese Academy of Sciences called part of Network specialists in Beijing to investigate the domain name systems of each country, then framed the domain name system of China.

17. In June 1993, experts of NCFC reiterated China's requests for being connected to the Internet at the '93 INET Conference, and discussed such issue with the global Internet communities. After the meeting, researcher Qian Hualin attended the CCIRN (Coordinating Committee for Intercontinental Research Networking) Meeting, and won the support of majority participants in favor of bringing the Internet connection to China. The conference gave a great boost to China's connection to the Internet.

18. On August 27, 1993, Premier Li Peng approved to use the Premier Reserve of 3 million USD to support the Golden Bridge Project in initiating its prophase construction.

19. On December 10, 1993, the National Joint Conference on Economy Informatinalizing had been formed. Zou Jiahua, the deputy Premier of the State Council was appointed the chair.
20. In December 1993, the backbone network construction of NCFC was accomplished. It connected three universities by high-speed optic cable and routers.

21. In early April 1994, the Sino-American Federation of Scientific and Technological Cooperation Committee held meeting in Washington. Before the meeting, on behalf of China, the academician Hu Qiheng, the vice-president of the Chinese Academy of Sciences reiterated to the National Science Fund (NSF) the request of China’s Internet connection. The proposal was approved.

22. On April 20, 1994, the NCFC project opened a 64K international dedicated line to the Internet through Sprint Co. Ltd of the United States, which achieved its full-functional connection to the Internet. Since then, China has been officially recognized as a country with full functional Internet accessibility. It was elected one of China's top 10 scientific and technological events in 1994 by the Chinese press community and designated as one of China's key scientific and technological achievements in 1994 by the State Statistical Communiqué.

23. On May 15, 1994, the High-Energy Physics Research Institute, CAS set up China's first web server and made the first set of web pages. Apart from briefing on the development of high technology in China, there was another column called "Tour in China". Since then, the column expanded its range to the information about news, economies, culture and business and provided essays together with pictures and renamed "Windows of China" afterward.
24. On May 21, 1994, with the assistance of Professor Qian Tianbai and Karlsruhe University (Germany), the computer network information center, CAS finished setting up the China's top domain name (CN) servers, which ended the history of location abroad of CN servers. Qian Tianbai and Qian Hualin are nominated managing contactor and technical contactor respectively.

25. In May 1994, the National Research Center for Intelligent Computing System opened the first BBS in Chinese mainland – Dawn BBS.

26. On June 8, 1994, general office of the State Council issued "General Office of the State Council's Notice on the Related Issues of 'Three Golden Projects' ". From this day on, the prophase construction of the Golden Bridge Project was entirely carried out.

27. On June 28, 1994, with help of Tokyo University of Sciences, Beijing University of Chemical Technology began the pilot run of the leased line connecting with the Internet.

28. In earlier July 1994, the six-college-established (mainly by Tsinghua University) trial network "China Education and Research Network" began to operate. By using IP/x.25 technique, it became a TCP/IP based computer network that connected Beijing, Shanghai, Guangzhou, Nanjing and Xi'an, and also connected with the Internet through the international port of NCFC.
29. In August 1994, the project of China Education and Research Network (CERNET) was officially set. It was invested by the State Development Planning Commission and charged by the State Development Planning Commission, and aimed at connecting college computers and share the resources by using advanced computer and network communication technologies. Further more, it planed to connect with international learning networks, and establish a full functional administrative network system.

30. In September 1994, Directorate General of Telecommunications P & T and the Department of Commerce of United States signed an agreement on the Internet connection. In the agreement, the Office of Telecommunication should open two 64K leased lines (one was in Beijing, another was in Shanghai) with the assistance of the Sprint Corporation in America. It marked the start-up of the CHINANET.

31. In November 1994, the Administrative Commission of NCFC hosted the annual meeting of Asia-Pacific Networking Group (APNG) in Tsinghua University with assistance of CAS, Peking University and Tsinghua University. It was the first International annual meeting of Internet community in Asia-Pacific region held in China.

32. In January 1995, Directorate General of Telecommunications P & T, China Telecom opened Beijing and Shanghai 64K leased lines to the United States with help of Sprint Co. Ltd. It began to provide Internet accessing services through telephone networks, DDN leased lines and X.25 networks.
33. In January 1995, "Chueng Kong Scholars" (Chisacm), the journal published by Ministry of Education (State Educational Committee) was put onto the Internet through CERNET, focusing on providing information to the students abroad. It was the first Chinese E-journal in China.

34. In March 1995, CAS completed the long-distance connection to its four branch institutions in Shanghai, Hefei, Wuhan and Nanjing with IP/X.25 technology. It is the first step that China began to spread the Internet connection to the whole nation.

35. In March 1995, Professor Li Xing from Tsinghua University was elected the Executive Committee member of the Asia-pacific Network Information Center (APNIC) for the first time.

36. In April 1995, Chinese Academy of Sciences (CAS) launched the project of connecting its institutes that out side Beijing (known as "100 CAS Institutes Connection Project"). The objective of the project was to expand the institute network (connected over 30 institutes of CAS in Beijing) to 24 cities all over the country, in order to realize the fully connection of all domestic learning institutions and the connection with the Internet. Based on this project, the network expanded continuously, and gradually connected with many scientific academies and researching outside CAS. It became a scientific oriented national network, serving scientific users, research branches and relevant governmental departments. Its name was also changed into “China Science and Technology Network”(CSTNet).
37. In May 1995, the China Telecom began to prepare for building up the national backbone network for CHINANET.

38. In July 1995, China's first 128K leased line that connects to the United States was opened by CERNET; meanwhile, CERNET also opened DDN channels for its backbone network, connecting with eight cities - Beijing, Shanghai, Guangzhou, Nanjing, Shenyang, Xi’an, Wuhan and Chengdu. The connecting speed was 64Kbps. The NCFC connection was also achieved.

39. In August 1995, the primary phase of "Golden Bridge Project" was accomplished. It achieved the connection (through satellite network) with 24 provinces and cities all over the country, and it further connected with the Internet.

40. In December 1995, "100 CAS institutes connection project" was accomplished.

41. In December 1995, "CERNET demonstrate project" was accomplished. This project was designed and constructed wholly by Chinese engineers.

42. In January 1996, the Informatization Leading Group of the State Council and its executive office were established. Zou Jiahua, the deputy premier of the State Council leaded the group. The former office of National Economic Informatization Joint Meeting was renamed the office of Informatization Promotion Leading Group of the State Council.
43. In January 1996, CHINANET backbone network completed its construction and began to provide network services throughout the country.


45. On February 27, 1996, China International E-Commerce Center of China International Electronic Commerce Center was formally established.

46. In March 1996, Tsinghua University proposed "the Unified Transmission Standard for Chinese Character Coding Adept in Different Countries" to IETF and was approved as RFC1922. It was the first Chinese proposal being approved as RFC document.

47. On April 9, 1996, the Ministry of Posts and Telecommunications issued "Rules for Administration of China's Public Computer Networks and International Connection", and effective as of the same day.

48. On June 3, 1996, the Electronics Industry Administration published "The Relevant Decisions on Administering the International Connection of Computer Information Networks". In the document, "China GBN" was renamed "China Golden Bridge Information Network". It also accredited Jitong Communication Co. Ltd the
inter-connecting organization of China Golden Bridge Information Network, which was responsible for managing the connection of inner organizations and users.

49. In July 1996, the Information Office of The State Council called specialists from relative institutions to investigate the current technique implemental and administrative situations of 4 major Networks and nearly 30 ISPs in China. The investigation facilitated the standardization of network administration.

50. On September 6, 1996, the China Golden Bridge Network (China GBN) opened a 256K leased line connected to the United States. China GBN also announced the decision to provide Internet access service, mainly for institutional users through dedicated lines and individual users through telephone lines.

51. On September 22, 1996, the first domestic City Area Network (CAN) - Shanghai Hotline started its test run, which marked the accomplishment of the Shanghai Public Information Network – the main structure of Shanghai information port project.

52. In September 1996, the State Development Planning Commission formally approved starting the first stage project of “the Golden Bridge”.

53. On November 15, 1996, the Shihuakai Corporation built up the Shihuakai Internet Café besides the capital gymnasium; it was the first Internet café in China.

54. In November 1996, CERNET opened the 2M international line connected to
U.S. In the same month, during the German president's visiting, CERNET opened the learned network between China and Germany – CERNET-DFN, which is the first Internet connection to Europe from Chinese mainland.

55. In December 1996, the China Public Multimedia Communication Network, known as Net 169 began its operation. As preliminary group of connected web sites, Guangdong Shilingtong, Tianfu Hotline and Shanghai Online had officially opened.

56. On January 1, 1997, People’s Daily Online (directed by People’s Daily) connected to the Internet. This is the first key news website of central government.

57. In February 1997, the Info-Highway Network began its operation. In three months, it achieved the connection of eight cities including Beijing, Shanghai, Guangzhou, Fuzhou, Shenzhen, Xi’an, Shenyang and Haerbin. It became the earliest and largest private ISP/ICP.

58. From April 18 to 21, 1997, The State Council held National Informatization Workshop in Shenzhen and finalized the definition, elements, guidelines, working principles, objectives and chief missions of the national informatization mechanism. The workshop also approved “the 9th five-year planning” and “2000 long-range objective”. Chinese Internet project was listed on the construction agenda of the State Information Infrastructure. The workshop also proposed to set up national network information center and Internet exchange center.

59. On May 20, 1997, the State Council promulgated “the State Council's Decision on
Revising the Provisional Regulations of the People's Republic of China on Managing Computer Internet Information Networks”. It amended “the Provisional Regulations of the People's Republic of China on Managing Computer Internet Information Networks”.

60. On May 30, 1997, the Informatization Leading Group Office of the State Council issued “Interim Policies on the Administration of Internet Domain Names in China”. It then accredited CAS as the institute for founding and administering China Internet Network Information Center (CNNIC), while gave the authorization to the center of CERNET for managing “.edu.cn” through a contract with CNNIC.

61. On May 31, 1997, Beijing University of Chemical Technology cut off the satellite leased line and connected to the China Education and Research Network (CERNET).

62. On June 3, 1997, entrusted by the Office of Informatization Promotion Leading Group of State Council, CAS set up China Internet Network Information Center (CNNIC) in its Computer Network Information Center. CNNIC operates as the national Internet information center. On the same day, the Office of Informatization Promotion Leading Group of State Council announced the formation of CNNIC Steering Committee.

63. In October 1997, China's first national Internet backbone (ChinaNet) realized the connection with other three backbone networks -- China Science and Technology Network (CSTNET), China Education and Research Network (CERNET) and China Golden Bridge Network (CHINAGBN).
64. In November 1997, CNNIC published the first “Statistical Report on Internet Development in China”. By October 31, 1997, there were 299,000 computer hosts and 620,000 Internet users in China; 4,066 domain names were registered under .CN. China had about 1,500 WWW web sites and 25.408M of the international bandwidth.


67. In March of 1998, the first meeting of the 9th National People’s Congress gave approval of the establishment of the Ministry of Information Industry (MII). The major task for MII is to administrate the national manufacturing of IT products, national communication and software industries, facilitating the informatization of the national economy and social services.

68. In May 1998, the project of constructing China Great Wall Network was approved by central government.

69. In June 1998, CERNET formally participated in the trail network of the next
70. In July 1998, China Information Technology Security Certification Center (CNITSEC) initiated its trial operation after obtaining the acceptance of the Informatization Leading Group office of the State Council.

71. In July 1998, CHINANET launched the second-phase project of its backbone network construction. This would expand the backbone bandwidth in its major 8 regions into 155M; all the node routers in these regions will be upgraded to kilo-mega bit routers.

72. In August 1998, the MPS officially formed the Public Information Network Security Supervision Bureau. It takes the responsibility of maintaining computer network securities, striking against crime in cyberspace, supervising the security protection of computer information systems.

73. On January 22, 1999, leaded by China Telecom and the Economic Information Center of the State Economic and Trade Commission, over 40 relevant government departments (offices and bureaus) hosted the Conference for Launching the E-Government Project of P.R. China in Beijing. www.gov.cn, the primary website of the project initiated its trial operation.

74. In January 1999, CNNIC published “the Third Statistic Report on the Development of Internet in China”. By December 31, 1998, there were 747,000 computer hosts and 2.1 million Internet users in China; 18,396 domain names were registered under .CN. China
had about 5,300 WWW web sites and 143.256Mbit/s of international bandwidth.

75. In January 1999, CERNET opened all its satellite backbone networks, which enormously increased the transmission speed. In the same month, China Science and Technology Network (CSTNET) launched two sets of satellite systems, which replaced IP/X.25, and connected with more than 40 cities all over the country.

76. On February 3, 1999, “the Certification System of Electronic Business Information Security” – one of the Key Technological R&D Programs of China’s 9th five-year planning (powered by China International E-Commerce Center) passed the technical achievement appraisal by the Ministry of Science and Technology and the National Passcode Administrative Commission. It also obtained the license for selling information security products from relevant departments, and became the first purely self-developed and copyright self-owned CA security certification system for E-commerce. This system was successful in administrating the quota licenses of domestic textile.

77. In February 1999, China National Information Security Testing Evaluation & Certification Center (CNISTEC) was established.

78. On April 15, 1999, 23 influential presses of domestic websites gathered together for the first time to discuss the development of the press media of Chinese websites. “Chinese Journalistic Circles Network Media Joint Pledge” was approved in principle. The participants called on the recognition and protection of the information property on the Internet.
79. In May 1999, CCERT (CERNET Computer Emergency Response Team) was formed in the Network Engineering Research Center of Tsinghua University. It is the first organization for dealing with network emergencies in China.

80. On July 12, 1999, ChinaNet went public on Nasdaq. This is the first Chinese conceptual stock of network company in Nasdaq.

81. In August 1999, over 200 colleges in 6 provinces used “All-China College Students Recruiting System” on CERNET, and achieved the first success.

82. On September 6, 1999, China International Electronic Commerce Exhibition (E-COMMERCE Expo’99) was held in Beijing. The exhibition was hosted by the Ministry of Foreign Trade and Economic Cooperation and the Ministry of Information Industry (MII). For the first time, Chinese government hosted an E-commerce exhibition, and for the first time, China held such a fruitful conference that demonstrated so many E-business technologies and applicable resolutions.

83. In September 1999, China Merchants Bank took the lead in providing the online banking service called “All in One Net”, establishing the online service system that was composed mainly by enterprise/individual oriented bank, online payment, online negotiable securities and online shopping. Approved by the People’s Bank of China on conducting personal banking business, China Merchants Bank became the first online commercial bank in China.
84. In October 1999, Mr. Wu Jianping, a professor of Tsinghua University was nominated the member of Address Supporting Organization (ASO) of the Internet Corporation of Assigned Names and Numbers (ICANN).

85. On November 2, 1999, Mr. Chen Yin, the deputy director general of Telecom Administrative Bureau of MII attended ICANN Governmental Advisory Committee (GAC) Meeting.

86. On December 23, 1999, the State Informatization Steering Group came into existence, Wu Bangguo, the Vise Premier of the State Council chaired the group. The former State Office of Informatization was renamed the State Office of Informatization Promotion.

87. On January 1, 2000, “Regulations for the Protection of National Computer Networks” was promulgated by National Administration for the Protection of State Secrets, and was put into force on the same day.

88. On January 17, 2000, the Ministry of Information Industry (MII) approved “China International Economy and Trade Net” (CIETNet) project which would be conducted by China International E-Commerce Center.

89. On January 18, 2000, China Internet Network Information Center (CNNIC) published the fifth “Statistical Report on Internet Development in China”. By the end of December 31, 1999, there were 3.5 million computer hosts and 8.9 million Internet users in China.
48695 names were registered under .CN, and China had about 15153 WWW websites and 351Mbit/s of the international bandwidth.

90. On January 18, 2000, accredited by MII, China Internet Network Information Center (CNNIC) launched the trial system of Chinese domain name.

91. On March 30, 2000, a national Internet exchange center started operation in Beijing, which increased the inter-connection bandwidth of domestic backbone networks from less than 10Mbit/s to 100Mbit/s.


93. On May 17, 2000, China Mobile Network (CMNET) was put into operation. On the same day, China Mobile Co. formally initiated the “Global link WAP” Service.

94. On May 20, 2000, Chinese Domain Name Consortium (CDNC) was founded in Beijing. It takes the responsibility of harmonizing and regulating the development of Chinese domain name at a nongovernmental level.

95. On June 21, 2000, China Electronic Commerce Association was formally established. It aimed at strengthening the cooperation and communication among China and overseas in the field of E-commerce.
96. On July 1, 2000, being authorized by the State Council, the State Development Planning Commission designated http://www.chinabidding.gov.cn the sole network media that was entitled to publish government bidding announcement.

97. On July 7, 2000, directed by the State Economic and Trade Commission and MII, China Telecom Group and the State Economic and the Economic Information Center of the Trade Commission jointly launched “the project of enterprise accessing the Internet”.

98. On July 18, 2000, Qian Hualin, the research fellow of the Computer Network Information Center, CAS, was elected the chair of Asia-Pacific Top Level Domains (APTLD) and won all the ballots.

99. On July 19, 2000, China Unicom Public Computer Internet (UNINET) was officially opened.

100. In July 2000, Dr. Gao Lulin, the former director general of the State Information Property Bureau participated in the ICANN at-large board election. He was nominated as one of the candidates on August 1.

101. On August 21, 2000, World Computer Congress 2000 was held in Beijing International Conference Center. President Jiang Zemin gave an important lecture in the conference, he stressed the necessity of setting up the Internet pact, and also called on people to strengthen the administration of information security, and make full use of the Internet.
102. On September 25, 2000, the State Council issued “The Telecommunication Regulation of the People’s Republic of China”. This is the first integrated regulation for administering the industry of telecommunication in China, which marked the development of China’s telecommunication industry had marched into the legal system track. On the same day, the State Council implemented “Rules for Administering the Internet Information Services”.

103. In September 2000, Tsinghua University finished constructing DRAGONTAP, the first domestic exchange center of the next generation Internet. Through DRAGONTAP, the three domestic backbone networks (CERNET, CSTNET, and NSFCNET) were connected to STARTAP, an American exchange center of the next generation Internet located in Chicago, and an exchange center of Asia Pacific Advanced Network (APAN) in Tokyo, Japan. The connecting speed of the two lines was 10Mbps. The project built up the connection of many scientific networks such as Abilene, vBNS and CA*net3l, it also achieved the connection of the next generation Internet through out the world.

104. In September 2000, CERNIC, the information service center of CERNET took the lead in providing IPv6 assignment service in China.

105. On October 11, 2000, the 5th Plenary Session of the 15th Central Committee of Communist Party of China made a momentous decision in achieving the informatization. The plenary meeting reviewed and approved “Suggestions on Programming the 10th five-year plan on National Economy and Social Development by the Central Committee
of Communist Party of China”, which indicated “the promotion of national economy and social informatization is a strategic action which would be adopted along with achieving the modernization of socialism. Drive industrialization through informatization, make better use of their advantages as late starters and attain progress on social productivity by leaps and bounds.

106. On November 1, 2000, China Internet Network Information Center (CNNIC) published “Trial Measures for the Administration of the Registration of Chinese Domain Names” and “Trial Dispute Resolution Policy of Chinese Domain Names”. CNNIC also entrusted the Chinese domain name dispute resolution institution to China International Economy and Trade Arbitration Center (CIETAC).

107. On November 6, 2000, the State Council News Office, the Ministry of Information Industry (MII) issued “Interim Regulations for the Administration of Publishing News Materials on Websites”.

108. On November 6, 2000, the Ministry of Information Industry (MII) issued “Regulations for the Administration of the Internet Electronic Bulletin Services”.

109. On November 7, 2000, the Ministry of Information Industry (MII) issued “Announcement on Administering Chinese Domain Names”. In this document, MII standardized the registration services and administrations of Chinese domain names, and specifically accredited the Chinese domain name registry to CNNIC.
110. On November 7, 2000, China Internet Network Information Center (CNNIC) upgraded the Chinese Domain Name system, and initiated the registration services of Chinese domain names under “.CN”, “.China (in Chinese)”, “.Corporation (in Chinese)” and “.Network (in Chinese)”.

111. On November 10, 2000, China Mobile presented “Monternet Program”. By this means, it intended to found an open, cooperative and mutual beneficial chain of industrial value.

112. On December 7, 2000, initiated by the Ministry of Culture, the Central Committee of Communist Youth League, the State Administration of Radio Film and Television, National Students' Federation, the State Office of Informatization Promotion, Guangming Daily, China Telecom and China Mobile, “the Internet Manners and Culture Project” was launched in Beijing. “Civilized website accessing, civilized network establishment and civilized Internet environment” was the theme of the project.

113. On December 12, 2000, People’s Daily, XinhuaNet, ChinaNet, CCTV International Website, International Online Website, China Daily and CYCNET obtained the approval form the State Council News Office for press publication, and became the preliminary group of press websites that obtained official authorization.

114. On December 28, 2000, members of the Standing Committee of the 9th National People's Congress voted and approved “the Standing Committee of CPC’s Decision on Protecting the Internet Security” on their 19th session.
115. On January 1, 2001, the Internet project of “Every School Access the Network” entered the phase of formal implementation.

116. On January 11, 2001, the State Food and Drug Administration issued “Interim Regulations for the Administration of Internet Medicine Information Services”. It was implemented on February 1, 2001.

117. On January 17, 2001, China Internet Network Information Center (CNNIC) published “the 7th Statistical Report on the Development of the Internet in China”. By the end of December 31, 2000, there were approximately 8.92 million computer hosts in China, about 22.5 million Internet users. 122,099 domain names were registered under .CN. China had approximately 265,405 WWW websites, and 2,799Mbit/s of international bandwidth.

118. In early February 2001, China Telecom began to provide the service of International Roaming on the Internet.

119. On March 2, 2001, research fellow Qian Hualin and professor Li Xing of Tsinghua University were elected members of the Executive Committee of APNIC.

120. On April 3, 2001, the Ministry of Information Industry (MII), The Ministry of Public Security, the Ministry of Culture and the State Administration For Industry & Commerce jointly promulgated “Measures for the Management of Internet Cafés”, and
put it into effect as of the same day.

121. On April 13, 2001, the Ministry of Information Industry (MII), The Ministry of Public Security, the Ministry of Culture and the State Administration for Industry & Commerce started the special Rectification of “Internet Cafe”.

122. In April 2001, Professor Li Xing from Tsinghua University was elected the new chair of the Asia Pacific Network Group (APNG) Executive Committee.

123. On May 25, 2001, the Internet Society of China (ISC) was founded with the approval of the Ministry of Civil Affairs. It was established under the direction of the Ministry of Information Industry (MII), and was formed by over 70 relevant organizations, including domestic ISPs, ICPs, facility manufacturers, system integration business, academies and educational institutions.

124. In May 2001, approving by the Central Establishment Committee, China National Information Security Testing Evaluation and Certification Center was founded. The main task of the organization was to examine and confer state certifications on information security products, information system security, information security services and information security professionals.

125. On June 1, 2001, leading by the Customs General Administration of the People’s Republic of China, the port law enforcement system that was developed by 12 relevant ministries and commissions finished its trial operation in Beijing, Tianjin, Shanghai, and
Guangzhou. Thereafter China’s “Electronic Port” became functional all over domestic ports.

126. In July 2001, “NSFCNET” (a high-speed Internet, the biggest project invested so far by the Natural Science Foundation of China, 1999-2000), a momentous joint project of the national natural fund that was undertaken by Tsinghua University, Computer Network Information Center of CAS, Peking University, Beijing University of Posts and Telecommunications, Beijing Beihang University passed acceptance check, and established the first learning network of the next generation Internet in China. The contents include general design of China’s experimental network of the high speed Internet; density wave minute multiplexing optical fiber transmission system; high-speed computer network and key researches on applications and demo systems in the environment of high-speed networks.

127. On July 9, 2001, the Bank of China promulgated “The Interim Rules for the Administration of Online Banking Business”.

128. On July 11, 2001, the CPC held a lecture on legal affairs in Zhongnanhai Huairentang, with the theme of protecting and facilitating the sound development of information on the Internet by legal means. Jiang Zemin, the secretary general of the CPC chaired the lecture, and emphasized that China shall catch hold of opportunities, expedite the development of information and network technologies, and apply it to practice in economy, society, technology, national defense, education, culture and law.
129. On July 29, 2001, the Ministry of Information Industry (MII) announced the Structure Guideline of National Informatization, which became the warranty and measure for analyzing and quantizing the current level of informatization.

130. In July 2001, “the Key Informatization Program of 10th five-year plan on National Economy and Social Development” was promulgated.

131. On August 23, 2001, the State Informatization Leading Group was reestablished. Premier Zhu Rongji chaired the group.

132. In August 2001, the National Computer Network and Information Security Administration Center established the national “Computer Network Emergency Response Technical Team / Coordination Center of China” (CNCERT/CC).

133. On September 7, 2001, “The Program for the 10th Five-Year-Planning of Information Industry” was issued. This is the first industry program after establishing the strategy of informatization by the government.

134. On September 7, 2001, the State Office of Informatization Promotion published “the Survey Report on Quantity of Information Resources of the Internet in China”, the survey was entrusted by the State Office of Informatization Promotion, and jointly conducted by China Internet Network Information Center (CNNIC), China Electronic Information Industry Development Research Institute and Nanjing Researching Base of the National Information Resources Administration. This is the first domestic survey aiming at the
information resources on the Internet. By the end of April 30, 2001, China had 692,490 domain names, 238,249 websites, 159,460,056 web pages and 45,598 online databases.

135. On September 20 2001, the Ministry of Information Industry (MII) issued “Measures for Inter Accounting among Internet Backbone Networks”.

136. On September 29 2001, the Ministry of Information Industry (MII) issued “Interim Regulations for Connecting Services of the Internet Backbone Networks”.

137. On October 8, 2001, the Ministry of Information Industry (MII) published “The Interim Regulation for the Management of the Connection of Backbone Networks”.

138. On October 27, 2001, after the 24th session of the Standing Committee of the 9th National People's Congress, “the Information Network Dissemination Right” was formally included in the revised version of “The Copyright Law of People's Republic of China”. Relevant regulations would protect copyrights by legal means in the environment of Internet spreading.

139. On November 4, 2001, China Internet Network Information Center (CNNIC) began to provide the service of Internet Keyword.

140. On November 20, 2001, the demonstration project of Chinese electron government affairs application was approved by the relevant departments, which marked a momentous advancement of China’s “E-government”.
141. On November 22, 2001, the Central Committee of Communist Youth League, the Ministry of Education, the Ministry of Culture, the State Council News Office, All China Youth Federation, National Students' Federation, the National Working Committee on Young Pioneer and China Youth Network Association jointly presented “the Civilized Internet Pact of All Country Teenagers”, a set of criteria for millions of domestic teenagers to regulate their behaviors when using the Internet.

142. In November 2001, Academician Hu Qiheng, the vice Chair of Chinese Association of Science, the director general of CNNIC Steering Committee was appointed as the member of ICANN Internationalized Domain Name (IDN) Committee.

143. On December 3, 2001, China Internet Network Information Center (CNNIC) published the first “The Survey Report on the Internet Bandwidth in China”. By the end of September 30, 2001, the international bandwidth in China reached 5724M.

144. On December 20, 2001, “The Project of Families Access the Internet” was formally initiated. The project was led and directed by the Ministry of Information Industry (MII), the National Women's Federation, the Central Committee of Communist Youth League, the Ministry of Science and Technology and the Ministry of Culture.

145. On December 20, 2001, the Telecommunication Administration Bureau of MII promulgated “Regulations for Financial Accounting of the National Internet Exchange Center”.

146. On December 20, 2001, the 10 domestic backbone networks signed the interconnection agreement, which implied more convenient accessing of the Internet by users in different regions.

147. On December 22, 2001, China Unicom announced in Beijing that the first-phase project of China Unicom CDMA mobile telecommunication network had accomplished on time, and started its operation since December 31, 2001 in 31 provinces, municipalities and cities. The building up of China Unicom’s CDMA network indicated that the telecommunication technology of China Mobile had stepped into a new era.

148. On December 25, 2001, Premier Zhu Rongji, Chair of the State Informatization Leading Group (SILG) moderated the first SILG meeting. As Premier Zhu pointed out, the construction of China’s informatization should be pushed forward by attaching greater importance to unified planning, persisting with marketing, and preventing repeated construction of a same project.

149. At the end of December 2001, “China Education and Research Network CERNET”, a high-speed backbone network project (1999—2001) was obtained its qualification from the government. The project was a main element of “the modern remote education project” in “the national education promotion plan of 21st century”, and also the important base for constructing the lifelong education system in China. Based on DWDM/SDH, the project finished building the high-speed transmitting network with a capacity of 40Gbps and backbone transmit rate of 2.5Gbps. Except for Lhasa in Tibet,
CERNET connected with other 35 provinces and central cities at speed of 55Mbps. Nearly 100 colleges were connected at speed of 100~1000Mbps. Based on CERNET, the Ministry of Education had approved 47 colleges’ setting up network educational institutes (later enlarged to 67 colleges), and also allowed 19 online cooperative research centers to carry out remote education and scientific research through CERNET.

150. On December 31, 2001, the National Internet Exchange Centers began their operation in Shanghai and Guangdong respectively.

151. On January 15, 2002, China Internet Network Information Center (CNNIC) published the 9th “Statistical Report on the Development of Internet in China”. By the end of December 31, 2001, there were about 125.4 million computer hosts and 33.7 million Internet users in China. 127,319 domain names were registered under .CN. China had over 277,100 WWW websites and 7597.5M of international bandwidth.

152. On March 14, 2002, the Ministry of Information Industry (MII) approved “Rules for the Administration of Internet Domain Names in China” in its 9th session. The regulation was put in force on September 30, 2002.

153. On March 26, 2002, the Internet Society of China (ISC) issued “Self-Discipline Treaty of Internet Industry in China” in Beijing, establishing the foundation of domestic self-discipline mechanism.

154. On May 17, 2002, the Ministry of Culture issued “Notification on Strengthen the
155. On May 17, 2002, China Telecom made a start on “China Vnet” plan in Guangzhou, which indicated the alliance of ISPs and ICPs in building the industrial chain on broadband Internet.

156. On May 17, 2002, China Mobile took the lead in providing GPRS services in the whole country. On November 18, Telecommunication Corporation of China Mobile and AT&T jointly announced the starting of the GPRS International Roaming Service between the two companies.

157. On June 27, 2002, the State Administration of Press and Publication and the Ministry of Information Industry (MII) jointly issued “Interim Regulations for the Administration of the Internet Publications”. The regulation was formally put into force on August 1, 2002.

158. On July 3, 2002, the State Informatization Leading Group hosted its second meeting. During the meeting, three documents were approved, i.e., “Informatization – the Key Program in the 10th five-year plan on National Economy and Social Development”, “Guiding Suggestions on Constructing China’s E-government” and “Proceeding Program on Promoting Software Industry”.

159. On September 25, 2002, China Internet Network Information Center (CNNIC) issued “Detailed Rules for the Registration of Domain Names”, “Domain Name Dispute
Resolution Policy” and “Rules for Accrediting Domain Name Registrars”.


161. On September 30, 2002, “Rules for the Administration of Internet Domain Names in China” was put into force.

162. From October 26 to 31, 2002, the Internet Corporation of Assigned Names and Numbers (ICANN) held its meetings in Shanghai. This was the first ICANN meeting in China. The conference was hosted by China Internet Network Information Center (CNNIC) and the Internet Society of China (ISC).

163. On November 1, 2002, ISC formed the Counter-junk mail coordinated group in Beijing with assistance of 263 Group and Sina.com. The main task of the working group is to protect the proper benefits of Internet users and E-mail service providers in China, fairly use the Internet resources and regulate domestic E-mail service system.

164. On November 22, 2002, the Ministry of Information Industry (MII) issued “The Bulletin about Internet Domain Name System in China”.

165. On November 25, 2002, approving by the Ministry of Information Industry (MII), the first Internet Conference and Exhibition of China was held in Shanghai with the
Internet Society of China as the host. The conference mainly discussed the innovation of the Internet application in China, directing the further development of China’s Internet industry. The theme of the conference was “The application of the Internet – long for innovation”.

166. On December 16, 2002, as a sole registry of .CN, China Internet Network Information Center (CNNIC) transmitted its customer services to the accredited registrars. This is a fundamental innovation in domain name registration service system since the deployment of .CN ccTLD in 1990 in China.

167. On January 16, 2003, China Internet Network Information Center (CNNIC) published the 11th “Statistical Report on the Development of the Internet in China”. By the end of December 31, 2002, there were about 20.83 million computer hosts and 59.10 million Internet users in China; 179 thousand domain names were registered under .CN. China had about 371 thousand WWW websites and 9380M of the international bandwidth.

168. On March 17, 2003, China opened the name space of the second level domain under .CN ccTLD. People now are permitted to register names directly under .CN.

169. On March 20, 2003, a youth from Hubei province named Sun Zhigang was beaten to death in Guangzhou. Online Medias around the nation actively participated in reporting this tragedy and raised high concerns of the society. The Internet demonstrated its great power as a media to voice public opinion. The pressure urged the related authority to
successfully close the case, and pushed the state council developed policy to protect homeless people.

170. On April 9, 2003, China Netcom (CNC) announced in Beijing that it was officially independent from CHINANET of China Telecom, and ceremoniously launched its new service brand – “Broad Band CHINA 169”.

171. On May 10, 2003, the Ministry of Culture issued “Provisional Regulations for Administering Internet Culture”. It took effect on July 1, 2003.

172. On June 5, 2003, the Ministry of Culture issued “the Announcement of the Approval Situation of Nationwide Internet Accessing Chain Store Operators”. 10 organizations were approved to construct nationwide Internet accessing store chain.

173. On June 26, 2003, CAS researcher Qian Hualin, an expert of computer network and data communication, was elected as a member of ICANN board of directors with 3 years’ term. This was the first time for Chinese expert step into the highest decision making group of Internet address resources.

174. On July 9, 2003, the information working office of the State Council issued “Survey Report on China Internet Information Resources” in Beijing. By the end of December 31, 2002, the total number of domain names in China reached 940,300. China had 371,600 websites, 157 million web pages and 82,900 online databases.
175. On August 8, 2003, the first release of “China Internet Development Report” was formally published by ISC and CNNIC in Beijing. It was the first large-scale literature that comprehensively described the development situation of the Internet in China.

176. On August 8, 2003, the “anti-spam coordinate group” of ISC announced the first issue of “Spam Server Name List”, which attracted attentions of all circles of the society.

177. On August 11, the computer virus WORM_MSBlas.tA intruded upon China and infected the majority of domestic Internet users in a few days. The worm virus broke the record and became one of the most serious computer virus.

178. In August 2003, net game player Li Hongchen sued Beijing Arctic Ice Technology Development Co. Ltd, the operator of “Red Moon” net game, for losing his virtual equipments. This was the first net game case, and legally educed the issue of virtual property conception.

179. In August, 2003, the state council authorized to launched the model project of China’s next generation Internet — CNGI (China Next Generation Internet), CNGI was the initiative project for implementing the development strategy of next generation Internet in China. The project was led by eight ministries including National Development and Reform Commission, Ministry of Science and Technology, Ministry of Information Industry, the State Council Informatization Office, Ministry of Education,
Chinese Academy of Science, Chinese Academy of Engineering, and National Natural Science Foundation of China.

180. On September 27, Asia-Pacific Internet Research Alliance (APIRA) was formed in Beijing. The organization was initiated by CNNIC. The initial member organization also included Korea Network Information Center (KRNIC), City University of Hong Kong, University of Macao and Taiwan Network Information Center (TWNIC).

181. On November 18, 2003, the State General Administration of Sport formally approved the E-sports as the 99th national athletic sports.

182. On November 20, 2003, CNNIC published “Survey Report on the Hot Issues of Internet Use”. The report covered the information of website short message and bandwidth. It was the first time for CNNIC, even for the whole nation to publish such kind of survey report. Statistics showed that users averagely send 10.9 short messages through the Internet, while 70.8% of the broadband users use ADSL.

183. On December 6th to 7th, 2003, the second Internet Conference and Exhibition of China was held in Beijing with the Internet Society of China as the host. The theme of the conference was “Seeking the Perspective of Internet, Leaping for the E Era”. Mr. Huang Ju, the deputy premier of the state council sent greetings to the conference.
184. On January 12, 2004, the three nations’ project (China-US-Russia) - “Global Ring Network for Advanced Applications Development” (GLORIAD) was accomplished. GLORIAD was funded and constructed by CAS, the National Science Foundation (US) and Russia Ministry and Science Group Alliance. GLORIAD will support the three countries even the global advanced scientific and educational applications. Computer Network Information Center of CAS, National Supercomputing Application Center of Illinois University and Kolchatov Institute of Russia.

185. On January 15, 2004, CNNIC published the 13th “Statistical Survey Report on the Internet Development of China”. By the end of December 31, 2003, there were approximately 30.89 million computer hosts, 79.50 million Internet users in China; 340,040 names were registered under .CN domain. China had about 595,550 WWW website, and 27,216Mbps of international bandwidth.

186. From February 3 to 18, 2004, Sina, Sohu and Netease successively revealed their financial results in 2003. They reported annual profits of US$114 million, US$89 million and US$80 million respectively in 2003, achieving for the first time full-year profitability of the three firms.

187. On March 4, 2004, Linktone Ltd., a provider of entertainment-oriented wireless value-added services to mobile phone users in China, announced its listing on the
NASDAQ Stock Market in New York. Linktone has become the first firm specialized in SP (Service Provider) in China to have accomplished initial public offering (IPO). Afterwards, Tom Online, Shanda, Tencent, KongZhong Corporate, 51job, China Finance Online, eLong, Hurray! And The9 were successively listed on overseas stock market, indicating the second overseas IPO tide of Chinese Internet firms.


189. On April 14, 2004, IETF formally issued RFC 3743 with the title of “Joint Engineering Team (JET) Guidelines for Internationalized Domain Names (IDN) Registration and Administration for Chinese, Japanese, and Korean”, which was submitted by CNNIC, together with JPNIC and KRNIC. This is the second IETF RFC document participated and instituted by Chinese engineers ever in the history. RFC 3743 is focused on realizing equivalent conversion and transition of different forms (traditional/simplified/variant) of Chinese characters when using as IDN identifiers.

190. Created by the Internet News & Information Service Working Committee (INISWC) of the Internet Society of China, the website of net.china.cn was launched in Beijing on
June 10, 2004. The website was named the “Illegal and Inappropriate Information Report Center”, providing a channel for the public to report suspected illegal or offensive Internet activity and material, and to maintain public interests. The opening of the website is another essential step to strengthen self-discipline and public supervision of the Internet industry.

191. On July 16, 2004, a national teleconference on the crackdown against porn websites was held, marking the launch of a nationwide campaign against porn sites. On the next day, the Publicity Department of the Communist Party of China (CPC) Central Committee and some other 13 governmental organizations jointly published a notice to launch a nationwide crackdown project against pornographic websites according to the laws.

192. On July 21, 2004, the China Next Generation Internet (CNGI) Project Experts Committee was established by National Development and Reform Commission and other seven central government departments.

193. On August 28, 2004, the Law on Electronic Signature was passed on the eleventh meeting of the Standing Committee of the 10th National People's Congress (NPC). The law will take effects on April 1, 2005. The launch of the law was a notable step toward the legislation of informatization in China. It will also greatly facilitate and better ensure
the process of e-government and e-commerce in China.

194. On September 6, 2004, China's Supreme People's Court and Supreme People's Procuratorate jointly issued a new judicial interpretation for criminal cases concerning the production, duplication, publication, sale and dissemination of pornographic material via the Internet, mobile communications terminals and fixed-line telephone networks.

195. New “Measures for Administration of Internet Domain Names of China” were promulgated on November 11, 2004 as Decree No. 30 of the Ministry of Information Industry of the People’s Republic of China. These measures will take effects on December 20, 2004.

196. On November 29, 2004, the Internet Trust and Self-discipline Alliance, co-established by Internet companies Sina, Sohu and Netease, proclaimed self-disciplinary regulations for China's Internet wireless service providers (SPs), representing the continued and serious efforts put into the self-discipline of the Internet wireless SPs in China.

197. On December 23, 2004, the IPv6 address of China's Country Code Top Level Domain (ccTLD) name server was successfully registered in global domain name root
server, marking that the upgraded .CN name server has connected to the IPv6 network
and is capable of providing .CN domain name resolution services for IPv6 environment.
China’s .CN domain name system has进入了 IPv6 Era.

198. On December 25, 2004, one of the first backbone networks of China Next-
Generation Internet (CNGI), CERNET2, was launched and going into formal operation.
199. On December 29, 2004, the Unified Network Platform (UNINET) by China Unicom
won the first prize of the Science and Technology Award offered by China Institute of
Communications. UNINET has realized a network on a unified platform, simultaneously
providing voice, data, video, Internet, video conference, video telephone or CDMA 1X
mobile data services.

Internet Development in China”. By the end of December 31, 2003, there were
approximately 41,600,000 computer hosts and 94,000,000 Internet users in China;
432,077 names were registered under .CN ccTLD. China had about 668,900 WWW
websites, and 74,429 Mbps of international bandwidth. On June 30, Chinese Internet
users broke through 100 million for the first time, attained 103,000,000, broadband users
exceeded half of the Internet users for the first time.

201. On January 28, 2005, the Network Copyright Alliance of Self-Discipline Steering
Committee of the Internet Society of China (ISC) was established in Beijing, the alliance aims at strengthening the self-discipline of the Internet industry, impelling it to healthy and orderly development.

202. On February 8, 2005, Ministry of Information Industry (MII) issued “Administration Rules for Making Files of Non-profit Internet Information Services”. According to the rule, MII jointly with some other 13 Ministries — namely Chinese Central Propaganda Department, the News Office of the State Council, Ministry of Education, MPSand etc., — launched the centralized website for filing projects all over the nation. This project would establish three basic databases of ICP information, IP address information and domain name information for filing information of ICPs, and laying a foundation for strengthening the administration of the Internet.

203. On February 8, 2005, Ministry of Information Industry (MII) issued “Administrative Rules for Electronic Authentication Services”. It was implemented simultaneously with “Electronic Signature Law”, and laid the foundation for the development of China’s electronic authentication service industry.

204. At the end of April, 2005, Shanghai Television Station, subordinated to Shanghai Media Group (SMG) obtained the approval from The State Administration of Radio Film and Television (SARFT) to broadcast audio and video programs to TV sets and portable facilities over IP networks. It was the first IPTV license that the SARFT had issued.
205. On August 5, 2005, BaiDu Co.Ltd went IPO on NASDAQ. With the original offering price at USD 27 per share, in the first transaction day, it had a gap at USD 66 then peaked to USD 151.21, and closed at USD 122.54. It recorded the highest first day growth rate of 354% among all IPOs on NASDAQ since the year of the Internet Bubble in year 2000.

206. On August 11, 2005, Yahoo China announced to exchange 40% of Alibaba.com’s stock and 35% of the voting rights for 1 billion US dollars and all its assets, and transferred all business operations of Yahoo China to Alibaba.com. This was the first case for a global Internet giant giving all of its China’s business to a local company.

207. On September 11, 2005, the News Office of the State Council and Ministry of Information Industry jointly issued “Regulations for Administering the Internet News and Information Services” and the regulation came into effect on the same day.

208. On November 7, 2005, Beijing Olympic Organizing Committee announced that Sohu.com became the Internet content service sponsor of Beijing 2008 Olympic Games. For the first time, the Internet content service is set to be one of the sponsored items in the history of Olympic Games.
209. On November 3, 2005, Premier Wen Jiabao presides over the fifth meeting of the State Informatization Leading Group. The meeting reviewed and approved “The National Informatization Development Strategy (2006-2020)”. It was considered that developing and implementing the strategy was an important deployment of conformance to the world’s trend of informatization, and an important movement to achieve the goal of developing the economy and the society in the new stage.

210. On November 17, 2005, “Science Museums of China” and “Tianfu Agricultural Information Network” attained “World Information Summit Award” of “The World Summit on the Information Society (WSIS)” in Tunis phase, it is the first time for China’s website to attain such a great international award.

211. On December 31, 2005, .CN domain name registration exceeded one million for the first time, attained 1,096,924, which ranked first among all ccTLDs in Asia and sixth in the world.

212. In the year 2005, Blogers and attached concept of Web2.0 promoted tremendous development of China's Internet. The emerging concept of Web2.0 marked the beginning of a new evolution stage of new media on the Internet. As it was widely used, there also emerged a series of socialized applications such as Blog, RSS, WIKI, SNS friend-making
network and so on.

213. On January 1st, 2006, website of the Central People’s Government of the People’s Republic of China (www.gov.cn) formally launched. This website is a composite platform for the State Council and its departments, along with people’s governments of each province, autonomous region and municipality to release information of governmental affairs on the Internet and provide online services.

214. On January 17th, CNNIC issued “the 17th Statistical Survey Report on the Internet Development in China” in Beijing. The report shows that till Dec. 31st, 2005, China has had about 45,900,000 computers on the Internet, about 111,000,000 Internet users, 1,096,924 registered CN domain names, and about 694,200 websites. The international network bandwidth of China is 136,106 Mbps by then.

216. On March 19th, 2006, the National Informatization Leading Group issued the General Frame of National Electronic Government Information, set the requirements and targets for establishing the general frame of national electronic government information, described the form of the general frame of national electronic government information, and pointed out the value-orientation and development direction of national electronic government information for the next stage.

217. On March 30th, 2006, the Management Methods for Internet Email Service issued by MII began to take into effect.

218. In June 2006, MII decided to initiate the targeted movement of regulating and standardizing the rates and charging behavior of mobile information service nationwide. On Sep 14th, MII issued “the Notice on Regulating Rates and Charging Behavior of Mobile Information Service”. During September to November, provincial communication management bureaus found out and punished at least 245 illegal mobile value-added service providers. As a result, the profits of the listing mobile value-added service providers in 2006 decreased a lot.

219. In June 2006, Xiang Wenbo published article titled “Xuzhou Construction Machinery Group Co., Ltd.(XCMG) Acquisition: a beautiful lie” on his weblog along
with two other related articles to reveal the event of Carlyle Group's buying Xuzhou Construction Machinery Group Co., Ltd.. The articles arose great reverberation. The price for Carlyle Group to buy XCMG was downed from 375 million USD for 85% shares to 233 million USD for 45% shares. It highlighted the influence of small mass spreading. Investigation Report of China Blogs in 2006 issued by CNNIC shows that till August 2006, blog authors have increased to 17,485,000.

220. On July 1st, 2006, the Regulations on the Protection of the Right of Communication through Information Network approved in the 135th standing conference of the State Council began to take into effect.

221. On July 18th, 2006, the award of 16th “Chinese Journalism Prize” held by All-China Journalists’ Association was revealed. Network news articles were in the prize competition for the first time. Thirteen network news articles were awarded prizes.

222. On September 23rd, 2006, the “Core Network (CNGI-CERNET2/6IX) of the Model Network of Chinese Next Generation Internet (CNGI) Project” built by the network center of China Education and Research Network (CERNET) and other 25 universities such as Tsinghua University was formally accepted by the country.
223. On October 13th, 2006, the International Engineering Task Force (IETF) formally issued the Registration and Administration Recommendation for Chinese Domain Names as RFC4713. The standard was mainly constituted by CNNIC.

224. On October 26th, 2006, Internet Society of China set up the “Anti-Malicious Software Collaborative Working Group”.

225. On November 16th, 2006, the “Golden Shied Project”, a project for establishing national police affairs information management system, formally obtained the national completion acceptance in Beijing.

226. On December 18th, 2006, six ISPs include China Telecom, China Netcom, Chunghwa Telecom, Korea Telecom, and Verizon of US announced in Beijing that they will jointly to build the Trans-Pacific Fiber Cable System.

227. On the night of December 26th, 2006, 7.2 (Richter Scale) earthquake occurred in south Taiwan, China, which broke 11 optical-fiber submarine cables, including China-US submarine cable, Asia-Pacific No.1 submarine cable, Asia-Pacific No.2 submarine cable, FLAG submarine cable, Asia-Euro submarine cable and FNAL submarine cable. This
caused a large area of Internet from China Mainland to Taiwan, North America, Europe and Southeast Asia paralyzed, and access many oversea websites are obstructed.

228. In the end of 2006, a virus called “Nimaya” broke out. Millions of computers were affected and damaged. The investigation shows that: 90% of the new viruses in 2006, showed evident characteristics of for profits. The purpose of virus producers veered from showing off their techniques to pursuing illegal profits.

229. On January 23, 2007, China Internet Network Information Center (CNNIC) released the 19th statistical report on the development of the Internet in China. By December 31, 2006, there were about 59.4 million computers in China which had access to the Internet. The number of Internet users was about 137 million, and the proportion of the number of netizens in the population of the country exceeded 10% for the first time. The total number of domain names was 4,109,020, the number of websites was about 843,000, and the network bandwidth of international export was about 256,696Mbps.

230. On January 23, 2007, the Political Bureau of the CPC Central Committee collectively studied the development of world network technology and the construction and management of Internet culture in China. Secretary-General Hu Jintao pointed out while presiding over the study that whether we could actively use and effectively manage the Internet and whether we could truly make the Internet a new approach for transmitting advanced socialist culture, a new platform of public cultural services, and a new space of people’s healthy spiritual and cultural life were related to the healthy
development of the socialist cultural cause and cultural industry, to the cultural and
information safety and the long-term stability of our country, and to the overall situation
of the socialist cause with Chinese characteristics.

231. On February 15, 2007, 14 ministries and commissions including the Ministry of
Culture issued the Circular Concerning Further Strengthening the Management of
Internet Cafés and Online Games, which regulated, for the first time, the virtual currency
transaction in online games.

232. On February 28, 2007, People’s Daily, the largest comprehensive print media and
the newspaper of the CPC central government, formally issued mobile phone newspapers
all over the country. It became a landmark event in the integration of modern
communication technology and news media.

233. From May 2007, 11 websites such as qianlong.com, sina.com, sohu.com, 163.com,
tom.com, and china.com held Online Lecture Hall activities to transmit scientific and
cultural knowledge in such forms as online video lecturing, textual recording and netizen
interactive communication. By the end of December, altogether over 330 lectures had
been held, and the accumulated hits exceeded 100 million person-times.

234. On June 1, 2007, the National Development and Reform Commission and the State
Council Informatization Office jointly released the first E-commerce development plan in
China—the Eleventh Five-Year Plan for the Development of E-commerce, which, for the
first time, determined the strategy and tasks for developing E-commerce at the level of
235. On June 18, 2007, the Anti-Junk Mail Comprehensive Treatment Platform of the Internet Society of China was formally opened, and the number of e-mailbox users of the 10 email operating enterprises connected to this platform accounted for over 80% of the total number of e-mailbox users in China.

236. In July 2007, Wang Xiao, the blog owner of Leading Brother 777, called the Number One Blog in the World in the hot wave of the stock market in China, was brought under criminal detention by the police in Jilin. The nature of the case was determined to be new mass-related economic crime. The event showed the negative effect of blog products, and meanwhile reflected the new complexity in the course of public opinion formation.

237. On August 21, 2007, the Blog Service Self Discipline Convention was formally released in Beijing. This Convention advocated the real name registration system. Over 10 renowned blog service providers jointly signed the convention on the site of the release meeting.

238. From September 3 to September 6, 2007, TOM withdrew successively from the Hong Kong Stock Exchange and the NASDAQ Stock Exchange of the United States, and became the first China concept stock that withdrew from the stock market.

239. On September 7, 2007, the Survey Report on Internet Development in Rural China
2007 was released. By June 2007, the scale of rural netizens in China exceeded 37 million. There was a big gap between the city and the countryside. The internet penetration rate in the countryside was 5.1%, while the internet penetration rate in the city at the same time was 21.6%. This was the first time for our country to issue a survey report on the development of the Internet in the countryside.

240. On September 30, 2007, the central government transmission backbone network of the national e-government network was formally opened, which symbolized that a uniform national e-government network framework was basically formed.

241. On October 15, 2007, Secretary-General Hu Jintao pointed out at the 17th National Congress of the Communist Party of China, We should have a comprehensive understanding of the new situation and tasks in China's advance toward an industrialized, information-based, urbanized, market-oriented and internationalized country; integrate IT application and industrialization; strengthen efforts to develop and manage Internet culture and foster a good cyber environment. Clear requirements were put forward to the development of IT application and the Internet.

242. On November 1, 2007, Shanghai Giant Network Technology Ltd. was listed in the New York Stock Exchange of the United States. It was the first Chinese network company listed in the New York Stock Exchange and became the online game enterprise with the highest market value in China.

243. On November 1, 2007, seven national standards on information security were

244. On December 4, 2007, the NASDAQ Stock Exchange of the United States announced that Baidu Company became a part of the NASDAQ 100 index and NASDAQ 100 average weighted index. Baidu was the first Chinese company selected into NASDAQ 100 index.

245. On December 18, 2007, the International Olympic Committee and CCTV jointly signed the Agreement on the Transmission Right of the Internet and Mobile Platform in China Regarding the 2008 Beijing Olympics. This was the first time in the Olympic history when new media including the Internet and mobile phones were listed separately into the transmission system of the Olympics as independent transmission platforms.

246. On December 24, 2007, the Ministry of Finance, the Ministry of Civil Affairs and
the State Administration of Sport jointly issued the Circular Concerning the Related
Issues of Lottery Organizations’ Resort to the Internet to Sell Lotteries. The sales of
lotteries on the Internet were forbidden and the rapidly growing online lottery sales were
stopped urgently.

247. On December 29, 2007, the State Administration of Radio, Film and Television and
the Ministry of Information Industry jointly issued the Regulations on the Administration
of Video and Audio Program Service on the Internet.

248. On December 31, 2007, the number of registration for CN domain names, i.e., the
country code top-level domain names, reached 9.002 million, accounting for 75.4% of the
total number of domain names in China, and the websites under CN domain names
reached 1.006 million, accounting for 66.9% of the total number of websites in China.
This symbolized that CN domain names had become the mainstream domain names
registered and applied in China.

249. In December 2007, the Eleventh Five-Year Plan for IT Application in National
Economy and Social Development was released, which put forward the overall objective
of IT application and Internet development of the country in the period of the Eleventh
Five-Year Plan, deployed main tasks, arranged major projects and clarified guarantee
measures. This was an important measure in accelerating the integration of IT application
and industrialization and implementing the scientific outlook on development.

250. In 2007, the market value of Tencent, Baidu and Alibaba successively surpassed
USD 10 billion. Chinese Internet enterprises ascended to the list of the largest Internet enterprises in the world.

251. In 2007, PPG Clothes (Shanghai) Co., Ltd. (PPG) won altogether an international venture capital of USD 50 million. This kind of B2C new E-commerce direct sales mode without stores or channels reflected the channel value of the Internet and showed the further integration of the traditional industry and the Internet.

251. According to the statistics of China Internet Network Information Center (CNNIC), by December 31, 2007, the number of Internet users in China has reached up to 210 million, while the number of the broadband Internet users has reached 163 million, accounting for 77.6% of the total. There are totally 11,931,277 domain names in China with 9,001,993 CN names, about 1,503,800 websites, and international bandwidth about 368,927Mbps.

251. During the period from January to February 2008, many x-rated indecent photos of some Hong Kong female entertainers were leaked to the Internet and disseminated quickly, which was known as the “Nude Picture Scandal”. It has started heated discussion on issues of the purification of the Internet environment and protection of personal privacy on Internet.

253. February 25, 2008, eight ministries and administrative offices jointly issued the Opinions on Intensifying Supervision over Internet Maps and Geographic Information Service Websites, requiring further regulations on the Internet maps and geographic

254. March 11, 2008, in accordance with institutional reform of the State Council passed at the 1st Session of the 11th National People’s Congress, the Ministry of Industry and Information Technology was set up under the State Council. Responsibilities of the former Ministry of Information Industry and the former State Council Informatization Office have been transferred to the Ministry of Industry and Information Technology which now becomes the administrative authority of the Internet industry in China.

255. April 28, 2008, commissioned by the Ministry of Industry and Information Technology, the Internet Society of China set up the “12321 Information Center of Indecent and Unsolicited Electronic Messages”, and the complaints and reports can be submitted via telephone calls, feedbacks on websites, e-mail messages, mobile phone texting and WAP.

6. Since May 2008, with the rapid spreading of SNS (Social Networking Service) websites as Kaixin (“being happy”) and Xiaonei (“on the campus”), SNS has become one of the most popular Internet applications in 2008.

256. As for relief news after the earthquake on May the 12th, 2008, in Sichuan Province,
people.com, xinhuanet.com, chinanews.com and cctv.com had released about 123,000 pieces of news on the earthquake relief (including pictures, texts, audios and videos) by May 23, 2008, and played a leading role in news releasing; sina.com, sohu.com, NetEase and Tencent jointly released 133,000 pieces of news. The above eight websites received 11.6 billion hits on news with up to 10.63 million follow-up replies. The Internet played an important role in news releasing about earthquake relief, helping people find their missing kin, delivering aids and soliciting donations. The development of China’s Internet media has come to a new stage.

257. June 20, 2008, President Hu Jintao communicated with the Internet users on line through the ChinaForce BBS on people.com. As a key channel for information exchange, the Internet has attracted more and more attention of the government.

258. Up to June 30, 2008, the total number of Internet users in China reached 253 million, ranking first in the world for the first time. On July 22, the CN domain name became the world’s top national domain name with a large registration number of 12.188 million.

259. July 2, 2008, Beijing Administration for Industry and Commerce officially issued the Opinions on Strengthening Supervision and Administration over the Order of Electronic Commerce Market which provides that, from August 1, each profitable on-line shop must obtain a business license before business operation.

260. September 17, 2008, Premier Wen Jiabao made comments on the “reporting letter posted on a blog about concealing of deaths in the landslide accident in Loufan County,
Shanxi Province on August 1”, requiring relevant authorities to carry out careful inspection and verification of the major accident of burst of a dam at a refuse ore. The function of Internet as means of supervision by public opinions has caught further attention of the central government.

261. September 28, 2008, according to the official reply to each local taxation bureau by the State Administration of Taxation, the incomes obtained by individuals purchasing virtual currency from Internet players and reselling to others with premiums should be subject to individual income tax, and a 20% individual income tax under the category of “income from transfer of property” should be levied.

262. From November to December 2008, the CCTV exposed successively the defects of the business operational model of two major search engines – Baidu and Google. It has triggered a crisis of confidence of the Internet users in those search engines, and advantages or disadvantages of the pricing on ads based on hitting employed in search engines have also become a hot topic.

263. December 22, 2008, sina.com announced an acquisition of the outdoor digital advertising business of Focus Media Group at a price of about 1.3 billion USD, which was so far the largest Internet purchase in China.

264. According to the statistics of China Internet Network Information Center (CNNIC), by December 31, 2008, the number of Internet users in China has reached up to 298 million with an Internet penetration rate of 22.6%. The number of the broadband Internet
users has reached 270 million, accounting for 90.6% of the total. There are totally 16,826,198 domain names in China with 13,572,326 CN names, about 2,878,000 websites, and international bandwidth about 640,286.67Mbps.
APPENDIX II

The National Medium- and Long-Term Program for Science and Technology Development (2006-2020)

An Outline

The State Council

The People’s Republic of China
Table of Contents

I. Preface

II. Guiding Principles, Development Goals, and Overall Deployment
   1. Guiding Principles
   2. Development Objectives
   3. Overall Deployment

III. Main Areas and Priority Topics

1. Energy
   (1) Industrial energy efficiency
   (2) Clean, efficient coal development and utilization, coal liquefaction, and gasification-based co-generation
   (3) Oil and gas prospecting, development, and utilization under complex geological conditions
   (4) Low-cost, large-scale development and utilization of renewable energy resources
   (5) Super large-scale electric power transmission and distribution and power grid safeguards

2. Water and Mineral Resources
   (6) Optimized distribution and comprehensive development and utilization of water resources
(7) Comprehensive water conservation
(8) Seawater desalination
(9) Resources prospecting for additional reserves
(10) Efficient development and utilization of mineral resources
(11) Efficient development and utilization of maritime resources
(12) Comprehensive zoning of resources

3. The Environment
(13) Comprehensive pollutant control and waste recycling
(14) Functional restoration and reconstruction of ecosystems in ecologically vulnerable areas
(15) Maritime ecological and environmental protection
(16) Global environmental change watch and response strategies

4. Agriculture
(17) Germplasm development, preservation, innovation and targeted cultivation of new varieties
(18) Healthy farming practices in domestic animals, poultry, and aquatic products, and associated epidemic disease prevention and control
(19) Deep processing and advanced storage and shipping of farm produce
(20) Integrated development and utilization of agro-forest biomass
(21) Agro-forest ecological safety and modern forestry
(22) Development and production of environment-friendly fertilizers,
herbicides, and pesticides, and ecoagriculture

(23) Multifunctional farm equipment and facilities

(24) Precision farming and associated informatization

(25) Modern dairy industry

5. Manufacturing industry

(26) Basic and generic parts and components

(27) Digital and intelligent design and manufacturing

(28) Green, automated process industry and corresponding equipment

(29) Recycling iron and steel process techniques and equipment

(30) Large-scale marine engineering technologies and equipment

(31) Basic raw materials

(32) Next-generation information functional materials and components

(33) Key accessory materials and engineering processes for defense industry

6. Transportation Sector

(34) Transport infrastructure construction and maintenance technologies and equipment

(35) High-speed rail transport system

(36) Energy efficient and new energy-based Automobiles

(37) Efficient transport technologies and equipment

(38) Intelligent traffic control systems

(39) Transport safety and emergency safeguard
7. Information Industry and Modern Service Industry

(40) Enabling information technology and major application software for modern service industry

(41) Major next-generation internet technologies and services

(42) High performance, dependable computers

(43) Sensor networks and intelligent information processing

(44) Digital media content platforms

(45) High definition large flat-panel display

(46) Core application oriented information security

8. Population and Health

(47) Safe contraception and family planning, and birth defects prevention and treatment

(48) Prevention and treatment of cardiovascular and cerebrovascular diseases, malignancies, and other major non-infectious diseases

(49) Prevention and treatment of common, frequently-occurring diseases in urban and rural communities

(50) Traditional Chinese Medicine: impartation and innovation

(51) Advanced medical equipment and bio-medicinal materials

9. Urbanization and City Development

(52) Urban planning and dynamic monitoring

(53) Uplifting urban functions and space efficiency
(54) Architecture energy efficiency and green buildings
(55) Urban ecological residential environment and quality control
(56) Urban information platforms

10. Public Security

(57) National public security emergency information platforms
(58) Major workplace accidents warning and rescue
(59) Food safety and entry-exit quarantine
(60) Major public emergency prevention and quick response
(61) Biosafety measures
(62) Major natural disasters prevention and preparedness

11. National Defense

IV. Major Special Projects

V. Frontier Technologies

1. Biotechnology

(1) Target identification technology
(2) Plant-animal varieties and drug molecular design technology
(3) Gene manipulation and protein engineering technology
(4) Stem cell based human tissue engineering technology
(5) Next-generation industrial biotechnology
2. Information Technology

   (6) Intelligent sensing technology
   (7) Ad hoc network technology
   (8) Virtual reality technology

3. Advanced Materials Technology

   (9) Intelligent materials and structural technology
   (10) High-temperature superconducting technology
   (11) Efficient energy material technology

4. Advanced Manufacturing Technology

   (12) Extreme manufacturing technology
   (13) Intelligent service robotics
   (14) Service life prediction technology for major products and facilities

5. Advanced Energy Technology

   (15) Hydrogen and fuel cell technology
   (16) Distributive energy supply technology
   (17) Fast neutron reactor technology
   (18) Magnetic contained fusion technology

6. Marine Technology

   (19) 3-D marine environment monitoring technology
(20) Ocean floor based multi-parameter fast sounding technology

(21) Natural gas hydrate exploitation technology

(22) Deep-sea operation technology

7. Lasers Technology

8. Aerospace technology

VI. Basic Research

1. Disciplinary development

   (1) Basic disciplines

   (2) Cross and emerging disciplines

2. Frontier Scientific Issues

   (1) Quantitative study and systematic integration of life process

   (2) Condensed matters and novel effects

   (3) Matters’ deep inner structures and physical laws at a cosmological scale

   (4) Core mathematics and its application in cross-disciplines

   (5) Earth system process and associated resources, environment, and disasters effects

   (6) Chemical process in creating and transforming new matters

   (7) Brain and cognitive sciences
(8) Innovation in scientific experiments, observational methods, techniques, and equipment

3. Basic Research in Response to Major National Strategic Needs

(1) Biological foundations of human health and diseases

(2) Crop genetic improvement and scientific issues in sustainable agricultural development

(3) Human activities and their impacts on the Earth system

(4) Global change and regional response

(5) Complex systems, disaster formation, prediction and control

(6) Key scientific issues in sustainable energy development

(7) New principles and methodologies for materials design and fabrication

(8) Scientific basis of manufacturing under extreme environmental conditions

(9) Major mechanical issues in aeronautics and space science

(10) Scientific basis for the development of information technology

4. Major Scientific Research Programs

(1) Protein studies

(2) Quantum regulation studies

(3) Nanometer studies

(4) Growth and reproduction studies
VII. Reform of the S&T System and the Construction of a National Innovation System

1. Supporting and Encouraging Enterprises to Become the Main Player in Technological Innovation

2. Deepening the Institutional Reform and Establishing a Modern Research Institute System

3. Advancing the S&T Management System Reform

4. Vigorously Pushing Forward the Construction of a National Innovation System with Chinese Characteristics

VIII. Major Policies and Measures

1. Financial and Taxation Policies Encouraging Technological Innovation at the Enterprise Level

2. Strengthening Assimilation and Absorption of imported technologies, and re-innovation

3. Government Procurement Favoring Indigenous Innovation

5. Financial Policies Encouraging Innovation and Pioneering

6. Accelerating industrialization of high technologies and diffusion of advanced appropriate technologies

7. Perfecting the mechanism for combining defense and civilian sectors, and making defense part of civilian sector

8. Expanding international and regional S&T cooperation and exchanges

9. Improving scientific and cultural literacy of the entire nation, and building a social environment conducive to S&T innovation

IX. S&T Input and S&T Infrastructure Platforms

1. Establishing a diversified, multi-channel S&T input system

2. Readjusting and optimizing input structures, and raising the cost-effectiveness of S&T expenditures

3. Strengthening the construction of S&T infrastructure platforms
4. Establishing a mechanism for sharing S&T infrastructure platforms

X. Talented Workforce Buildup

1. Accelerating the nurturing of a contingent of world caliber experts

2. Bringing into full play the important role of education in cultivating innovative talents

3. Supporting enterprises’ efforts in nurturing and attracting S&T talents

4. Intensifying efforts in attracting high caliber talents from overseas

5. Creating a cultural environment conducive to the Nurturing of Innovative Talents

The 16th National Congress of the Chinese Communist Party commissioned the formulation of an outline for a national medium- and long-term program for science and technology development in the context of the full-fledged construction of a well-to-do society and accelerating the socialist modernization drive, and the State Council has hereby prepared the following outline in compliance with the request.

I. Preface

Since the founding of the People’s Republic of China, especially since the introduction of the policy of reform and opening to the outside world, the nation’s
socialist modernization drive has attained universally acknowledged achievements. However, one has to be keenly aware that the nation is and will remain at a primary stage of socialism for a long time to come. In our effort to build a well-to-do society, we are faced with both rare historic opportunities and grave challenges. The nation’s economic growth shows an excessive dependence on the consumption of energy and resources, with high associated environmental costs; the economic structure is irrational, characterized by a frail agricultural base and lagging high-tech industry and modern service industry; and firms lack core competitiveness and their economic returns are yet to be improved as a result of weak indigenous innovation capability. There are a whole range of problems concerning employment, distribution, health care, and national security that need prompt solution. Internationally, the nation will be for a long period of time under enormous pressures from developed nations who possess economic and S&T superiority. In order to grasp the opportunities and meet the challenges, we must make all-round efforts, including coordinated overall development, deepening the system reform, improving democracy and the rule of law, and reinforcing social management. At the same time, we need to depend even more heavily on S&T progress and innovation in order to achieve substantial gains in productivity and advance the overall economic and social development in a coordinated and sustainable manner.

As the premier productive forces, science and technology are a concentrated reflection and a major hallmark of advanced productivity. In the 21st century, the new science and technology revolution is rapidly unfolding and gestating significant new breakthroughs, which will profoundly change the economic and social visages. Advances in information science and technology, still in the ascendant, will continue to be the
dominant driving force for economic growth; rapid advances in life science and biotechnology will play a key role in improving quality of life; renewed efforts in energy science and technology will open up new avenues for addressing global energy and environmental issues; and exciting new breakthroughs in nanometer science and nanotechnology will usher in a profound technology revolution. Exciting breakthroughs in basic research fields will create whole new horizons for science and technology development and economic growth. S&T achievements are being applied and transferred at an ever faster pace, thus creating new opportunities for catching up and leapfrogging. Therefore, we shall embrace the new era, meeting both opportunities and challenges brought on by the new S&T revolution with a global vision. In today’s world, many countries have made S&T innovation a national strategy and S&T inputs strategic investments by drastically increasing R&D spending. These nations lead the world in deploying and developing frontier technologies and strategic industries and implement important S&T programs in an attempt to enhance their national innovative capability and international competitiveness. Confronted with the new international situation, we must have a greater sense of responsibility and urgency, by making S&T progress a major driving force for the economic and social development more conscientiously and resolutely. We must place the strengthening of indigenous innovative capability at the core of economic restructuring, growth model change, and national competitiveness enhancement. Building an innovation-oriented country is therefore a major strategic choice for China’s future development.

Over more than five decades since the founding of New China, the consistent and painstaking efforts of several generations have led to huge, heartening achievements in
the fields of science and technology. Major S&T accomplishments hallmarked by nuclear weaponry and satellite technology, manned space flights, hybrid rice, theory of oil formation from continental moist depression and associated application, and high performance computers, have greatly enhanced the nation’s comprehensive national strength, uplifted its international position, and inspired the whole nation. However, compared with the developed nations, China’s overall S&T level still has a fairly big gap to close, compared with that of developed nations. This is mainly reflected in the following areas: we have a low rate of sufficiency in key technology supply and a limited number of invention patents; the technological level remains low in some regions, particularly in the rural areas of the central and western regions; the quality of scientific research still needs significant improvement due to a shortage of top notch S&T talents; and investments in science and technology are still insufficient; and there are numerous loopholes in the existing S&T system. Despite the size of economy, our country is not yet an economic power primarily because of our weak innovative capacity.

In the 21st century, China, being a large developing nation, is to accelerate its S&T development and narrow down the gaps with the developed nations. To this end, the nation must make unremitting efforts for a long period of time, while it is also blessed with numerous favorable conditions.

First, China’s sustained fast economic growth and social development creates a huge demand and thus lay a solid foundation for the S&T development. Second, the nation has a fairly consummate system of academic disciplines, with a huge pool of talented people. It has developed world-class R&D capability in a number of major fields,
thus positioning itself for tremendous S&T developments in the future. Third, our country’s continued opening to the outside world has enhanced its S&T cooperation and exchanges with the rest of the world, allowing the country to share the fruits from the new S&T revolution. Fourth, by adhering to the socialist system, China is able to combine the political advantage of mobilizing efforts to do great things and the basic role of market mechanism in effectively allocating resources. This provides an important system guarantee for the prosperous development of S&T activities. Fifth, ours is a country with a 5000-year history of civilization and a culture that is both broad and profound, capable of incorporating things of diverse nature, which favors the creation of a uniquely innovative culture. As long as we strengthen our national confidence, hold scientific concept of development, implement the strategies of rejuvenating the nation through science and education, work hard to catch up over the next 15 years or more, we will be able to produce brilliant S&T achievements that live up to the expectations of our times.

II. Guiding Principles, Development Goals, and General Deployment

1. Guiding Principles

The first 20 years of the century are a period of important strategic opportunities for our country’s economic and social development and S&T progress. Under the guidance of Deng Xiaoping Theory and the “Three Representations” and by implementing the scientific concept of development and the strategy of rejuvenating the nation through science and education and talented people and proceeding from our own
national conditions and taking people-based approach, deepening reforms and expanding
the opening to the outside world, we must strive for the prosperous development of
China’s scientific and technological enterprise so as to realize the goals of the full-
fledged construction of a well-to-do society and provide powerful S&T support for
building a harmonious socialist society.

The guiding principles for our S&T undertakings over the next 15 years are:
“indigenous innovation, leapfrogging in priority fields, enabling development, and
leading the future”. Indigenous innovation refers to enhancing original innovation,
integrated innovation, and re-innovation based on assimilation and absorption of
imported technology, in order improve our national innovation capability. Leapfrogging
in priority fields is to select and concentrate efforts in those key areas of relative strength
and advantage linked to the national economy and people’s livelihood as well as national
security, to strive for breakthroughs and realize leaping developments. Enabling
development is an attempt to strive for breakthroughs in key, enabling technologies that
are urgently needed for the sustainable and coordinated economic and social development.
Leading the future reflects a vision in deploying for frontier technologies and basic
research, which will, in turn, create new market demands and new industries expected to
lead the future economic growth and social development. The guideline is a summary of
China’s practice and experience in S&T development for more than a half century, and an
important choice for realizing the great renaissance of the Chinese nation.

This calls for placing the strengthening of indigenous innovation capability at the
core of S&T undertakings. The Party and government have long advocated and paid close
attention to indigenous innovation. To press ahead with the modernization drive under conditions of opening to the outside world, we must earnestly study and draw on all the fine achievements of human civilization. During the past two decades or so since we began to pursue the policy of reforms and opening to the outside world, our country has imported a huge amount of technologies and equipment, which played an important role in raising the overall technological level of our industries and promoting the country’s economic development. However, one should be clearly aware that importation of technology without emphasizing assimilation, absorption, and re-innovation is bound to weaken the nation’s indigenous R&D capability, which in turn widens the gap with world advanced levels. Facts have proved that, in areas critical to the national economy and security, core technologies cannot be purchased. If our country wants to take the initiative in the fierce international competition, it has to enhance its indigenous innovation capability, master core technologies in some critical areas, own proprietary intellectual property rights, and build a number of internationally competitive enterprises. In a word, the improvement of indigenous innovation capability must be made a national strategy that is implemented in all sectors, industries, and regions so as to drastically enhance the nation’s competitiveness.

S&T talents are critical to increasing indigenous innovation capability. The first and foremost task is to create a favorite environment for cultivating and attracting S&T personnel, with high-quality talents in particular, giving full scope to the enthusiasm and creativity of the broad masses of S&T personnel, so that a constant stream of talents is ensured and the best of S&T talents is brought out. We should make unremitting efforts to build a large, well-structured, high-quality S&T workforce compatible with economic
and social development and national defense work in order to ensure the talents and knowledge base for the nation’s science and technology development.

2. Development Goals

The general objectives for the nation’s S&T development (2006-2020) will be to: noticeably enhance indigenous innovation capability and S&T level in promoting economic and social development and in maintaining national security, in an effort to provide powerful support for the building of a well-to-do society; noticeably improve comprehensive strength in basic research and frontier technology development; and attain a series of high world impact S&T achievements and join the ranks of innovative countries, thus paving the way for becoming a world S&T power by mid 21st century.

Through efforts over the next 15 years, the nation will meet the following objectives in some major scientific and technological areas: 1) mastering core technologies in equipment manufacturing and information industry that are critical to the nation’s competitiveness, and bringing the technological capability of manufacturing and information industries to the world advanced levels; 2) making the nation a world leader in overall agricultural S&T capability, raising the comprehensive capacity of China’s agricultural production, and ensuring the nation’s food safety.; 3) achieving technological breakthroughs in energy development, energy conservation, and clean energy, and advocating optimized energy structures, with unit energy consumption of major industrial products reaching or approaching world advanced levels; 4) establishing technological development models featured with cyclic economy in major sectors and municipalities,
and providing S&T support for building a resource saving and environment friendly society; 5) noticeably enhancing the level of major diseases prevention and control, curbing the spread of major diseases, including HIV/AIDS, hepatitis and other major diseases, striving for breakthroughs in new drugs and key medical equipment, and developing a technological capability for industrialization; 6) in defense science and technology, basically meeting the needs in developing modern arms and associated information technology, and providing S&T support for safeguarding national security; 7) establishing a world-caliber contingent of scientists and research teams, attaining high-impact innovative achievements in the mainstream of science development, bringing the technological level in such frontier areas as information, biology, materials, and space to world advanced levels; and 8) establishing a number of world-class research institutes and universities, and world-competitive industrial R&D centers so that a fairly comprehensive national innovation system of Chinese characteristics can take shape.

By 2020, the nation’s gross expenditures on R&D (GERD) are expected to rise to 2.5% or above of the gross domestic product (GDP) with the rate of S&T contribution to the economy reaching 60% or above, and dependence on imported technology reduced to 30% or below, and the annual invention patents granted to Chinese nationals and the international citations of scientific papers moving into the top five countries.

3. Overall Deployment

In the next 15 years, China’s S&T undertakings will be deployed as follows: 1) In light of our country’s concrete conditions and needs, identify a number of priority areas,
break through some major technological snags so as to raise the nation’s overall S&T support capability. This Outline identifies 11 priority areas for economic and social development, from which 68 priority topics of clearly defined missions and possible technical breakthrough in near term will be selected. 2) Implement some special major projects that are in line with national objectives, and will lead to the leaping development or fill up a blank. The Outline makes the arrangement for total of 16 special major projects. 3) To respond to future challenges, advance deployment will be made for frontier technologies and basic research topics, in order to ensure sustained innovative capability and lead future economic and social development. The Outline selects 27 frontier in 8 technological fields, and 18 basic scientific issues as priorities. It also proposes to implement four major scientific research programs. 4) Deepen the S&T system reform by perfecting relevant policies and measures, increasing S&T investment, strengthening the buildup of S&T talents, and promoting the creation of a national innovation system in order to provide reliable support for the nation to become an innovation-oriented society.

Strategic priorities are identified according to the urgent needs for building a well-to-do society, international S&T development trends, and the nation’s overall strength. 1) Energy, water resources, and environmental protection related technologies are selected as priorities, in an effort to address major bottleneck issues in the economic and social development. 2) Efforts should be made to grasp the rare opportunities presented by continued strong development of information technology and advanced materials, making proprietary intellectual property rights in equipment manufacturing and information industries a major breakthrough point for enhancing the nation’s industrial
competitiveness. 3) Biotechnology is selected as a priority for the future development of the high-tech industry together with enhanced biotechnological applications to agriculture, industry, population and health. 4) Accelerate the development of aerospace and marine technologies. 5) Strengthen basic research and frontier technology development, particularly interdisciplinary research.

III. Main Areas and Priority Topics

The nation’s S&T development shall be planned and deployed according to the principle of coordinated arrangement and advancement, with due consideration to priority areas and topics, so as to provide full and forceful support for addressing urgent issues in economic and social development”.

Priority areas refer to such industries and sectors that are both critical to economic and social development and national security and in dire need of S&T support. Priority topics within the priority areas are defined as urgently needed technology clusters that have clearly defined missions, sound technical foundations, and promising prospects for breakthroughs in the near term. The principles for selecting priority topics are: 1) topics that are desirable for breaking up bottleneck constraints and for enhancing the sustainability of economic growth; 2) topics that are desirable for mastering key and enabling technologies and for improving core industrial competitiveness; 3) topics that are desirable for addressing major public good S&T issues and raising the capability in providing public services; and 4) topics that are desirable for the development of dual-use technologies designed to enhance the capability in ensuring national security.
1. Energy

Energy is of crucial strategic importance to the national economy. Our country is currently suffering from sharp discrepancies between energy supply and demand, an irrational energy structure, and low energy efficiency, with a predominantly coal-based primary energy consumption, resulting in severe environmental pollution. Over the next 15 years, meeting the fast growing demand for energy and for its clean and efficient utilization constitutes a major challenge for the development in energy-related science and technology.

Development paths: 1) Take energy saving as a top priority and reduce energy consumption. Overcoming technological snags critical energy saving in major energy consuming sectors and vigorously develop technologies for energy saving buildings so as to significantly improve efficiency in primary and end use of energy. 2) Increase energy supply by promoting a diversified energy structure. While raising the technological level of oil-gas utilization and hydroelectric power, it is encouraged to vigorously develop nuclear energy technology to acquire indigenous technology development capability in nuclear power systems. Strive for breakthroughs in renewable energy, including wind energy, solar energy, and biomass energy, and associated scale applications. 3) Promote clean and efficient use of coal in order to reduce environmental pollution. It is encouraged to vigorously develop clean, efficient, and safe coal exploration and aim at the world advanced levels. 4) Strengthen the assimilation and absorption of imported energy technologies and associated re-innovation. Master core technologies in building
major equipment for coal-fired and nuclear power generation. 5) Raise the technological capability of optimizing regional energy distribution. Priorities will be given to developing advanced and reliable power transmission and distribution technologies to realize large volume, long distance, and efficient power transmission.

Priority topics:

(1) Industrial energy efficiency

Priorities will be given to research on and development of energy-saving technologies and equipment for major high energy consumption sectors, including process industries, such as metallurgical, chemical industry, and transportation industries. Developing energy-saving technologies for mechanical and electronic products, highly energy-efficient, long-life cycle LED products. Develop comprehensive utilization technologies at different energy gradients.

(2) Clean, efficient coal development and utilization, coal liquefaction, and gasification-based co-generation

Priorities will be placed on developing efficient mining technologies and equipment, and efficient power generation technology and equipment, including heavy duty gas turbines, integrated gasification combined cycle (IGCC), high-parameter supercritical generators, and large supercritical circulating fluidized beds (CFB). It is also encouraged to develop transformation technologies for coal liquefaction, coal gasification, coal chemistry, coal gasification based polygeneration, and technologies and equipment for comprehensive control and utilization of pollutants derived from coal burning.
(3) Oil and gas prospecting, development, and utilization under complex geological conditions

Priorities will be given to the development of technologies for oil-gas prospecting in complex environment and rock strata, technologies for efficient and scale development of low grade oil-gas resources, technologies for increasing oil recovery in old oil fields, and technologies for prospecting and mining deep oil-gas reserves.

(4) Low-cost, large-scale development and utilization of renewable energy resources

Emphasis will be on the development of large wind power generators, construction technologies and equipment for coastal and inland wind fields as well as wind energy intensive areas in Western China, cost-effective technologies for solar photovoltaic batteries, technologies for solar-based power generation, technologies for built-in solar energy building structures, and technologies for developing and utilizing biomass and geothermal energy.

(5) Safeguards of super large electricity transmission and distribution networks

Priorities will be to develop technologies and equipment for long distance and large volume DC transmission, and for super high voltage AC transmission. Developing technologies for batch power grid and associated transmission and distribution, power quality monitoring and control, and safe power supply for large Internet networks, key technologies for west-to-east electric power diversion project, technologies for automated grid dispatch system, and technologies and systems for efficient transmission and distribution management.
2 · Water and Mineral Resources

Water and mineral resources constitute an important material basis for the sustainable economic and social development. Our country suffers from serious shortage of water and mineral resources, a low rate of comprehensive utilization of resources such as mineral resources and irrigation water which far below that of internationally advanced levels. With complex geological conditions for resources prospecting and increasing difficulties, there is an urgent need for technologies that can improve resources prospecting and utilization and raise the level of resources utilization.

**Development paths:**
1) **Assign priority to** resources saving. The focus will be research on technologies for agricultural water saving and urban cyclic water utilization, and technologies for trans-basin water diversion, rainfall and flood water utilization, and sea water desalination. 2) Overcome barriers of complex geological conditions so as to expand the existing resources reserves. Priorities will be placed on studying mine formation mechanism, and develop technologies for deep-mine evaluation and efficient prospecting, and fast prospecting technologies for mineral deposits under complex geological conditions in regions such as the Qinghai-Tibet Plateau. Striving to discover a number of large backup resource bases for additional resources supply. Develop technologies for efficient mining and comprehensive utilization in order to enhance comprehensive utilization of water and mineral resources. 3) Vigorously develop and utilize non-traditional resources. Master key technologies for the development and utilization of coal-bed methane and marine minerals so as to raise the research and
development capability of novel resources utilization. 4) Strengthen innovative capability in developing equipment for resource prospecting. Vigorously develop technologies for high precision prospecting and drilling equipment, large mining machinery, and marine development platforms, to bring major resources prospecting equipment and facilities to world advanced levels.

**Priority topics:**

(6) **Optimized distribution and comprehensive development and utilization of water resources**

Priorities will be given to developing technologies for the conversion and optimal distribution of atmospheric moisture, surface water, soil moisture, and underground water, technologies for the utilization of contaminated water and rainfall and flood water, technologies for artificial rain enhancement, and key technologies for water control projects in major river systems, including the Yangtze River and Yellow River, and for major hydrological projects such as the south-to-north water diversion project.

(7) **Comprehensive water conservation**

Priorities will be to developing technologies for industrial cyclic utilization of water and water efficient production activities. Developing outfitting technologies for water saving in irrigation, dry land farming, and biological water efficiency. Strive for major breakthroughs in precision irrigation technology, and intelligent farming water management technology and equipment. Develop water saving technologies and devices for daily life applications.
(8) **Seawater desalination**

Priorities will be given to developing technologies for seawater pre-handling, nuclear energy coupling and electricity-heat cogeneration, low-cost membrane-based desalination and critical materials, and comprehensive utilization of salty water. Develop seawater desalination-based heating equipment for scale applications, seawater desalination facilities, and integrated coupling.

(9) **Resources prospecting for additional reserves**

Priorities shall be placed on studying the law of mineral formation mechanisms and prediction technologies, developing air-born geophysical survey techniques, and fast, comprehensive and in-depth prospecting technologies such as 3-D high-resolution earthquake and high-precision geomagnetism and geochemistry.

(10) **Efficient development and utilization of mineral resources**

Priorities will be on studying comprehensive technologies for deep and complex mining and wasteless mining; developing new processes and large equipment for automated ore preparation and smelting; and developing technologies for the utilization of low grade and complex mineral resources.

(11) **Development and utilization of maritime resources**

Priorities shall be placed on: developing prospecting technologies for offshore oil-gas deposits and comprehensive recovery technologies for thick-oil oilfields; developing technologies for the protection and effective utilization of marine biological resources;
and developing technologies for direct seawater utilization and comprehensive exploitation of seawater chemical resources.

(12) Comprehensive zoning of resources

Priorities will be given to: research on technologies for comprehensive optimization of water and soil resources, farming activities, and ecological and environmental protection; developing analytical techniques for the optimization of multi-variable based large area resources distribution corresponding to regional distributions of water and land resources; and establishing decision-making models for optimized development of water and land resources in different areas.

2. The Environment

Ecological and environmental improvement constitutes a major issue concerning the sustainable economic and social development and the quality of people’s livelihood. The country is confronted with serious environmental pollution problems, with an increasingly degraded ecosystem and a weak capability of handling pollutants. Global environmental issues have become an international concern. China needs to enhance its capability in being involved in the global efforts for environmental change. Sustaining rapid economic growth under the prerequisite of overall environmental improvement imposes major strategic demands for innovation in environment science and technology.

Development paths: 1) Guiding and supporting the development of cyclic economy. Vigorously develop integrated clean production technologies for highly polluting
industries, intensify the reduction of wastes and safe treatment of wastes, and strengthen the development of common technologies for the cyclic economy; 2) comprehensive control of regional environment. Conduct comprehensive control and treatment of water environment in drainage areas and regional atmospheric pollution, establish technical integration and demonstration for comprehensive control of typical ecologically degraded areas, and develop technologies for drinking water safety and pre-warning for ecological and environmental monitoring, so as to drastically increase the S&T capability for environmental quality improvement. 3) promoting the development of environmental protection industry. Priorities will be given to developing major environmental protection equipment and facilities in line with the country’s concrete conditions, securing more market share for domestic environmental protection products, and raising the technical level of environmental protection equipment. 4) Vigorously participate in international cooperation in the field of the environment. Strengthen research on response strategies in implementing the global environment convention and on scientific uncertainties of climate change and their implications, develop technologies for global environmental change watch and greenhouse gases emission reduction, and enhance the capability in responding to environmental changes and in implementing the international convention.

**Priority topics:**

(13) Comprehensive pollutant control and waste recycling

Priorities will be to develop pre-warning technologies for regional environmental quality monitoring; master key technologies for urban atmospheric pollution control, develop technologies for non-conventional pollutants, technologies for turning wastes
into useful resources, and integration technologies for clean production in heavily polluting sectors; establish technical demonstration models for the cyclic economy.

(14) Functional restoration and reconstruction of ecosystems in ecologically vulnerable areas

Priorities will be given to developing dynamic monitoring technologies for typical vulnerable ecological areas, including Karst areas, the Qinghai-Tibet Plateau, the middle and upper reaches of the Yangtze River and Yellow River, Loess Plateau, deserts and desertification lands, farming-grazing areas, and mining areas; developing technologies for pasture degradation and rodents control, and technologies for restoring and reconstruction of degraded ecosystems; developing ecological protection and restoration technologies for major engineering works such as the Three-Gorge Dam project and the Qinghai-Tibet Railway, and complex mining areas; establishing technical support models for restoring the functions of diverse ecosystems and maintaining the improvement; and establishing a comprehensive evaluation and technical assessment system for the functionality of ecosystems.

(15) Maritime ecological and environmental protection

Priorities will be given to developing technologies and equipment for marine ecological and environmental monitoring, strengthening the study of marine ecological and environmental protection, developing technologies for offshore ecological and environmental protection and repair, and sea emergency response and handling, and developing high-precision digital technologies for marine dynamic environment prediction.
(16) Global environmental change watch and response strategies

Priorities will be placed on developing technologies for accurate monitoring of large scale environmental changes, greenhouse gases emission control and utilization, including carbon dioxide and methane utilization in major industries, biological carbon fixation and carbon fixation engineering, climate change study, biodiversity protection, ozone layer protection, and sustainable organic pollutants control.

3. Agriculture

Agriculture is the foundation of the national economy. Our country is increasingly constrained by natural resources, with its per capita arable land and water resources noticeably lower than the world average. The growing demand for major agricultural produces, including grains and cotton, and pressures of yield increase, increasing farmers’ income, and intensified competition of agricultural products will be a long standing phenomenon. China’s agricultural structure remains irrational, with a low industrialization level and low value-added agricultural products. The poor ecological and environmental conditions impose serious constraints on the sustainable agricultural development, coupled with thorny food and ecological safety problems. With the country’s basic situation and tough challenges it has to face, scientific and technological progress constitutes a fundamental approach through which major agricultural problems can be addressed. It includes raising the agricultural scientific and technological level, enhancing the diffusion of advanced appropriate technologies, alleviating the constraints of resources, improving comprehensive agricultural productivity in a sustainable manner,
and accelerating the pace of agricultural modernization.

Development paths: 1) Transform conventional farming technologies through the introduction of high technologies so as to enhance comprehensive agricultural productivity in a sustainable manner. Priorities will be placed on carrying out research on applied biotechnology, strengthening the integration and compatibility of agricultural technologies, overcoming technological problems in crop breeding, efficient production, animal and aquatic breeding and production and diseases control, developing diversified compound agricultural operations, improving the quality of agricultural products, and sustaining yield increase. 2) Extend agricultural production chain in order to achieve an overall improvement of agriculture related industrialization and comprehensive agricultural returns. Priorities shall be given to developing technologies for precision and deep processing of agricultural produce, post-production loss reduction, and commercial applications of green supply chains. Developing advanced technology and equipment for food processing and food safety monitoring. Developing a food processing industry featured with healthy foods, and a modern circulation industry, and creating more room for increasing farmers’ income. 3) Develop technologies for comprehensive agricultural and forestry development while ensuring ecological safety. Priorities will be to develop technologies for environment friendly fertilizers and pesticides, precision farming operations, resources-oriented utilization of agricultural and forestry residues, comprehensive agricultural environment control, promote the development of new farming industries, and raise the ecological environment quality of agriculture and forestry. 4) Develop a factory-like agriculture in order to increase labor productivity of farming activities. Priorities will be given to developing farming facilities related
technologies, including farming environment regulation and efficient crop cultivation with super high yield, developing modern farm machinery with multiple functions, and accelerating the integration and application of agriculture related information technology.

**Priority topics:**

(17) **Germplasm development, preservation, and innovation in and targeted cultivation of new varieties**

Priorities will be assigned to research on and development of fine agricultural crop, tree, pasture, and aquatic species, molecular evaluation of germplasm, animal and plant molecular breeding and targeted hybrid breeding, scale seed breeding, reproduction, and comprehensive processing.

(18) **Healthy farming practices in domestic animals, poultry, and aquatic products, and associated epidemic disease prevention and control**

Priorities will be on developing technologies for producing safe and high quality feedstuffs and facilities for scale healthy breeding; developing valid specific vaccines, and safe veterinary drugs and instruments; developing technologies for monitoring, diagnosing, preventing, treating and eradicating epidemic diseases affecting both humans and animals; developing technologies for offshore and freshwater aquaculture and technologies and equipment for ocean-going fishery and storage and processing.

(19) **Deep processing and advanced storage and shipping of farm produce**

Priorities will rest on developing technologies and equipment for clean and deep
processing of agricultural produce and specialty agricultural and forestry products, post-
production loss reduction for grains and edible oils, green storage, fresh-keeping and
delivery of live agricultural produce, and cold chain delivery.

(20) Integrated development and utilization of ago-forest biomass

Priorities will be on: developing key technologies for efficient, scale and low-cost
cultivation, collection, and conversion of agricultural and forestry biomass; developing
key technologies for biomass energy production, including methane, fixed and liquid
fuels, and new biomaterials; developing technologies for resource-oriented utilization of
rural garbage and contaminated water, methane-based power generation, and new
biomaterial equipment possessing proprietary intellectual property rights.

(21) Agro-forest ecological safety and modern forestry

Priorities will be placed on: developing technologies for establishing agriculture
and forestry ecosystems, technologies for regulating forestry and pasture ecosystems,
technologies for monitoring, prevention and control of forest and pasture fires, and
agriculture and forestry related diseases and pest control; developing technologies for
combating biological invasion and ecological and meteorological disasters, technologies
for the sustainable operation of ecological forestry economy, technologies for artificial
grassland improvement and high quality grass breeding, and technologies for producing
environment friendly composite materials made of bamboo or wood.

(22) Development and production of environment-friendly fertilizers, herbicides,
and pesticides, and eco-agriculture
Priorities will be given to: developing key technologies for environment friendly fertilizers and pesticides, technologies and equipment for slow-release fertilizers, and technologies for comprehensive prevention and control of hazardous organisms featured with efficient, long lasting, and safe functions; establishing a quarantine pre-warning system in response to invasion of hazardous organisms; and developing environment friendly farming technologies that can improve soil fertility, reduce soil contamination and soil erosion, and restore the functions of degraded grassland.

(23) Multifunctional farm equipment and facilities

Priorities will be given to: research on and development of key multifunction equipment suitable for our country’s farming operations, developing economical agriculture and forestry machinery, intelligent machinery with positioning and quantity adjustment functions, technologies and equipment for healthy breeding, farming machinery and technologies with protection functions, greenhouse facilities, and support equipment.

(24) Precision farming and associated informatization

Priorities will be given to developing digital technologies for collecting animal-plant growth and ecological environment related information, and technologies for real-time monitoring of soil elements, including moisture, fertilizer, light, and temperature; developing technical systems for precision operation and management and digital technology dedicated to remote rural areas; developing technologies and equipment for viewable information service, agriculture and forestry ecosystem monitoring, and virtual
(25) Modern dairy industry

Priorities will be assigned to research on and development of technologies for fast breeding of high quality stud bulls, and industrialized production of dairy cow fetus; developing advanced technologies for cow feeds, cultivation and effective utilization of pasture; developing technologies for diseases prevention and control, and scale breeding, and technologies and equipment for dairy products deep processing.

4. Manufacturing Industry

Manufacturing industry makes a mainstay of the national economy. China is a large manufacturing economy, but not yet a manufacturing power. China’s manufacturing technology has a weak foundation, with a limited innovation capability, primarily low-end products, high consumption of resources and energy, and serious pollution.

Development paths: 1) raising the capability of equipment design, manufacturing, and integration. With promoting industrial technological innovation as a starting point, realizing proprietary design and manufacturing of high-end programmed machine tools, major set equipment, key materials, and key components; 2) developing environment friendly manufacturing. Accelerating application of proven technologies in the entire manufacturing cycle of products, including materials and products development and design, processing, manufacturing, sale, service, recovery, and utilization. Developing environment friendly cyclic manufacturing techniques featured with energy efficiency. Making China’s manufacturing industry part of the internationally advanced, in the
context of resources consumption and environmental loads; 3) transforming and upgrading manufacturing industry using high technology. Promoting information process in the industry, developing basic raw materials, raising the grade, technology content, and added values of products, and uplifting the overall technical level of manufacturing industry.

**Priority topics:**

(26) **Basic and generic parts and components**

Priorities will be to develop key technologies for major basic and generic parts and components and associated design, manufacturing, and mass production; develop advanced moulding and processing technologies for large and special parts and components; develop design and manufacturing technologies for generic parts and components as well as precision test instruments.

(27) **Digital and intelligent design and manufacturing**

Priorities will be on given to research on digital design, manufacturing, and integration technologies, and establish a number of industrial platforms for digital product design and manufacturing. Develop product-cycle oriented innovative and network-based digital and intelligent design approaches and technologies, computer-aided engineering analysis and process design and integration technologies.

(28) **Green, automated process industry and corresponding equipment**

Priorities will be to develop environment friendly processes and manufacturing
technologies as well as techniques, processes and equipment for efficient and clean utilization of resources; develop technologies for process scale-up, ecological industry concept-based system integration and automation; develop sensors and intelligent testing and control technologies, equipment, and control systems needed by process industries. Develop large cracking furnace technology, large steam ethylene cracking technology and set equipment, and large energy efficient chemical fertilizer process and equipment.

(29) Recycling iron and steel process techniques and equipment

Priorities will be given to research on and development of new generation circular iron and steel processes based on smelting reduction and optimized utilization of resources, and with the combination of production, energy conversion, and recycling of wastes, which will be made a role model for the circular economy. Develop technologies for cyclic utilization of secondary resources, cogeneration technology for metallurgical processes, and gradient utilization technology for low thermal value steam. Develop technologies for efficient and low-cost clean steel production, non-adhesive coking, integration design, manufacturing, and system coupling technologies for large continuous plate casters and continuous rollers.

(30) Large-scale marine engineering technologies and equipment

(31) Basic raw materials

To meet the needs of the primary industry, priorities will be placed on developing technologies for manufacturing high-performance composite materials and super large compound components, high-performance engineering plastics, light high-intensity
metals and inorganic non-metal structural materials, high-purity materials, rare earth materials, petrochemicals, precision chemicals, catalysts, separating materials, light textile materials and associated applications, and environment friendly green and healthy materials.

(32) Next-generation information functional materials and components

(33) Key accessory materials and engineering processes for the defense industry

5. Transportation

Transportation represents the lifeline of the national economy. Currently, the country’s existing major transport facilities and core technologies deplore a large gap from the world advanced levels, as characterized by inadequate transport capability, lagging construction of comprehensive transport systems, poor coordination of various means of transportation, and high energy consumption and severe environmental pollution. The construction of a full-fledged well-to-do society imposes greater demand for the transportation sector, calling for significant improvement of transport science and technology.

Development path: 1) enhance indigenous innovative capability in aircraft, automobile, ship, and rail transport; 2) aim at providing a smooth, convenient and humanized transport services by strengthening coordinated planning, developing technologies for traffic information system and intelligent process, and safe and high-
speed transport systems, improving transport networks’ capability and efficiency, realizing traffic information sharing and effective connection among different traffic means, uplifting the technical level of traffic operation management, and developing an integrated transport system; 3) promote the development of transportation in the direction of energy efficiency, environmental protection, and safety by striving for major breakthroughs in key technologies necessary for such improvement; 4) master key technologies for the construction and maintenance of major national transport infrastructure while improving construction quality and cost-effectiveness.

Priority topics:

(34) Transport infrastructure construction and maintenance technologies and equipment

Priorities will be given to developing critical technologies and equipment with respect to rail transport, cross-bay routes, offshore deep water harbors, large airports, large bridges and tunnels, integrated 3-D traffic hubs, deep-sea oil-gas pipelines, and other sophisticated transportation infrastructure.

(35) High-speed rail transport systems

Priorities will be given to research on and development of key technologies for high speed rail transport control and speed regulation systems, locomotive building, rail line construction, and system integration in order to acquire set technologies. Carry out operation tests so as to master technologies for operation control, rail line construction, and system integration.
(36) Energy-efficient and New Energy-based automobiles

Priorities will be assigned to research on and development of key technologies for design, integration, and manufacturing of hybrid, alternative fuel, and fuel cell automobiles, power system integration and control technologies, automobile computation platform technologies, and technologies for high-efficiency and low-emission internal combustion engines, fuel cell engines, accumulator batteries, driving motors, and other critical components, and technologies for developing experiment and test techniques and infrastructure for automobiles using new energy.

(37) Efficient transport technologies and equipment

Priorities will be given to research on and development of heavy duty passenger cars, large power locomotives, special heavy duty vehicles, urban rail transit systems, large high-tech ships, large ocean-going fishing boats, scientific expedition ships, and novel shipping tools, including lower-altitude multipurpose aircrafts, and high viscosity crude oil and multiphase flow pipeline transport systems.

(38) Intelligent traffic control systems

Priorities will be to develop technologies for traffic information platforms, information sharing, modern logistic systems, urban traffic control systems, intelligent automobiles, and new -generation air traffic control systems.

(39) Transport safety and emergency safeguards

Priorities will be to develop technologies for traffic accident prevention and pre-
warning, emergency handling, active/passive safety for transport tools, techniques for traffic accident reconstruction, fast traffic emergency response system, and quick search and rescue missions.

6. **Information industry and Modern Service Industry**

   The development of information industry and modern service industry constitutes a key link in advancing the new industrialization drive. The increasingly information technology-based national economy and modern service industry impose a higher demand for the development of information technology.

   Development paths: 1) strive for breakthroughs in core technologies that constrain the development of information industry and master core technologies for integrated circuits and key components, major software, high performance computers, broadband mobile telecommunication, and the next generation internet, in order to upgrade indigenous development capability and overall technological level; 2) strengthen integrated innovation in information technology products and improve design and manufacturing capability so as to ensure scalability, user friendliness, and cost-effectiveness of information technology products, nurture new technologies and businesses, and enhance the competitiveness of information industry; 3) driven by market demand, attach more importance to and strengthen integrated innovation and develop technologies and products that support and lead the development of modern service industry while promoting the transformation and technological upgrading of the traditional industries; 4) with attention focused on creating highly credible networks,
develop network information security technologies and products, establish technical support systems for information security, and develop the technological capability in handling information security emergencies.

Priority topics:

(40) Enabling information technology and large application software for modern service industry

Priorities will be given to developing highly credible online software platforms, large enabling application software, mediumware, built-in software, grid computation platforms and infrastructure, software system integration, and overall solutions required by modern service industry, including finance, logistics, online education, media, health care health, tourism, e-government, and e-commerce.

(41) Major next-generation internet technologies and services

Priorities will be to: develop key technologies for high performance core network equipment, transmission equipment, and connecting equipment; develop key technologies for scalability, security, mobility, service quality, and operation management; establish a credible network management system; develop intelligent terminals and household network equipment, and develop broadband related new businesses and applications such as multimedia and network computation.

(42) High performance, dependable computers

Emphasizing the development of computation methods and theories that embody
new concept, efforts will be made to develop new concept-based super trustworthy computer with at least a thousand trillion floating-point operations per second and the next generation server systems, and develop a range of key technologies for innovative system structures, mass storage, and fault tolerance.

(43) Sensor networks and intelligent information processing

Priorities will be assigned to: developing new sensors and technologies for advanced automatic barcode identification, radio frequency tags, and multiple sensor information-based intelligent information processing; developing low-cost sensor networks and real-time information processing systems; and providing more convenient and more powerful information service platforms and environment.

(44) Digital media content platforms

Priorities shall be to develop critical technologies concerning digital media content processing for a range of business sectors, including the cultural and entertainment market, radio and TV broadcasting, and audio-video information services, developing comprehensive media information content platforms featuring easy accessibility, interaction, copyright protection, and effective management.

(45) High definition large flat-panel display

Priorities will be given to developing a range of flat-panel and projection display technologies, including high definition large flat-panel display products, organic electroluminescent display, field emission display, and laser display, with a view to establishing an industrial chain for flat-panel display materials and components.
(46) Core application-oriented information security

Priorities shall be to develop security technologies concerning national infrastructure information network and important information systems, develop novel **coding** technologies for network survival under complex large systems, active real-time protection, safe storage, network virus control, prevention of vicious attacks on web pages, and network credit systems.

7. Population and Health

Building a harmonious society calls for stabilizing a low birth rate, raising population quality, and effectively preventing and controlling major diseases. Controlling population and improving population quality and health all depend on powerful support from science and technology.

Development paths: 1) Birth rate control and population capacity building. Priorities will be given to acquiring key technologies for birth rate monitoring and reproductive health, developing a series of drugs, instruments, and health products for reproductive health to ensure that the country’s population is below 1.5 billion and birth defect rate is below 3%. 2) While adhering to the principle of prevention first and combining health improvement and diseases control and treatment, carry out studies on critical technologies for disease prevention and early diagnosis, thus ensuring markedly improved capability in the diagnosis and prevention and treatment of major diseases. 3) Strengthen **inheritance** and innovation in Traditional Chinese Medicine(TCM) and
promote TCM modernization and internationalization. While inheriting and developing TCM theory, efforts shall be made to establish technical approaches and standard regulatory systems for TCM through technological innovation and multi-disciplinary interaction so as to improve clinical treatment and promote a sound development of TCM.

4) Develop major new drugs and advanced medical equipment. While overcoming key technological snags in developing new drugs, large medical equipment, medicinal materials, and drug release systems, accelerate the establishment of a national technical platform for drug development and propel indigenous innovation in major new drugs and novel medical equipment.

Priority topics:

(47) Safe contraception and family planning, and birth defects prevention and treatment

Priorities will be to develop new technologies and products for safe and effective contraception and for the prevention of sexually transmitted diseases, develop technologies for efficient and safe early screening, test and diagnosis of birth defects and for biological treatment of inherited diseases.

(48) Prevention and treatment of cardiovascular and cerebrovascular diseases, malignancies, and other major non-infectious diseases

Priorities will be given to developing key technologies for early warning and diagnosis of major diseases, including cardiovascular and cerebrovascular diseases and tumors, and for early intervention in disease risk factors while developing key
technologies and solutions for standardized, individualized and integrated treatment.

(49) Prevention and treatment of common, frequently-occurring diseases in urban and rural communities

Priorities will be given to research on and development of technologies for monitoring, preventing, diagnosing, and treating frequently occurring and common diseases in addition to developing compact mobile medical service equipment and distance diagnosis and technical service systems.

(50) Traditional Chinese Medicine: impartation and innovation

Priorities will be given to encouraging innovation in basic TCM theory, and inheriting and tapping on TCM experience, studying TCM diagnosis and therapy and associated assessment techniques and standards, carrying out research on and development of modern TCM and manufacturing technologies. These efforts are designed to protect and utilize TCM resources in an effective and rational manner while strengthening the protection of intellectual property rights and establishing international cooperation platforms.

(51) Advanced medical equipment and bio-medicinal materials

Priorities will be to develop novel therapeutic equipment and conventional diagnostic and therapeutic equipment, digital medical technologies, and individualized medical engineering technologies and equipment in addition to studying nanotechnology-based biological drug release systems and tissue engineering and developing innovative bio-medicinal materials such as including proxy human tissues and organs.
9. Urbanization and City Development

China has entered a phase of rapid urbanization. Urbanization process and coordinated urban development are in earnest need of science and technology.

Development paths: 1) By stressing scientific urban planning in cities and towns, efforts will be made to promote rational layout of urban and rural areas and associated scientific development. Develop key technologies for modern urban planning and dynamic monitoring and control so as to realize an organic combination of urban development planning and regional economic planning in response to the sustaining capacity of regional resources and environment. 2) In light of energy and water efficiency, establish resource saving cities, strive for technological breakthroughs in urban energy efficiency and rational development and utilization of new energy, and develop resource efficient, long durability, green construction materials so in order to raise urban resources and energy efficiency. 3) Raise comprehensive urban management level by strengthening the application of information technology. Develop integrated digital urban management technology in order to establish an efficient, multifunctional, and integrated technical system for urban management. 4) Develop urban ecological residential environment and green building structures and noticeably improve urban living environment by utilizing technologies for hazardless handling and recycling of urban sewages and garbage and developing environment friendly technologies for improving urban residential areas and indoor environment, and noticeably raising the quality of urban living environment.
Priority topics:

(52) Urban planning and dynamic monitoring

Priorities will be set up to develop technologies for urban layout design and system design, and urban infrastructures and public service facilities planning and design. Developing technologies for integrated configuration and associated sharing, and interactive simulating prediction and dynamic monitoring of a range of urban elements, including urban planning, population, resources, environment, and economic development.

(53) Uplifting urban functions and space efficiency

Priorities will be to develop a range of technologies involving urban traffic system, intelligent urban public transit management, urban utility infrastructures, and disaster prevention and mitigation, studying the formation mechanism of urban hot-island effect and artificial control technology. Developing technologies for land mapping and resource saving, simulation prediction of urban spatial changes, and urban underground development and utilization.

(54) Architecture energy efficiency and green buildings

Priorities will be to develop green architecture design technologies, architecture energy-saving technology and equipment, renewable energy devices, and integrated application technology, precision construction technologies and equipment, energy efficiency and green construction materials, and energy efficiency architecture standards.
(55) Urban ecological residential environment and quality control

Priorities shall be given to developing technologies for indoor pollutants monitoring and cleanup, ecological control of urban environment, and recycling of urban garbage, cyclic utilization of water, urban pollution control, minimal emission in residential areas, and intelligent management of ecological residential areas.

(56) Urban information platforms

Priorities will be to develop technologies for sharing urban online information, urban basic data acquisition and updating, urban data consolidation and mining, multidimensional urban construction modeling and simulation, urban dynamic monitoring systems and associated application, standards for urban online information sharing, and urban emergency response services.

10. Public Security

Public security constitutes a footstone for national security and social stability. The country’s public security is facing severe challenges, which in turn raises major strategic demands for scientific and technological support.

Development paths: 1) Strengthen technical support for quick response to and handling of emergency events. With application of information and intelligent technologies at the core, efforts will be made to develop a national public security system featured with multifunction and integrated emergency response support. Establish a public security technical system consisting of scientific prediction, effective prevention and control, and quick response mechanism. 2) Improve the capability of early detection
and prevention. Priorities will be given to studies on technologies for monitoring, warning, and preventing coalmine and other production-related accidents, social emergency events, natural disasters, nuclear safety, and biosecurity. 3) Enhance comprehensive response and rescue capability. Focus shall rest on developing rescue technologies for coalmine disasters, major fires, major natural disasters, leakage of hazardous chemicals, and mass poisoning. 4) Accelerate the modernization of public security equipment and facilities. Develop major equipment for production safety, food safety, biosecurity and public safety, and associated protection products and the relevant industries.

**Priority topics:**

(57) **National public security emergency information platforms**

Priorities will be to develop technologies for all-round and obstacle-free risk source detection and monitoring, precision positioning, and information acquisition. Develop technologies for multi-scale dynamic information analysis and handling, and decision making. Develop integration technology for a national public security emergency command platform and establish an integrated emergency decision-making platform featured with early monitoring, quick advance warning, and efficient handling.

(58) **Major workplace accidents warning and rescue**

Priorities will be to develop pre-warning and control technologies and associated equipment for mine gas, water bursting, power failures, and major industrial accidents, including open burning, explosion, and hazardous leakage.
(59) **Food safety and border entry-exit inspection and quarantine**

Priorities shall be to work on a range of key technologies concerning food safety and entry-exit quarantine related risk assessment, pollutants tracking, safety standard formulation, and quarantine monitoring and testing, and develop intelligent technologies for food contamination prevention and control and high flux quarantine monitoring.

(60) **Major public emergency prevention and quick response**

Priorities will be set to work on technologies involving individual biological characteristic identification, evidence gathering, quick screening, ratification, and simulation prediction, technologies and equipment for distance positioning and tracking, real-time monitoring, evidence identification, and quick handling, fire-fighting in high-rise buildings and underground structures, distance probe of explosives, illegal drugs, and nuclear and biological sources of terrorism, and on-site handling and protection.

(61) **Biosafety measure**

Priorities will be to produce a range of technologies involving fast, sensitive, and specific monitoring and detecting, including technologies capable of detecting in-body toxic chemicals, advanced disinfectors and fast disinfection, hazardous medium identification and control, biological invasion prevention and control, and vaccines, immunoadjuvant, antitoxin, and other drugs.

(62) **Major natural disasters prevention and preparedness**

Priorities will be to develop key technologies for monitoring, warning, and
emergency handling of earthquakes, typhoons, torrential rains, floods, and geological disasters; develop monitoring and warning technologies for forest fire, dam breakage and leakage, and risk assessment techniques for major natural disasters.

11. National defense

IV. Major Special Projects

Historically, the implementation of major special projects represented by A-bomb, H-bomb, satellites, manned space flights, and hybrid rice has played a crucial role in enhancing China’s comprehensive strength. The United States, Europe, Japan, Korea, and others have all made the implementation of major special projects to meet national goals an important measure in raising their national competitiveness.

In the course of defining priority topics in the main areas, a number of major special projects involving strategically important products, critical common technologies, and major engineering projects, are identified in line with national objectives. These major special projects are designed to strive for breakthroughs, taking full advantage of the socialist system in pooling up resources to do big things and the role of the market economy system as well. These major special projects are expected to spring from scientific and technological progress in limited areas to a leapfrogging development in overall productivity while helping fill up the country’s strategic blanks. The basic principles under which major special projects are screened out are as follows:

1) strategic industries that are closely linked to the major demands of the nation’s
economic and social development, capable of coming up with core proprietary intellectual property rights, and having a major impact on indigenous innovative capacity at the enterprise level; 2) key enabling technologies that have an overarching bearing on raising the overall industrial competitiveness; 3) efforts that are aimed at overcoming major bottlenecks to economic and social development; 4) activities that combine both civilian and defense efforts or make defense part of the civilian industry and have a major strategic importance to maintaining national security and strengthening comprehensive national strength; 5) efforts that are in line with the nation’s development status and within the reach of its strength. It is according to the above-mentioned principles that a number of major special projects are selected to address a range of issues involving high tech industry development, traditional industry transformation, bottlenecks to the nation’s economic development, raising people’s health level, and safeguarding national security. These major special projects will be implemented upon a further review and approval case by case in light of ranking priority of the nation’s development requirement and necessary conditions for implementation.

In addition, dynamic readjustment will be made to pace the implementation of these major special projects as determined by the nation’s strategic needs and changing situation. For the major special projects aiming at strategic products, enterprises are expected to be the principal player in terms of research and development and investment. They will start from research on and development of major equipment so as to take advantage of allocating S&T resources through market mechanism while the starting fund appropriated by the state will be mainly used to address key and core technological snags.
Major special projects are major strategic products, critical common technologies, and major engineering projects which are selected for realizing national objectives and must be completed by massing resources and making breakthroughs in core technologies within a set period of time, thus being the top priority in the nation’s science and technology development. The Outline has defined 16 major special projects, including core electronic devices, high-end generic chips and basic software, super large-scale integrated circuit manufacturing technology and associated techniques, the next generation broadband mobile telecommunication, high-end numerically controlled machine tools and basic manufacturing technology, the development of large oil-gas fields and coal-bed methane, large advanced pressurized water reactors and high temperature gas-coolant reactor nuclear power stations, water body contamination control and treatment, new genetically modified varieties, major new drugs, prevention and treatment of major infectious diseases such as HIV/ADIS and viral hepatitis, large passenger aircrafts, high resolution earth observation systems, manned space flights, and the moon probe. The major special projects cover a range of strategic sectors including information and biotechnology, major pressing issues concerning energy, resources, the environment, and public health, dual-use technologies, and defense technologies.

V. Frontier Technologies

Frontier technologies refer to major visionary, pioneering, and exploratory technologies in the realm of high technology. Frontier technologies constitute an important basis on which future high technologies stem out and emerging industries grow. They represent a nation’s comprehensive high-tech innovation capability. Frontier
technologies are selected in accordance with the following principles: 1) representing the development direction of world high-tech frontiers; 2) having a pioneering role in shaping and developing new industries in the future; 3) being conducive to industrial technology upgrading and for realizing the leapfrogging development; and 4) possessing a strong team of talented personnel and a sound R&D basis. Under the above-mentioned principles, a number of frontier technologies will be pre-deployed in an attempt to lead the future S&T development and raise the nation’s high-tech R&D capability and international competitiveness.

1. **Biotechnology**

Biotechnology and life science will become an important force triggering a new round of S&T revolution in the 21st century. Genomics and proteomics studies are leading advances in biotechnology in the direction of systemized research. Genome sequencing and genetic structure analysis have turned in the direction of functional genomic studies and the discovery and application of functional genes. Drugs and animal-plant based directional molecular design and construction have become an important direction for species and drug-related studies. Development and application of frontier technologies, including biochips, stem cells, and tissue engineering, breeds major breakthroughs in diagnosis, therapeutic treatment, and regenerative medicine. Critical breakthroughs are required in the fields of functional genome, proteomics, stem cells, and therapeutic cloning, tissue engineering, biocatalysis, and conversion technologies.

**Frontier technologies:**
(1) **Target identification technology**

Target identification is important for developing new drugs, biodiagnostics, and biotreatment. Efforts shall be focused on studying scale identification of key genetic functions and their regulatory networks in the physiological and pathological process, making breakthroughs in techniques for identification of functions of disease-causing genes, expression manipulation, target screening, and verification, and innovative new drug manufacturing from “gene to drug”.

(2) **Plant-animal varieties and drug molecular design technology**

Plant-animal species and drug molecular design technology is made up of molecule docking, molecule simulation, and molecule design based on biomacromolecules’ 3-D structures. Priorities shall be given to studying protein and dynamic cellular process and associated bioinformatic analysis, consolidation, and simulation. Develop virtual plant-animal species and drug design technology, simulation technology for plant-animal species growth and pharmaceutical metabolism engineering, computer aided composite bank design, synthesizing, and screening.

(3) **Gene manipulation and protein engineering technology**

Gene manipulation technology is a key link to the utilization of genetic resources. Protein engineering constitutes an important approach to efficient utilization of genetic products. Efforts will be focused on developing technologies for highly effective expression and regulation, chromosome structuring and positioning, coded protein gene design and transformation technology, protein peptide chain decoration and restructuring
technology, protein structure analyzing technology, and scale protein isolation and purification technology.

(4) Stem cell based human tissue engineering technology

Stem cell technology is a process that can be used to develop in-vitro stem cells, or harvest different tissues or cells clinically needed through directional induced differentiation or isolation. It also can construct in-vitro human organs for replacement and repairing treatment. Priorities shall be to develop therapeutic cloning technology, in-vitro stem cells construction and directional induction technology, in-vitro human tissue construction and associated scale production technology, multiple human cell-based sophisticated tissue construction and dysfunction repairing technology, and biomanufacturing technology.

(5) New-generation Industrial biotechnology

Biocatalysis and biotransformation constitute the mainstream of the new generation industrial biotechnology. Priorities will be to develop scale screening technology for functional strains, directional biocatalyst upgrading technology, biocatalysis technology system for scale industrial production, clean transformation media manufacturing technology, and associated industrialized transformation process.

2. Information Technology

As information technology will continue to develop in the direction of high performance, low-cost, pervasive computation, and intelligent process, seeking new and
innovative computing and processing approaches and associated physical realization represents a major for the future development of information technology. The crossing and integration of nanotechnology, biotechnology, and cognitive science will induce advances in information technology that are human-centered, image and natural language comprehension-based, and featuring biological characteristics, thus promoting innovation in numerous fields. Priorities will be to develop low-cost ad hoc networks, individualized intelligent robots and human-machine interactive systems, high-flexibility attack free data networks, and advanced information security systems.

**Frontier technologies:**

(6) **Intelligent sensing technology**

Research will be focused on intelligent information processing and control technologies based on biological characteristics and image and natural language comprehension and centered on humans, while developing processing systems for Chinese language information, systematic technologies involving biological characteristics identification, and intelligent traffic systems.

(7) **Ad hoc network technology**

Priorities will be to develop technologies for ad hoc mobile networks, ad hoc computing networks, ad hoc storage networks, and ad hoc sensor networks, low-cost real-time information processing systems, multi-sensor information integration, individualized interactive interface, high-flexibility attack free data networks, advanced information security systems, and ad hoc intelligent system and intelligent personal system.
(8) Virtual reality technology

Research will be focused on technologies for integrating different disciplines, including electronics, psychology, cybernetics, computer graphics, database design, real-time distribution system, and multimedia technology in addition to studying virtual reality technologies and associated systems for related fields, including medicine, entertainment, arts, education, military affairs, and industrial manufacturing management.

3. Advanced Materials Technology

Advanced material technology will go for composite structural functions, intelligent functional materials, integration of materials and components, and environment-friendly manufacturing and applications. Efforts will be made in seeking breakthroughs in material design, assessing, and characterizing, and in advanced manufacturing and processing technologies. Based on studies in nano-science, develop nanomaterials and nanocomponents, special functional materials such as superconductor materials, intelligent materials, energy materials, super structural materials, and new generation optoelectronic information materials.

Frontier technologies:

(9) Intelligent materials and structural technology

Intelligent materials and intelligent structures constitute a smart or intelligent structural systems that integrate sensors, control, and drive (execution) and other
functions. Priorities will be to develop technologies for intelligent material manufacturing and processing, intelligent structure design and manufacturing, key equipment monitoring, and failure control.

(10) High-temperature superconducting technology

Research will be focused on novel high-temperature superconducting materials and associated manufacturing technology, superconducting cables, superconducting motors, and high performance superconducting electric devices while studying a range of sensitive detecting devices such as superconducting biomedical elements, high-temperature superconducting filters, high-temperature superconducting injury-free detectors, and scanning magnetic microscopes.

(11) Efficient energy material technology

Research will be focused on critical technologies for solar cell related materials and associated key technologies, critical technologies for fuel cell materials, high volume hydrogen storage material technology, efficient rechargeable cell materials and associated key technologies, key super capacitor materials and associated manufacturing technology, and efficient energy conversion and storage material systems.

4. Advanced Manufacturing Technology

Advanced manufacturing technology will be increasingly based on information, extremism, and environmental friendliness. Such a tendency will create a foundation on which future manufacturing industry will survive, and a key link to its sustainable
development. Efforts will be focused on overcoming difficulties in extreme manufacturing technology, system integration, coordination technology, intelligent manufacturing and application technology, set equipment and system design and verification technology, high reliability-based large sophisticated systems and equipment design technology.

**Frontier technologies:**

(12) **Extreme manufacturing technology**

Extreme manufacturing refers to the manufacturing components or functional systems at an extreme scale (extremely large or extremely small) or with extremely powerful functions under extreme conditions or environment. Research will be focused on design, manufacturing, and test technologies for micro and nanometer electro-mechanic systems, and technologies for micro and nanometer manufacturing, super precision manufacturing, giant system manufacturing, and intense field manufacturing.

(13) **Intelligent service robots**

An intelligent service robot is an intelligent equipment integrated with a number of high-tech elements, able to provide diverse services needed by humans, in a non-structural environment. The focus will be on service robots and dangerous operation robots in order to study common basic technologies, including design approaches, manufacturing techniques, intelligent control, and application system integration.

(14) **Service life prediction technology for major products and facilities**
Service life prediction technology for major products and facilities represents a key technology for improving operational reliability, safety, and maintainability. Efforts will be made to study prediction control and optimization technology for elements design for components and prototyping process, knowledge-based prototyping and simulation technology, onsite manufacturing process test and evaluation technology, component service life prediction technology, and reliability, safety, and service life prediction technology for major products, complex systems, and large facilities.

5. **Advanced Energy Technology**

Advances in energy technology in the future will mainly be characterized with cost-effectiveness, efficiency, and clean utilization in addition to novel energy sources. Technology development with respect to the fourth generation nuclear energy system, advanced nuclear fuel cycle, and fusion energy has drawn increasing attention. Hydrogen, an ideal energy carrier that can be obtained through diverse approaches, will bring about new changes for clean energy utilization. Fuel cell and distributive energy supply technology, featured with cleanliness and flexibility, will eventually become an important form of terminal energy application. Research efforts will be focused on hydrogen utilization and distributive energy systems, advanced nuclear energy, and fuel cycle technology in addition to developing technologies for fossil fuel energy utilization, featured with efficiency, cleanliness, and near-zero emissions, and low-cost and efficient new renewable energy applications.

**Frontier technologies:**
(15) Hydrogen and fuel cell technology

Research efforts will focus on technologies for making hydrogen through the use of efficient low-cost fossil fuel energy and renewable energy, cost-effective hydrogen storage and transport, technologies for manufacturing basic key fuel cell components, thermopile integration, fuel cell applications to power generation and automobile propulsion systems. Efforts will also be made to develop technical standards for hydrogen energy and fuel cell technology.

(16) Distributive energy supply technology

Distributive energy supply technology constitutes an important means of providing comprehensive energy services featured with flexibility and energy efficiency. The focus will be on mastering technologies for fossil fuel-based mini gas turbines and energy conversion such as innovative thermal cycle, energy storage, and triple-generation technology, with view to establishing renewable energy based distributive terminal energy supply systems made up of mini gas turbines and fuel cells, supplemented by fossil fuel energy.

(17) Fast neutron reactor technology

A fast neutron reactor is a nuclear reactor where fission chain reaction is triggered by fast neutrons to realize nuclear fuel breeding. It is capable of full utilization of uranium resource in addition to handling long-life span radioactive wastes. Conduct research on and master fast neutron reactor design and core technologies, nuclear fuel and structural materials, while striving for major technological breakthroughs in sodium cycle,
developing a 65MW experimental fast reactor for critical and grid power generation.

(18) Contained magnetic fusion technology

Taking advantage of participating in research on and construction of the International Thermal-nuclear Experimental Reactor project, focus our research on technologies concerning large superconducting magnets, microwave heating and driving, neutral beam injection heating, blanketing, large real-time tritium isolation and purification, diverters, numerical modeling, plasma control and diagnosis, and key materials for an experimental reactor. Deepen the study of high-temperature plasma physics and exploring non-Tokamak approaches for some energy applications.

6. Marine Technology

More attention will be given to developing comprehensive marine development technology featured with multifunction, multi-parameter, and long lasting operation in order to raise the nation’s comprehensive technological level of deep-sea operations. Research will focus on developing technologies involving natural gas hydrates exploitation, sea-floor metal and mineral resources gathering and transport, on-site extraction, and large marine engineering projects.

Frontier technologies:

(19) 3-D marine environment monitoring technology

3-D marine environment monitoring is a technology designed for synchronized
monitoring of marine environmental elements from space, offshore stations, water surface, and in-water. Research will be focused on remote marine sensing technology, acoustic probe technology, buoy technology, shore-based long-range radar technology, and marine information processing and application technology.

(20) **Ocean floor-based multi-parameter fast sounding technology**

Sea-floor based multi-parameter sounding is a technology for synchronized collection of different parameters, including sea-floor geophysics, geochemistry, and biochemicals, capable of transmitting information and data on a real-time basis. Research priority will be on sensor technology, automatic sensor positioning technology, and sea-floor information transmission technology under abnormal environment and conditions.

(21) **Natural gas hydrates exploitation technology**

Natural gas hydrate is a **carbon nitrate** bedded at the deep seafloor or underground. Research will focus on prospecting theory and exploitation technology for such a compound, geophysics and geochemistry based gas hydrate prospecting and assessing technology. Strive for breakthroughs in gas hydrate drilling technology and safe mining technology.

(22) **Deep-ocean operation technology**

Deep-ocean operation technology is an under-water process for deep seafloor engineering operation and mining activities. Research focus will be on underwater carrying technology at a large depth, life maintaining system technology, high-power dynamic device technology, high fidelity sample collection and distance information...
transmission technology, deep-sea operational equipment manufacturing technology, and
deep-sea space station technology.

7. Lasers Technology

7. Aerospace Technology

VI. Basic Research

Basic research constitutes an important source for high-tech development, a cradle
for nurturing innovative personnel, a foundation for building an advanced culture, and an
inner driving force for the future S&T development through profound understanding of
natural phenomena, unveiling natural laws, and acquiring new knowledge, new principles,
and new methodology. The development of basic research shall adhere to the principle of
combining meeting the national objectives and encouraging free exploration. In addition,
基本 research activities shall observe the law of scientific development, respect
scientists’ exploratory spirit, and pay more attention to the long term value of sciences,
with stabilized support, visionary deployment, and dynamic readjustment in line with
new trends of scientific development. The Outline has made deployment in four major
areas, involving basic and major scientific research activities that are in line with
disciplinary development, scientific frontiers, and major national strategic demands.

1. Disciplinary Development
An overall deployment is made for basic disciplines, taking into account a range of characteristics of basic research activities, including long term efforts for limited breakthroughs, exploratory nature, and difficulties in predicting progress. The deployment is made as such that different disciplines are allowed to cross and infiltrate one another in an effort to bring out new growing points for disciplines. It is expected that long-term and in-depth academic studies and accumulations will eventually lead to improved capability in original innovation and to advancing coordinated multi-discipline based development.

(1) Basic disciplines

Pay more attention to capacity building in basic theories and disciplines, with a coordinated development of mathematics, physics, chemistry, astronomy, earth sciences, and biology.

(2) Cross and emerging disciplines

Encourage interweaving and melting between basic disciplines, between basic disciplines and applied disciplines, and between natural science and social science. Such a combination, more often than not, will lead to the birth of major scientific discoveries and new disciplines. It is one of the most active parts in scientific research. In this context, it is worth a raised attention and well-thought deployment.

2. Frontier Scientific Issues

The unity of micro and universal worlds, the combination of Reductionism and
Entirety, the interwoven multidisciplinary practice, the infiltration of basic sciences such as mathematics into diverse other areas, and application of advanced technologies and means, all hallmark the major characteristics of modern frontier scientific development. They are conceived with major scientific breakthroughs, which makes people’s knowledge of objective world deeper and better. Frontier scientific issues are selected in line with the following principles: having a spurring role for the development of basic sciences, having a solid foundation, able to make a full display of China’s strength and specialty, and desirable for raising China’s international position in basic sciences.

(1) Quantitative study and systematic integration of life process

Main research directions: gene language and regulation, model biology, epigenetics, untranslated RNA, life structural function and regulation network, life reconstruction, bioinformatics, computational biology, life characteristics in extreme environment, origin and evolution of life, systematic development, and evolutionary biology.

(2) Condensed matters and novel effects

Main research directions: strongly correlated systems, soft condensed matters, condensed matters of novel quantum properties, self-similar cooperative growth, Open Complex Giant System (OCGS), Bose-Einstein Condensation, superfluid-superconducting mechanism, structural phase transformation emissions, condensed matters under extreme conditions, electronic structure, and diverse primary excitation processes.

(3) Matters’ deep inner structures and physical laws at cosmological scale
Main research directions: matter structures and physical laws at micro or universal scale and under extreme conditions, such as high-energy, high-density, super high pressure, and super intense magnetic field, the theory of unifying all physical laws, basic frontier issues of particle physics, substances of dark matter and dark energy, origin and evolution of the universe, formation and evolution of black holes and diverse celestial bodies and structures, impacts of solar activities on earth environment and disasters and associated prediction.

(4) Core mathematics and its application in cross disciplines

Main research directions: major issues concerning core mathematics, intercrossing between mathematics and other disciplines, and new mathematic problems in scientific research and practical applications such as discrete problems, random problems, quantum problems, and mathematical theories and methodologies in a range of non-linear problems.

(5) Earth system process and associated resources, environment, and disaster effects

Main research directions: interactions between different earth systems (atmosphere, hydrosphere, biosphere, earth crust, mantle and core), in-depth earth drilling, physical, chemical, and biological processes in the earth system and associated resources, environment, and disasters effects, theory of continental and marine origin of mineral reserves, land, sea, air, and space based earth observation and probe systems, earth simulation systems, and earth system theory.

(6) Chemical processes in creating and transforming new matters
Main research directions: function design, controllable synthesis, preparation and transformation of new specific molecules of defined structures, condensed molecules, and polymeric molecules, environment friendly new chemistry system, formation and transformation of matters at different temporal and spatial scales, relationship between chemical properties, performance, and structures of complex systems such as life process and ecological environment, and associated rules for transformation.

(7) **Brain and cognitive sciences**

Main research directions: cellular and molecular mechanism of brain functions, genesis and development mechanism of major brain diseases, relationship between brain development, plasticity and human intelligence, the process of higher cognitive functions, including learning memory and thinking, and associated neuroscience basis, expression of brain information and brain-like information processing system, and dialogue between human brain and computer.

(8) **Innovation in scientific experiments, observational methods, techniques, and equipment**

Main research directions: life science related tests, imaging, analysis, and manipulation, featured with dynamic, timing, no-injury, sensitivity, and high definition; new technologies for acquiring matter composition, function, and structure related information, and associated characterizing technology, new observational means and approaches for information acquisition in earth and space research.

3. **Basic Research in Response to Major National Strategic Needs**
A knowledge based society has intense needs for the development of science. The competition for comprehensive national strength appeals to basic research with an ascending tendency. Being a developing nation enjoying fast economic growth make it all the more necessary to stress that basic research must serve to meet the national objectives and help address key and bottleneck issues in future development. In this context, basic research directions are defined according to the following principles: having strategic, overall, and long term importance to the national economic and social development and to the national security; capable of playing a critical role in future development; and able to result in a combination of basic sciences and technology sciences, thus leading the future high tech development.

(1) Biological foundations of human health and diseases

Priorities will be selected to study the genesis and development process of major diseases, and associated molecular and cellular basis for interference; the role of nervous system, immune system, and endocrine system in health and major diseases; dissemination and mutation of pathogens and associated diseases causing mechanism; drug effects at molecular, cellular, and co-regulating levels; interference of environment in physiological process; and theoretical system of traditional Chinese medicine.

(2) Crop genetic improvement and scientific issues in sustainable agricultural development

Priorities shall be given to studying crop genes, functional genomes, and the alike; biodiversity and genetic basis for new species breeding; crop stress resistance and
mechanism for efficient utilization of moisture, nutrients, and sunshine; interactions between crops and ecological environment; and agro-biological safety and principles of major crop diseases control.

(3) **Human activities and their impact on the Earth system**

Research will be focused on disaster and risk prediction for resources prospecting and development activities; extensive human activities in major river basins and their ecological implications, adaptability, and regional ecological safety; energy cycle of major ecosystems and associated regulation; biodiversity protection models; land use and changes in land cover; regional water demand and ecological equilibrium; genesis of environmental pollution and control principles; and sustainable marine resources utilization and marine ecological environment protection.

(4) **Global change and regional response**

Priorities will be given to studying global climate change and its impact on China; large scale hydrological cycle and its response to global change; global change and its impact on regional water resources; interactions between human activities and monsoon systems; sea-land-air interactions and mutation of Asian monsoon systems and associated prediction; carbon cycle process in China’s offshore-land ecosystem; the Qinghai-Tibet Plateau and polar regions and their response to global change, and associated climate and environment effects; climate system modeling and associated simulation and prediction; greenhouse effect and associated mechanism; genesis and evolution of aerosols and its impacts on climate change, and associated control.
(5) Complex systems, disaster formation, prediction, and control

Research will focus on the relationship between micro-mechanisms and macro-phenomena in engineering projects, nature, and socioeconomic complex systems; mechanism and evolution of structure formation, and relationship between structure and system behavior in a complex system; movement of complex systems and associated system mutation and regulation; relativity between behaviors at different scales in a complex system, and new theory and methodology concerning complex systems.

(6) Key scientific issues in sustainable energy development

Research will be focused on the physical and chemical basis of efficient and clean fossil fuel energy utilization and transformation; high performance thermal energy transformation and key scientific issues in efficient energy storage; scale utilization of renewable energy and associated principles and new approaches; theory of safe, stable, and economic operation of power grids; and scientific basis of large-scale basic nuclear energy technologies and hydrogen technology.

(7) New principles and methodologies for materials design and fabrication

Priorities will be given to studying the physical and chemical basis of optimizing basic materials; phase change and structure control mechanism; principles of multi-enhanced treatment; physical and chemical properties of new materials; new physical mechanisms, new effects, and new material design, including artificial structures, minimization, and multifunction based integration; new principles and techniques of material manufacturing; new principles of structure and performance characterizing; interactions between material service and the environment and associated performance
evolution, failure mechanism, and service life prediction.

(8) Scientific basis of manufacturing under extreme environmental conditions

Research will focus on deep matters and energy interactions; micro-scale transmission of high-density energy and matters; precision expression and measuring of micro-structural shape; scale effects on manufacturing prototyping, property formation and system integration and associated interfacing science; smooth movement certainty of a complex manufacturing system, and uniqueness of manufacturing subjects.

(9) Major mechanical issues in aeronautics and space science

Priorities shall be placed on studying the mechanical issues involving supersonic propulsion systems and super high-speed collision; multidimensional propulsion systems and theory of complex movement control; theory of compressible turbulent flows; high temperature thermodynamics; magnetic fluid and plasma dynamics; microfluid and microsystem dynamics; and structural dynamics of new materials.

(10) Scientific basis for the development of information technology

Priorities will be given to studying new algorithms and basic software theory; mechanisms of virtual computation environment; theory and methods for mass information processing and knowledge mining; interactive theory; network security and credible and controllable information security theory.

4. Major Scientific Research Programs
Four major scientific research programs are identified and deployed in line with the world S&T development trends and China’s major national strategic needs. These programs are qualified for playing a strong role in S&T development, triggering a rapid improvement of sustainable innovation capacity, and possessing a high-caliber research contingent. Breakthroughs in these directions will noticeably raise the nation’s international competitiveness, advance its sustainable development, and realize leapfrogging development in selected areas.

(1) Protein studies

Protein is a principal carrier of life activities and an executor of different functions. An in-depth study of protein’s diverse sophisticated structures and functions, interactions and dynamic changes can unveil the nature of life phenomena at molecular, cellular, and biological levels, which constitute the main mission for the post-genome era. In the meantime, protein-related research findings will result in a range of new biotechnological activities, spur up the development of pharmacy, agriculture, and the so-called “green industry”, and lead the future development of bioeconomy. In this context, protein study is an area of life science that sees fierce competition among developed nations.

Research will be focused on transcriptomics, proteomics, metabolomics, structural biology, biological functions of proteins and associated interactions, protein-related computational biology and systems biology, methodologies for protein research, and relevant applied basic research.

(2) Quantum regulation studies
Microelectronics-based information technology will soon reach its limit. Hence, the development of information technology is facing severe challenges: mankind has to find a new way out. In this context, quantum effects-based new information means brings up a new hope, and has become a new competition target among the developed nations. The so-called quantum manipulation explores new quantum information, and develops a range of related sciences, including quantum informatics, correlated electronics, quantum communication, confined small-scale quantum system and artificial photonic crystal. These will constitute a theoretical basis for the future information technology development. As a visionary discipline, quantum technology may produce an inestimable impact on the economic and social development over the next 20 to 30 years.

Priorities will be to study carriers of quantum communication and associated manipulation principles and methodologies; quantum computation, charge-spin-phase-trajectory relevancy, and new quantum manipulation methods; new quantum effects of confined small scale quantum system; macro quantum effects of photonic material; and new principles and technical basis for quantum manipulation characterizing and measuring.

(3) Nanometer studies

Matters at a nanometer scale can produce a bizarre phenomenon or rule, which will eventually change the existing framework of relevant theories, allowing people to have a brand new knowledge of the matter world. This, in turn, will give birth to a new technology revolution, and create huge development space for materials, information, green manufacturing, biology, and medicine. Nanoscience and nanotechnology have
become a strategic alternative for raising a nation’s core competitiveness. It is also one of the areas where China expects to realize the leapfrogging development.

Research will be focused on controllable preparation and self-assembly of nanomaterials and associated functionality; nanomaterial structure, special properties, and manipulation mechanism; principles of nanoprocessing and associated integration; conceptual and principle-demonstrating nanocomponents; nanoelectronics, nanobiology, nanomedicine; optical, electronic, and magnetic properties of molecular aggregates and biomolecules, and associated information transmission; single molecule behavior and associated manipulation; molecular machine design, assembly, and control; characterizing and measuring at a nanoscale; and applications of nanomaterials and nanotechnology in the fields of energy, the environment, information, and medicine.

(4) Growth and reproduction studies

A range of eye-catching scientific accomplishments, including animal cloning and stem cells, has brought about huge opportunities for the future development of life and medical sciences. However, most of these findings remain unready to directly serve humans as a result of lacking a systematic and in-depth knowledge of reproduction and development process and associated mechanisms. China has a high population growth rate and a high birth defect rate. Confronted with a serious shortage of replacement organs, compounded by the coming peak of an aging population, the nation is in dire need of breakthroughs and technological innovation in reproduction and growth-related theories.
Research will focus on stem cell breeding, isolation, and manipulation; generation, maturity, and fertilization of reproductive cells; manipulation mechanism for fetus development; somatic dedifferentiation and animal cloning mechanism; degeneration of human reproductive functions and regressive mechanism; and safety and ethics of aided reproduction and stem cells technology.

VII. Reform of the S&T System and the Construction of a National Innovation System

Since the introduction of the policy of reform and opening up, the nation’s S&T system reform has made important breakthroughs and substantial strides as it has strictly positioned around forging close links with the economy, aimed at strengthening technological innovation and conversion and industrialization of S&T achievements, stressed structural realignment and mechanism shift, and adopted a series of major reformative measures. Nevertheless, one has to be keenly aware that China’s existing S&T system remains inadequate in meeting the needs of the socialist market economy and that of greater economic and S&T development. First, our enterprises are yet to become a principal player in technological innovation as their innovative capability remains weak. Second, the S&T sector is compartmentalized, resulting in dispersion and duplication of efforts and low overall performance level. S&T innovation capability in the public good sector is especially weak. Third, S&T management at the macro level is terribly uncoordinated, with an S&T resources allocation pattern and evaluation system falling short of accommodating the needs for the new S&T development and government mandate shift. Fourth, mechanisms for rewarding outstanding personnel and encouraging
innovation and pioneering activities are not yet consummate. These problems have seriously compromised the nation’s innovation capacity building.

Guiding thoughts for deepening the S&T system reform are defined as follows: promoting the full-fledged construction of a national innovation system with Chinese characteristics, focusing on S&T resources distribution efficiency and comprehensive integration, and effecting a breakthrough in building an enterprise-centered technological innovation system featuring the integration of industry, academia, and research, so as to greatly advance the construction of a uniquely Chinese national innovation system and drastically enhance the nation’s indigenous innovation capability.

At present and over a period of time in the future, the S&T system reform will strive to accomplish the following major missions:

1 · Supporting and Encouraging Enterprises to Become the Main Player in Technological Innovation

Market competition is an important driving force behind technological innovation while technological innovation is the ultimate route to enhanced enterprise competitiveness. Along with deepened reform and opening up, Chinese enterprises are playing an increasingly important role in technological innovation. To substantially enhance the motivity and vitality of technological innovation at the enterprise level, more agreeable conditions need to be provided, a better environment created, and reforms deepened.
Firstly, let economic and S&T policies play a guiding role in order to enable enterprises to become the major R&D spender. Efforts must be accelerated to create a unified, open, competitive, and orderly environment for the market economy by way of fiscal, taxation, and monetary policies so that enterprises, particularly large enterprises, are induced into increasing their R&D spending and establishing their own R&D bodies. National engineering laboratories and sectoral engineering centers should be established at transformed research institutes or large enterprises possessing fairly strong R&D and technology spin-off capabilities, in collaboration with universities and research institutes. Encourage technology innovation consortia of various forms initiated by enterprises, in collaboration with universities and research institutes, for the purpose of technology innovation capacity building. Secondly, reform the modality of S&T programs to enable enterprises to undertake national R&D missions. National S&T programs shall reflect more of the major industrial needs for science and technology, and attract more enterprises to be part of such programs. In the fields of obvious market application prospects, establish an enterprise-led mechanism with the involvement of universities and research institutes. Thirdly, perfect the technology transfer mechanism to facilitate the integration and application of industrial technologies. Establish and perfect intellectual property rights related incentive mechanism, and an IPR trading system. Vigorously develop various kinds of S&T intermediary service organizations to meet the needs of enterprises, facilitating knowledge flow and technology transfer between enterprises, and between enterprises and universities and research institutes. National key laboratories and engineering (technology research) centers shall be made more accessible to enterprises. Fourthly, accelerate the establishment of a modern enterprise system so as to enhance the
innate drive for enterprise technology innovation. Technology innovation capacity building shall be taken as important indicator in measuring the performance of state-owned enterprises while technology factor-based distribution be made an important part of property rights reform destined for the high-tech industry. Stick to the direction in which application-oriented R&D institutes are transformed into enterprises and deepen the reform of property rights at such institutes. This will not only lead to an improved management system and the establishment of a rational and effective incentive mechanism, but will also enable the transformed R&D institutes to play a major role in high technology industrialization and sectoral technology innovation. Fifthly, create a fine innovation environment to spur innovative activities at small- and medium-sized enterprises (SMEs). As SMEs, particularly technology-based SMEs, are highly innovative but frail in risk-taking ventures, a more favorable policy environment should be created for such enterprises by drafting and formulating preferential laws and policies, particularly in the context of market accessibility and anti-unfair competition. Vigorously develop an S&T investment and financing system and a venture capital mechanism and quicken the construction of S&T intermediary service bodies, so as serve the needs for technology innovation at SMEs.

3. Deepening Institutional Reform and establishing a Modern Research Institute System

Research institutes engaged in basic research, frontier technology development, and public good research constitute a major force in the nation’s S&T innovation activities. Establish a stable, high caliber research contingent that serves national
objectives and is devoted to S&T undertakings is crucial for the future and destiny the nation’s S&T enterprise. Thanks to efforts in restructuring and personnel diversion, a number of high quality research institutions have merged, to which stable support from the government is critical. While giving ample scope to the important roles played by these research institutes, innovation capacity building must be taken as an objective, mechanism improvement a focal point, management system reform deepened, so as to accelerate the establishment of a modern research institute system under the principle of “clearly defined terms of reference, scientific evaluation, orderly open access, and regulated management”.

Firstly, strengthen the capacity building of research institutes in keeping with the terms of reference defined by the state. Earnest efforts must be made to address the problem where some research institutes suffer from undefined terms of reference, uncoordinated research efforts, and weak innovative capability. The allocation of resources should be optimized in order to make concerted efforts in creating disciplines and research bases with clear superiority. Public good research institutes shall take advantage of technical strength in their respective fields, raising S&T innovation and service capability, and addressing major S&T issues in the social development. Basic science and frontier technology-oriented research institutes shall take advantage of their disciplinary strength in uplifting research levels, striving for theoretical innovation and technology breakthroughs, and addressing major S&T issues. Secondly, establishing a stable S&T investment mechanism designed to support innovation activities at research institutes. Given the fact that disciplinary capacity building and major innovation achievements are the results of tireless efforts over a long period of time, state treasury
should provide fairly stable appropriation support to research institutes engaged in basic research, frontier technology development, and public good research. Per capita overhead expenditure level will be raised in line with different types of research institutes in support of disciplinary capacity building, basic research activities, and cultivation of talented S&T personnel. Thirdly, establish an operational mechanism conducive to original innovation at research institutes. Freely selected research topics are extremely crucial for raising the original innovation capability and for nurturing high caliber personnel. The support for free research topic selection based research should therefore be strengthened. While perfecting the system under which the director assumes all power and responsibility at research institutes, delegate more autonomous decision-making power to research institutes in S&T expenditure and personnel affairs so as to ensure greater capability in coordinating and integrating innovation activities at the institute level. Fourthly, work will be carried out to establish a system to assess the overall innovation capability of research institutes. Accordingly, a scientific and rational system will be established to make an overall assessment of institutional innovation capability in terms of the quality of S&T achievements, the buildup of S&T talents, and management/operation mechanisms, in order to raise the management level and enhance innovation capability. Fifthly, efforts will be made to put in place an effective mechanism for opening up and collaboration. Establish a personnel management system featuring the combination of permanent staff and temporary or contract personnel by introducing a retainer and vacancy management mechanism for full-fledged open recruitment of research and management personnel. For the purpose of promoting knowledge flow, personnel mobility, and S&T resource sharing, effective mechanisms should be put in place to facilitate various forms of collaboration between research institutes, enterprises,
and universities.

Universities are not only an important base for nurturing high caliber innovative talents but also a principal player in basic research and original technology innovation activities and a commendable force in addressing major S&T issues in the national economy, materializing technology transfer, and effecting technology spin-off and commercialization. Accelerating the establishment of high caliber universities, particularly world-class research universities, is a prerequisite for enhancing the nation’s S&T innovation and establishing a national innovation system. At present, our country has already built a number of high-caliber universities with appropriate scales, comprehensive disciplines, and assembled talents, and these universities should be given full scope for their important roles in S&T innovation.

Vigorous support and encouragement need to be provided for university-based original innovation in basic research, frontier technology development, and public good research. Universities should be encouraged to enter full-fledged cooperation with enterprises and research institutes so that they can provide better and more extensive services to economic development at the national, regional, and sectoral levels. The capacity building of major academic disciplines and S&T innovation platforms at universities will be accelerated in order to nurture and assemble a number of world-class academic leaders and build up a faculty contingent with high ethical standards, strong innovative spirit, and international competitiveness. Further accelerate the reform of university internal management system by optimizing education structure, S&T related organizational structure, and innovation mechanism and associated management system.
Establish a scientific, rational evaluation system and an operational mechanism conducive to the nurturing of high quality talents and the improvement of innovative capability, so that every talent finds ample scope for his abilities and a constant stream of talents is sustained. Vigorous efforts should be made to explore ways and means of building a modern university system with Chinese characteristics.

3. Advancing the S&T Management System Reform

In view of the protuberant problems in our country’s S&T management at the macro level, the reform of the S&T management system must be advanced, and be centered on improving the national S&T decision-making mechanism, overcoming systemic and institutional barriers, strengthening inter-ministerial, inter-province, ministry/province, defense/civilian overall planning and coordination, so that our ability can be substantially enhanced in mustering S&T resources for initiating major S&T undertakings.

Firstly, a national S&T decision-making mechanism should be created and then constantly improved. The business discussions procedures for the nation’s major S&T decision-making should be improved so that a normative consultation and decision-making mechanism is in place. Efforts should be made to expand government roles in overall configuration and macro management of S&T development, strengthen coordination in formulating major S&T policies, implementing major S&T programs, and in constructing S&T infrastructures. Secondly, establish and improve a macro S&T coordination mechanism at the national level. Define the basic status of S&T policies as a
national public policy and develop an interactive policy coordination system between national S&T policies and national economic policies, in response to the objectives of promoting S&T innovation and indigenous innovation capability. Create a mechanism to coordinate inter-agency allocation of S&T resources. Accelerate government mandate shift at the government agencies in charge of S&T management, practice governance according to the law, and upgrade the macro management and service level. Ways by which programs are managed must be improved to bring into full play the role of government agencies and local authorities in program management and project implementation. Thirdly, the S&T review and evaluation system must be reformed to reflect principle of fairness, impartiality, openness, and encouraging competition, thereby creating conditions for the springing up of various types of talented people, especially the young. The review of major projects must be brought in line with national objectives. The peer review system should be improved by creating a reviewer credibility system and a review mechanism involving international peers, by strengthening the supervision of the review process, and by expanding the openness of review activities and ensuring reviewees’ access to appropriate information. Special attention and support shall be given to highly innovative small projects, uncommon projects, and interdisciplinary projects, with emphasis on the evaluation of quality, capability, and research level of individuals or teams, and on whether it is encouraging original innovation. Establish an independent review system to evaluate the implementation of major national S&T programs, the Knowledge Innovation Program(KIP), and projects funded by the National Natural Science Foundation. Fourthly, reform the S&T achievements evaluation and award system. Perfect the research assessment and indicator systems in light of different characteristics of S&T innovation activities and in accordance with the principle of
openness, fairness, rule abiding, and streamlined procedures. Avert excessive evaluation or desires for quick success and short-term behavior. For innovation activities involving market-oriented applied research and experiments, evaluation shall be conducted mainly on the obtaining of proprietary intellectual property rights and the contribution to industrial competitiveness. Public good research activities shall be evaluated in line with public needs and social benefits derived, while basic research and frontier scientific exploration shall be evaluated in line with scientific significance and academic value. Establish a personnel assessment system capable of judging personnel qualifications in different S&T fields. Reform the national S&T award system by reducing the number and levels of awards. Give prominence to government conferred awards by focusing on talented individuals while rewarding prize-winning projects. In addition, the creation of non-governmental awards should be encouraged and regulated.

4. Vigorously Pushing Forward the Construction of a National Innovation System with Chinese Characteristics

The objective for deepening S&T system reform is to advance and enhance the construction of a national innovation system. The national innovation system is a government-led public system which gives full play to the basic role of the market in resource allocation while letting various innovation players forge close links and interact with one another. Currently, the construction of the national innovation system with Chinese characteristics shall emphasize the following:

Firstly, build an enterprise-led technology innovation system featuring the
combination of enterprises, universities, and research institutes, which will be a breakthrough point for the full-fledged construction of the national innovation. Only when such a system is led by enterprises, it can ensure the market orientation of technology innovation and effectively combine industry-university-research strengths for the enhancement of national competitiveness. Only when enterprises, universities, and research institutes work together, can S&T resources be efficiently allocated, the vitality of research institutes be activated, and enterprises acquire capabilities in sustaining innovation. While drastically improving enterprises’ technology innovation capability, it is imperative to establish new mechanism allowing research institutes and universities to provide services tailored to the needs of enterprises’ technology innovation activities.

Secondly, with creating an open, mobile, competitive, and collaborative operational mechanism at the core, efforts should be made to promote the collaboration and resource sharing between research institutes and with universities. Strengthen the construction of public good scientific research system. Develop research universities and a number of top-notch, resource sharing basic science and frontier technology bases. Thirdly, establish a national defense S&T innovation system highlighting the combination of both the defense and civilian needs as well as a civilianized defense industry by making defense S&T part of the civilian operations. Promote the close combination of civilian and defense S&T findings in a range of areas, including macro management, development strategies and planning, R&D activities, and commercial applications of S&T findings. Strengthen the development of dual-use technologies, creating an environment where high caliber civilian S&T personnel provide services to defense S&T innovation, while defense related S&T achievements find quick conversion to civilian applications.

Fourthly, establish regional innovation systems with diverse characteristics and strengths.
Regional innovation system planning and associated innovation capacity building shall be made in a unified and coordinated manner, taking into account the characteristics and strengths of the regional economic and social development. Deepen the reform of the local S&T system, with a view to mustering S&T forces at the central and local levels. Take full advantage of the important roles played by universities, research institutes, and national high-tech industrial parks in establishing regional innovation systems in order to enhance S&T innovation support for the local economic and social development. Reinforce S&T capacity building in the country’s central and western regions while earnestly strengthening the construction of grassroots S&T systems at the county (city) level. Fifthly, establish a socialized, networked S&T intermediary service system. In view of the fact that the S&T intermediary service sector is small in size, unitary in function, and weak in providing services, efforts should be made to vigorously nurture and develop S&T intermediary service organizations in diverse forms while taking full advantage of the important roles played by universities, research institutes, and social organizations and groups in providing S&T intermediary services. S&T intermediate service organizations should be guided in the direction of professionalism, scale, and standardization.

VIII. Major Policies and Measures

To ensure the implementation of the missions defined in the Outline, efforts should be made to formulate more effective policies and measures, in addition to addressing system and mechanism related issues. All policies and measures shall be made as such that they are conducive to enhancing indigenous innovation capability, spurring the enthusiasm
and creativity of S&T personnel, making full use of S&T resources both at home and abroad, supporting economic and social development through science and technology.

The S&T policies and measures listed in the Outline are designed to address major discrepancies and protuberant problems we are facing today, but will be adjusted and perfected in line with changing situations and progress in the implementation of the Outline.

1. Financial and Taxation Policies Encouraging Technological Innovation at the Enterprise Level

Encourage enterprises to increase R&D spending and strengthen technology innovation capability. Accelerate the imposition of a consumption based value added tax, and make the industrial payment to equipment procurement favored with a deductible value added tax. On the basis of further implementing a range of taxation holiday policies aimed at spurring technology innovation and accelerating S&T findings spin-off and equipment upgrading, encourage and support enterprises to develop new products, new techniques, and new technologies, by raising the level of incentive policies, including pre-tax deduction of enterprise R&D expenditure, in an effort to provide taxation holidays for the development of high tech businesses. Along with the reform of corporate income tax and corporate financial system, encourage enterprises to establish special funds earmarked for R&D activities. Enterprises shall be allowed to accelerate the depreciation of the instruments and equipment used in R&D activities. Enact taxation holiday policies for procuring advanced scientific instruments and equipment. Enhance foreign exchanges and fund raising support for enterprises establishing R&D facilities
overseas, and provide convenience and quality service for Chinese enterprises’ investment overseas.

Implement the PRC Law on Promoting Small- and Medium-Sized Enterprises, and support the establishment of various types of SMEs, in order to take full advantage of their vitality in technology innovation. Encourage and support SEM initiated collaborative R&D efforts in the form of joint venture or consignment by providing policy support for the commercialization of innovation achievements.

2. Strengthening assimilation and absorption of imported technologies, and re-innovation

Adjust and improve national policies on industrial technology so as to reinforce the assimilation and absorption of imported technologies and re-innovation. Policies should be developed to encourage indigenous innovation and restrict blind and duplicative technology importation.

Readjust the structure and priorities of government appropriations and establish special funds that can be used to support assimilation and absorption of imported technologies and re-innovation, and support the development of major technologies and equipment and critical common industrial technologies. Proactive policies and measures should be formulated increase investments through multiple channels in support of enterprise-centered efforts in the assimilation and absorption of imported technologies and re-innovation, in collaboration with universities and research institutes.
Major national construction projects should be taken as major carriers of uplifting indigenous innovation capability. Through the implementation of major national construction projects, assimilate and absorb a series of advanced technologies, master a number of critical technologies concerning the nation’s strategic interests, and develop a range of major equipment and key products that possess proprietary intellectual property rights.

3. Government Procurement Favoring Indigenous Innovation

Formulate implementing regulations of the “PRC Government Procurement Law” to encourage and protect indigenous innovation. Establish a coordination mechanism for government procurement of indigenous innovative products. Government practices a first-buy policy for major domestically made high-tech equipment and products that possess proprietary intellectual property rights. Provide policy support to enterprises in procuring domestic high-tech equipment. Develop relevant technology standards through government procurement.


Protecting intellectual property rights and safeguarding the interests of IPR owners is not only necessary for perfecting the nation’s market economy system and promoting indigenous innovation, but also important for establishing the nation’s credibility and image in international cooperation. It is important to further perfect the nation’s IPR
system, and create an agreeable legal environment that respects and protects IPR, increase public awareness of IPR, uplift the nation’s IPR management level, enhance IPR protection, and crack down on various IPR piracy activities according to law. In the meantime, it is necessary to establish a special IPR examination process for major economic activities, including mergers and acquisitions and technology trade, in order to **avoid** the loss of proprietary IPR. Prevent the abuse of IPR intended to unfairly restrict market competition or obstruct the diffusion and application of innovation and S&T achievements. Make IPR management part of the entire S&T management process to raise the nation’s S&T innovation level. Reinforce S&T personnel’s IPR awareness while enabling enterprises, research institutes, and universities to attach more importance to and strengthen IPR protection. Give ample scope to the important role of industrial associations in IPR protection. Establish and perfect a professional employment qualification system and public credit system that are conducive to IPR protection.

In line with the nation’s strategic demands and industrial development needs, cultivate a number of inventions and creations of major importance to economic, social, and S&T development in order to produce indigenous IPR. Organize enterprise-led collaborative efforts involving universities and research institutes in overcoming technological snags while providing support for patent application, standard formulation, and international trade.

The development of technology standards should be made an important objective of national S&T programs. Government agencies concerned and industrial associations shall strengthen guidance and coordination for the development of major technology
standards, which are to be adopted as a priority. Promote the system construction for technology laws and regulations and technology standards, and the integration of the development standards with scientific research, development, design, and manufacturing, in order to ensure the advanced nature and validity of standards. Encourage industry-academia-research collaboration in studying and developing major national technology standards, and associated priority adoption. Take an active part in international efforts for standards development, and strive to make our country’s technology standards international standards. Strengthen the development of system construction for technology trade measures.

5. Financial Policies Encouraging Innovation and Pioneering

Establish and perfect venture capital investment mechanism for innovation and pioneering activities, and prepare and formulate laws, regulations and policies to promote the healthy development of venture capital investment destined for pioneering activities. Advance the development of the second board stock exchange, and establish a multi-level capital market system that accelerates commercial applications of S&T achievements. Encourage qualified high-tech enterprises to be listed on the main and second board stock exchange while creating agreeable conditions for small and medium-sized high-tech enterprises to be listed abroad. Create more relaxed banking and foreign exchange policy environment for high-tech venture capital firms. Carry out experiment on circulating unlisted high-tech corporate real options at national high tech industrial parks and gradually establish a technology property rights trade market. Explore to establish a fund raising modality guided by state treasury appropriations, and mainstreamed by the
investment from policy oriented banks and commercial banks, in an attempt to attract more capital into venture capital investment market. Establish a nationwide self-regulating organization for S&T venture capital investments while encouraging banking institutions to provide favorable loans to major national S&T industrialization projects, and S&T commercialization activities. Create intellectual property credit and other credit assurance systems, in order to encourage technology innovation at small and medium-sized enterprises, and create a healthy fund raising environment for them. Establish science and technology related financial cooperation platforms in diverse forms. Government shall encourage banking institutions and private capital become part of S&T development and to improve and strengthen their services for high-tech enterprises, especially for small and medium-sized S&T businesses. Encourage insurance companies to enhance products and service innovation so as provide an overall risk guarantee for S&T innovation activities.

6. Accelerating the Industrialization of High Technologies and the Diffusion of Advanced Appropriate Technologies

High-tech industrialization shall be deemed as a priority in economic restructuring and changing economic growth modalities. Vigorously develop the high-tech industries that can lead to breakthroughs in driving economic growth.

Optimize the environment for high-tech industrialization. Efforts should be continued to strengthen the capacity building of high-tech industrialization bases, including national high-tech industrial parks, by formulating policies conducive not only
to the development of national high-tech industrial parks but also to helping spur the
development of adjacent areas. Establish information platforms for technology exchange
and trade information, and provide policy support for technical development and
associated service provided by S&T intermediary services, including university S&T
parks, S&T business incubators, productivity promotion centers, and technology transfer
centers.

Enhance the support for the diffusion of agricultural technology in order to
establish new mechanisms for diffusing advanced appropriate technologies to rural areas.
The dissemination of agricultural S&T achievements should be made an important factor
for qualifying for an S&T award, while efforts will be made to create a qualification
attestation system for agricultural technology diffusion personnel, and encouraging S&T
personnel to be part of front line diffusion efforts in different forms. Establish special
funds for agriculture S&T achievements related spin-off and diffusion, promoting the
diffusion of advanced appropriate technologies in rural areas, and supporting technology
innovation, invention and creation made by rural residents. The state shall provide a
classified guidance and support for the diffusion of agricultural S&T findings,
encouraging and supporting the development of diffusion organizations in different forms,
and created diversified diffusion systems.

Support industrial sector-oriented applications of critical enabling technologies.
Effective policies and measures will be worked out to support the development, diffusion,
and application of pre-competitive industrial technologies, particularly the diffusion and
application of key technologies in the fields of electronics and information, biology,
information technology-based manufacturing, advanced materials, environmental protection, and energy efficiency. Promote the transformation and upgrading of traditional industries, and strengthen the capacity building of technology engineering platforms, industrialization demonstration bases, and intermediate pilot bases.

7. **Perfecting the Mechanism for Combining Defense and Civilian Sectors, and Making Defense Part of the Civilian Sector**

Strengthen the overall planning and coordination in integrating the defense and civilian sectors. The S&T management system that separates the defense from the civilian must be reformed to allow for the creation of a new S&T management system embracing both the defense and civic sectors. Encourage defense-related research institutes to work on civilian research topics, while defense-related R&D activities be made open to civilian research institutes and industries. Expand the scope of defense procurement from civilian research institutes and industries. Reform the management system to ensure fair competition between non-defense and defense research institutes for defense-related research and production contracts while establishing public platforms for the integration of the defense and civilian sectors, and for dual-use applications.

Establish a new mechanism adapting to the characteristics of both defense and civic scientific research activities. Coordinate the deployment of basic research in defense and civilian sectors, and strengthen the integration of research and development efforts in both sectors. Establish an interactive mechanism between the defense and civic sectors, coordinating the development and production of defense and civilian products, and
fostering an organic combination of S&T efforts in both sectors.

8. Expanding International and Regional S&T Cooperation and Exchanges

The improvement of the nation’s indigenous innovative capability calls for taking full advantage of the merits derived from opening to the outside world, and a significantly higher level of international and regional S&T cooperation and exchanges in various forms.

Encouraging research institutes and universities to establish joint laboratories or R&D centers with overseas research institutes; support the implementation of international cooperation projects under bilateral or multilateral S&T cooperation frameworks; and establish a collaborating S&T mechanism between the mainland and Hong Kong, Macao and Taiwan, to strengthen communications and exchanges.

Support our country’s enterprises in their “going out” efforts. Expand the export of high technologies and products, encouraging and helping them to establish R&D centers or industrialization bases overseas.

Participate actively in large international scientific projects and international academic organizations. Supporting our scientists and research institutes to be part of or take the lead in large international and regional scientific projects. A training system should be established in order to increase the ability of our scientists to engage in international academic exchanges and to take up senior positions at major international
academic organizations. Encourage multinational corporations to establish their R&D centers in our country while offering favorable conditions for making our country the physical location of international academic organizations or their regional offices.

9. **Improving Scientific and Cultural Literacy of the Entire Nation and Building a Social Environment Conducive to S&T Innovation**

Implement a nationwide scientific literacy action plan. Improve the scientific and cultural literacy of the entire nation with a view to advancing people’s overall development. Advocate scientific spirit, spread scientific thinking and practices, and diffuse scientific knowledge. Strengthen popular science activities in rural areas, gradually establishing a training system that helps raise farmers’ farming technologies and vocational skills. Organize systematic scientific exploration and experiencing activities in different forms both on and off campus. Strengthen innovation oriented education, and raising teenagers’ innovation awareness and capability. Strengthen science and technology related training for public servants at different levels.

Strengthen the national capacity building in the field of popular science by rationally distributing and building popular science facilities and improving the quality of existing popular science sites. Establish a system making research institutes and universities accessible to the public on a regular basis, while strengthening communications and exchanges with the public through the implementation of S&T programs and projects. In order to bring about a flourishing development in popular science writings and creating popular science brand names, encourage renowned
scientists and other experts and scholars to become involved in popular science writings, developing major popular science topics, and fostering original popular science writings. Establish S&T communications as a major at universities, in order to strengthen basic theoretical studies concerning popular science and train popular science professionals.

Establish a sound operational mechanism for popular science activities. Strengthen concerted efforts of government agencies, private groups, and large enterprises, facilitating interaction and collaboration between the S&T and education communities and the mass media. Encourage the development of business oriented popular science activities by relaxing restrictions to allow private and overseas capital to access popular science activities and by formulating preferential policies for establishing diversified investment mechanisms. Advance the reform of public good popular science system in order to activate vitality, increase service conscientiousness, and enhance sustainable development capability.

IX. S&T Input and S&T Infrastructure Platforms

S&T input and basic facilities platforms constitute a material basis for S&T innovation, and an important prerequisite and a fundamental guarantee for sustainable S&T development. Today’s S&T input is literally an investment in the future national competitiveness. Since the adoption of reform and opening up policy, the nation has seen continued increases in S&T input. However, to meet the major demand in greater S&T development and in the full-fledged construction a well-to-do society, and compared with the developed and emerging industrialized nations, the nation’s total and intensity of S&T
input remains insufficient, with irrational aspects in the investment structure, and a weak S&T infrastructure. Given the fact that both developed and emerging industrialized nations around the world have made the increase of S&T input a strategic measure to raise their national competitiveness, our country should respond to the trend and need for enhancing the nation’s indigenous innovation and core competitiveness by drastically increasing its input in S&T activities and strengthening the construction basic S&T facilities, so as to ensure the fulfillment of the missions defined in the Outline.

1. Establishing a Diversified, Multi-channel S&T Input System

Taking full advantage of the guiding role played by the government in enhancing S&T input, efforts are to be made to enhance government capability in mobilizing nationwide S&T resources through diverse financial means such as direct appropriations and referential taxation breaks. State treasury appropriations will be mainly used to support public S&T activities that cannot be effectively covered by the current market system, including basic research, frontier technology development, public good research, and development of major key enabling technologies, in addition to its role in guiding industry and private sectors to enhance their S&T input. Government agencies at both central and local levels shall increase the proportion of S&T input in both annual budgeting and distribution of extra budgets, according to the PRC Law on S&T Progress, in an attempt to ensure an S&T expenditure growth noticeably higher than that of regular financial revenues, and in an effort to gradually raise the weight of state treasury S&T appropriations in GDP. Coordinate expenditure needs for implementing planned S&T activities in line with the national strength, to ensure the smooth implementation of major
special projects. The central government will continue to increase its investment in the construction of major S&T infrastructure, with a weighted appropriation support for construction activities at both central and local levels. While increasing government appropriated S&T input, efforts should be made to strengthen the principal position of enterprises in S&T input. In a word, these concerted efforts of all sectors are expected to bring about an increased R&D expenditure year by year, which will reach 2% by 2010 and 2.5% or above by 2020 as a percentage of GDP.

2. Readjusting and Optimizing Input Structures, and Raising the Cost-effectiveness of S&T Expenditures

Support will be strengthened for basic research, frontier technology development, public good research, S&T infrastructure, and popular science activities. Make appropriate funds available for regular expenditures needed by research institutes (bases), research projects, and S&T infrastructure construction. Steadily enhancing the investment in basic research and public good oriented research institutes, making popular science expenditures part of the financial budgeting at an equivalent level, and gradually raising the input in popular science activities. Establish and perfect an S&T expenditure management system, in line with the rules of scientific research and characteristics of S&T activities. Regulate the use of S&T appropriations in accordance with relevant state regulations on budgeting, and improve the safety and effectiveness of appropriations. Increase the openness, transparency, and fairness of national S&T program management, gradually establishing an S&T expenditure assessment system, and corresponding evaluation and supervision mechanism.
3. Strengthening the Construction of S&T Infrastructure Platforms

S&T infrastructures platforms are an enabling system consisting of research and experiment bases, large scientific facilities, instrumentation, and equipment, scientific data and information, and natural S&T resources, supported by information and network technologies and shared by the public in their innovation activities. The construction of S&T infrastructure platforms will focus on the following:

National research and experiment bases. Establish, in line with the nation’s major strategic needs, a number of national laboratories and scientific research and experiment bases, featuring a strong interdisciplinary research team and advanced level, in emerging fields or in the fields where China has a specialty or strength. Strengthen the capacity building of national key labs, and consistently raise its operation and management capability. Establish a national network for field scientific observation and research activities.

Large scientific projects and facilities. Pay more attention to the role played by scientific instruments and equipment in scientific research, and strengthen the proprietary research and development of scientific instruments and equipment and associated test techniques. Establish a number of large scientific projects and infrastructures, including high performance computers, large aerodynamic research and experiment, and scientific experiments under extreme conditions. Advance sharing and construction of large scientific instruments, equipment, and facilities, gradually forming up a nationwide
sharing network.

Scientific data and information platforms. Establish digital platforms ridden with S&T conditions and resources related information, by taking full advantage of modern information technology and means, facilitating sharing of scientific data and literatures, building an online scientific research environment, providing relevant services to the whole society, and promoting the reform of means and approaches used in scientific research.

Natural S&T resources service platforms. Establish a complete conservation system for plant and animal germplasm, microbes and bacteria species resources, and human genetic resources, and create a protection and utilization system for natural S&T resources, including experimental materials, specimens, and mineral fossils.

National technical system for standards, metrology, and test. Develop and formulate high accuracy and high-stability metrological bench standards and standard specimen system. Establish technology standards for major fields, and improve test lab systems, attestation and certification systems, and associated technical measures for technology trade.

4. Establishing a Mechanism for Sharing S&T infrastructure Platforms

The establishment of an effective sharing system and mechanism constitute a key link and prerequisite for the development of S&T infrastructure platforms. Under the
principle of “consolidating, sharing, perfecting, and upgrading”, and taking into account successful foreign experience, formulate standards and regulations involving different S&T resources, and establish a policy and law system promoting S&T resources sharing. Encourag flexible sharing modalities in line with different S&T resources and conditions, and break up the existing divided, closed, and redundant pattern.

X. Talented Workforce Buildup

S&T innovation is rooted in S&T personnel. Human resource has become a most important strategic resource. It is important to advocate the strategy of national capacity building with talented people, strengthening the capacity building of S&T personnel, and providing human resource support for the implementation of the Outline.

1. Accelerating the Nurturing of a Contingent of world caliber experts

Reinforce the nurturing of disciplinary leaders and advancing the buildup of innovative teams, through major scientific research and construction projects, at major disciplines and research bases, and through international academic exchanges and cooperation projects. Pay close attention to discovering and nurturing strategic scientists and S&T management personnel. Formulate special policies to attract high caliber experts in the core areas. Further break up the old practice that ranks a person according to seniority, overcoming the desire for quick results. Lose no time in nurturing young and middle-aged high caliber experts. Improve and perfect a range of high caliber personnel systems, including the job title system, academician system, special government
allowance system, and postdoctoral system. Establish a high caliber expert screening system, in an effort to let more talented people come out.

2. Bring into Full Play the Important Role of Education in Cultivating Innovative Talents

Strengthen the organic combination of S&T innovation and personnel nurturing, encouraging research institutes to nurture research oriented personnel, in collaboration with universities. Encourage undergraduates to take part in research activities, in order to cultivate their exploration enthusiasm and scientific spirit in innovation activities. Universities shall make a rational distribution of interdisciplines and emerging disciplines, and restructure subject composition accordingly, in line with the nation’s S&T development strategies and market demand for innovation personnel. Strengthen vocational education, continuing education and training, and paying more attention to the training of technicians for diverse technical applications, in response to the needs of the economic and social development. Deepen the reform of the curriculum design of primary and middle schools, promoting quality-centered education, and raising students’ scientific and cultural literacy.

3. Supporting Enterprises’ Efforts in Nurturing and Attracting S&T Talents

The state encourages enterprises to recruit and nurture high caliber S&T personnel, with corresponding policy support. Encourage and guide S&T personnel at research institutes and universities to work on innovation or create their own S&T businesses.
S&T personnel at research institutes and universities are allowed to take extra jobs for technology development at enterprises. Encourage university graduates to work for firms. Encourage enterprises to nurture technology talents, in collaboration with universities and research institutes. High caliber engineering talents can be nurtured through multiple channels and diverse modalities. State-owned high-tech businesses are allowed to introduce a range of incentive policies, including real options in honor of high caliber technicians and management personnel. Explore ways to establish a distribution system made up of diverse elements, including knowledge, technology, and management. Support industry to attract and recruit foreign scientists and engineers.

4. **Intensifying Efforts in Attracting High Caliber Talents From Overseas**

Formulate and implement programs to attract returned service of high caliber overseas Chinese students, with priorities on attracting high caliber personnel and expertise in shortage. Establish talents attracting centers tailored to the characteristics of overseas Chinese students, through diverse approaches. Enhance the financing of the return of high caliber personnel. Strengthen the construction of pioneering centers for overseas Chinese students. Perfect the policies and measures in favor of returned service of overseas Chinese students. Create more open recruitment opportunities for high caliber innovation talents. Gradually open up the recruitment of senior post vacancy before overseas candidates, including lab directors, academic leaders of major research institutes. Adopt attractive policies and measures to attract high caliber overseas S&T personnel or teams to work in China.
5. Creating a Culture Environment Conducive to the Nurturing of Innovative Talents

Advocate the patriotism featuring hardworking and dedication, and a teamwork spirit of pragmatism, innovation, collaboration and indifference to fame and wealth. Encourage rational skepticism and criticism, respecting individuality, tolerating failures, encouraging academic freedom and democracy, supporting exploration and standing out among peers, and respecting new theories and concepts. Stimulate innovative thinking, activate academic atmosphere, and strive to create a tolerant, harmonious, healthy, and upbeat innovation culture. Strengthen the ethics building in research activities while curbing flippancy and unethical practices in scientific research activities.

The implementation of the outline of the National medium and long term S&T development plan calls for a strengthened leadership and coordination as it has a broad coverage, long time span, and demanding requirements. Effective measures shall be adopted to ensure the implementation of the missions defined in the Outline. 1) Strengthening the interface between the Outline and the national economic and social development plan for the 11th five-year period. The Outline shall be implemented, according to the priority list, abreast with the implementation of the national economic and social development plan for the 11th five-year period, in an attempt to increase the feasible implementation of the Outline. The implementation will cover a sequence of efforts, including priority topics, major special projects, cutting-edge technology, basic research, construction of infrastructure platform, and S&T system reform, from which priorities will be selected to start immediately, or to be dealt with within the 11th five-
year period. Working out matching arrangements and deployment in the national economic and social development plan for the 11th five-year period. 2) Formulating practical and feasible supporting policies. Development objectives, major missions, and policies and measures defined in the Outline are direction pointing and guiding in nature, and need practical and feasible supporting policies to go along with. These policies will cover: supporting industry to be the mainstream of technology innovation, promoting digestion, absorption, and re-innovation of imported technologies, government procurement tilting to proprietary innovations, increasing S&T input, S&T fund efficiency, deepening the reform of S&T system, establishment of national innovation system, accelerating high tech industrialization, capacity building for S&T personnel, and promoting the combination of defense and civic sectors and making defense part of the civic applications. The above-mentioned policies shall be prepared and enacted in such a manner that authorities concerned will take a lead, with the participation of involving government agencies. The policies shall be prepared based on a thorough survey and investigation, in an attempt to make them closely associated and coordinated with other policies concerning industry, banking, finance, taxation, and economy. The policies shall be made and implemented in a prompt manner. 3) Establishing a dynamic readjustment mechanism for implementing the Outline. It is important to establish a dynamic readjustment mechanism for implementing the Outline, based on economic and social analysis, technology prediction, and regular evaluation, in an attempt to keep abreast with the fast S&T development in the world, and changes brought up by the domestic economic and social development. It is also meaningful to make a timely and necessary readjustment of the development objectives and major missions defined in the Outline, in line with new trends and breakthroughs of S&T development both at home and abroad,
and with the new demands rising from China’s economic and social development. Some
of the missions will possibly be strengthened and enhanced, while some others readjusted.

4) Strengthening the organizing and supervision of the implementation. It is necessary to
take full advantage of the initiatives of localities, government agencies, and private
groups to organize the implementation, under a unified leadership of the Central
Committee of the Chinese Communist Party and the State Council. Government
agencies, in particular, national authorities in charge of S&T management, development
and reform, and finance, shall live up to their respective responsibility through a close
coordination, and strengthen concrete guidance. Provinces, municipalities, and
autonomous regions shall implement the Outline in line with local development status.

The implementation of the Outline is associated with the full-fledged construction
of a well-to-do society, the success of socialist modernization drive, and the great
renaissance of the Chinese nation. Under the leadership of the Party Central Committee
headed by Secretary General Hu Jingtao, and with the guidance of Deng Xiaoping
Theory and the important doctrine of “Three Representations”, the nation will go all out
to materialize the grand blueprint of science and technology development, and build an
innovation-oriented nation with steadfast confidence and determination.