



www.ddsi.org

National Dependability Policy Environments

PEOPLE'S REPUBLIC OF CHINA

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: RAND Europe (NL)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the "Information Society Technology"
Programme (1998-2002)

Table of Contents

Overview of the Country's Information Infrastructure 3
Main ICT Regulatory and Legal Developments 4
Assessment of Phenomena Undermining Dependability 5
Government Initiatives Aimed at Tackling Cyber-Security 7
Industry and Other Non-Government Activities Related to Dependability 9
Research and Development 9

Overview of the Country's Information Infrastructure

In terms of general ICT trends, the People's Republic of China (PRC) has seen a constant increase in ICT development, installation, usage and commerce. The estimated number of Internet users in the PRC has increased from 60,000 in 1995 to 8,900,000 in 1999. The number of personal computers has grown from 2.8 million in 1995 to 15.5 million in 1999. The number of ISDN subscribers lay at 0 in 1995 but in 1999 was estimated at 168,000. It has since increased significantly. The annual investment in telecommunications has increased from 13,240 million EUR in 1995 to 21,222 million EUR in 1999. Expenditure on ICT represented 4.86 percent of the PRC's GDP, according to the World Bank in 1999.¹ In terms of ICT intensity, there were 12.2 computers per 1000 inhabitants in 1999.

The telecommunication service grew from EUR 9 billion in 1995 to EUR 32 billion in 1999 with annual average growth rate of 37.2 percent.² In 1997, the PRC's information technology (IT) market was valued at EUR 8.1 billion, with computer hardware accounting for 80.6 percent of sales; software accounts for EUR 448 million, and services EUR 407 million. Experts predict that the PRC's IT spending will increase to EUR 21 billion by 2001, with most of the spending on IT equipment and services. The information services and software industry is expected to grow at an annual rate of 28 percent until the year 2000, with applications software purchases expected to increase 34 percent during the same period, and reach over EUR 7.7 billion by 2002.

The PRC has 16.7 million Internet users, which is only 0.7–1 percent of the total number of Chinese people. China Daily and Nua Internet Surveys report, however, that this figure is closer to 30 million as of the end of 2000.³ Of the total access to the Internet, 50 percent of users access the Internet from home, 37 percent from work or school and 11 percent use Internet cafés.

The China Internet Network Information Centre reports that Internet use in the PRC increased from 4 million from January to June 2001, reaching a current total of 26.5 million people. There were also over 10 million personal computers connected to the Internet.⁴ The PRC has 3,500,000 computer hosts. Among them, 1,090,000 use leased line connections, 660,000 are dial-up users and 1,150,000 use both. Countries directly interconnected to the PRC's infrastructure include the United States, Canada, Australia, Britain, Germany, France, Japan, and South Korea.

The PRC has 17.7 phone lines per 100 people nationwide and 27.7 lines in cities (2001). According to the World Bank, the overall average is 86 telephone mainlines per 1000 people (1999).⁵

¹ World Bank Information Age factsheet: www.worldbank.org/data/wdi2001/pdfs/tab5_10.pdf (visited on 1 November 2001)

² For both amounts the January 1999 EURO-RMB exchange rate of 9,7213 is used: www.lu.se/eu-china/exchangerates/RMB/RMB99.html (visited on 1 November 2001)

³ "China to protect copyrights on the web", *Infowar* (visited on 22 December 2000): www.infowar.com/law/00/law_122200c_j.shtml (visited on 5 November 2001); Nua Internet Surveys, "Over 26m Internet users in China", China Internet Network Information Center (18 July 2001): www.nua.ie/surveys/?f=VSandart_id=905356992andrel=true (visited on 5 November 2001).

⁴ "Growth of Internet Users in China slows", *China Daily* (17 July 2001): search.chinadaily.com.cn/isearch/i_search.exe (visited on 28 January 2002).

⁵ World Bank Power and Communications factsheet: www.worldbank.org/data/wdi2001/pdfs/tab5_9.pdf (visited on 1 November 2001).

Most e-commerce in the PRC today involves B2C transactions rather than those related to B2B. Experts predict that the total volume of global e-business trade is expected to exceed EUR 1,100 billion by the year 2002 and further soar to EUR 1,650 billion by 2003. In 1999, on-line B2B is about 0.05 percent of the total transaction amount between businesses.

The PRC now has over 36 million mobile phone subscribers,⁶ with an average annual growth rate of mobile telephony being 150 percent in the 1990s. Despite the large absolute number of mobile phone subscribers, nation-wide cellular penetration remains low at about 1.5 percent. Four international companies are currently allowed to operate pilot projects with this technology in four Chinese cities: Lucent in Guangzhou, Motorola in Beijing, Nortel in Xian, and Samsung in Shanghai. Estimates place the total number of mobile phone users in the PRC at 100 million with a penetration of 8 percent by 2005, and 200 million with a penetration of 15 percent by 2010.

The PRC's largest satellite network was completed by the former Ministry of Posts and Telecommunications (MPT) in 1995. The network uses 18 earth stations in major cities and provides a total capacity of 7,500 voice-grade circuits. In addition, the PRC has a one-third share in Asiasat, Asia's most successful commercial satellite system.

Main ICT Regulatory and Legal Developments

In China's Ninth Five-Year Plan (1996-2000), the MPT funded EUR 85.3 million in construction investment. In March 1998, the MPT merged with the Ministry of Electronic Industry (MEI) to form the Ministry of Information Industry (MII).

The Ministry of Information Industry's responsibilities⁷ include the formulation and development of strategies, policies, laws, regulations, plans, and technical criteria for the information industry, the public telecom network, the radio and television network, and military telecom networks; the revitalisation of the telecom and software industries and the manufacture of electronic and information products by promoting R&D, technology imports, the application of research, and domestic industry; the approval of the telecom networking and terminal equipment and supervising product quality; the allocation and management of radio frequency resources, satellite orbit positions, telecom network codes, domain and Web site resources, approving the establishment of radio stations, and monitoring radio operations; the oversight of fair competition in the telecom and information service markets and promoting service quality, approving telecom and information service licenses, drafting regulations for interconnection and the settlement of telecom networks; the regulation of telecom service fees and the construction and management of special telecom networks for the Chinese Communist Party, government organs, the military, and guaranteeing state telecom and information security.

Responsibilities also involve the reorganisation of the relevant state-owned enterprises, preventing redundant construction and allocating industry resources; the promotion of the spread of information technology through education campaigns; the organisation and development and use of information resources and launching information projects; the co-ordination of economic relations between postal and telecom enterprises, subsidising postal and telecom services, and administering the State Postal Service

⁶ "UTStarcom Shines in China", [123Jump.com](http://www.123jump.com) Inc (20 July 2000): www.123jump.com/story.htm?story_id=3240 (visited on 28 January 2002).

⁷ China On-line Information Centre (2001): www.chinaon-line.com/refer/legal/Mmeyer_laws/important_documents.asp (read 1 November 2001).

Bureau; participation in related international organisations, signing inter-government agreements, organising economic and technological co-operation with foreign countries.

The PRC began the deregulation of telecommunications in 1993. Before then, the PRC's telecommunication services, including basic and value-added telecommunication services, were all operated and administrated by the MPT. Overlapping governmental sectors and the mixture of governmental functions and enterprise functions in the PRC's telecommunication field seriously hindered its telecom development. China Telecom was separated from MPT to operate the telecommunication services. MPT only handled the policy and strategy.

Although the PRC officially introduced competition in the telecommunication sector several years ago, 95 percent is still owned by the company that used to belong to the formerly state-run China Telecom, while domestic competitor China Unicom has 5 percent of the market. Until now, foreign companies were not allowed to compete in the PRC in telecommunication service, but only in telecommunication equipment and infrastructure. In order to attract foreign investment and advanced technology, the PRC has adopted a series of policies to encourage foreign investors to compete in this market.

The Chinese Government has already announced that it will invest EUR 187 million to bolster domestic mobile phone manufacturing. New (foreign) entrants are prohibited from owning more than a 49 percent stake in Chinese carriers.⁸ The PRC maintains a number of preferential policies for high-tech investments, including tax holidays and refunds. One of the major Chinese Government programs is favourable tax treatment of research and development (R&D).

Payment over the Internet is an important link for developing e-commerce and is viewed as a bottleneck in developing e-commerce in the PRC. Fortunately, since 1999, because of the extensive use of credit cards, this is being rapidly solved. Credit card use began in the PRC in 1985. In the last five years, the number of credit cards issued has grown on average by 64 percent. The extensive use of credit cards creates a favourable environment for e-commerce.

China will invest more in the software industry, encourage venture capital, cut taxation on software, and create more channels for software businesses to raise funds.

The Ministry of Education allocated EUR 10.7 million in 2001 to the country's disadvantaged remote western regions to launch distance education projects to help them catch up with the developed areas. In an effort to speed up basic education in these areas, the central government has invested EUR 321 million in the past three years.

Assessment of Phenomena Undermining Dependability

Very little data is available on dependability breaches. Some anecdotal evidence talks of malicious attacks against Chinese military computer systems, illegal transfer of bank accounts, or hacks in banks and securities firms.⁹ Authorities had expressed concerns about the vulnerabilities of exposed by the hacking of hospital records.¹⁰ In a 2000 survey asking Internet users whether hackers had corrupted their

⁸ Institute of Electrical and Electronics Engineers Inc, ComSoc Industry Newscache (20 December 1999): www.comsoc.org/inc/1999/122099.htm#story3 (read 2 November 2001)

⁹ Peter Grabosky, "The global and regional cyber-crime problem", Broadhurst (ed), Proceedings of the Asia Cyber-crime Summit, University of Hong Kong, 25 and 26 April 2001.

¹⁰ Grabosky, *ibid.*

computer, 63.68 percent said they Did Not Corrupt, 11.65 percent said Corrupted, and 24.67 percent responded Unknown.¹¹

Before 1994, IP (Intellectual Property) laws were only discussed in postgraduate law programmes. Now, many universities add IP law to undergraduate law curricula. The infamous piracy rate in the PRC has continually decreased, dropping from 97 percent of all software in circulation in 1994, to 91 percent in 1999. Despite significant government efforts to shut down manufacturers and retailers of pirated software, piracy continues to be a serious problem. Furthermore, as IP enforcement becomes stricter, many CD pirates appear to have moved to Hong Kong to continue their illegal activities.

The view has long been that the PRC is in the midst of the development of capabilities to undermine dependability internally. Officially, the offensive aspects are often given more coverage than defensive measures. However, with the increasing realisation that e-commerce relies upon secure information exchange, the Chinese government is beginning to accept the value of defensive Information Security practices.

The PRC is currently trying to balance the opposed ideals of economic modernisation, which has information freedom at its heart, and internal stability and the control of information. However, the slow pace of the development of the 'knowledge economy' in the PRC has meant that the government can devise a centralised national information security strategy. Chinese virus experts (namely the Chinese National Computer Virus Emergency Response Centre) were the first to report the existence of the Bin Laden worm, which appeared after the terrorist attacks on September 11th in the United States.

CCERT also released the first survey on computer security in July 2001. Information was collected in conjunction with the Ministry of Public Security. The survey revealed that the PRC is just as susceptible to computer viruses as other nations. Only 27 percent of computer users are free from viruses and 59 percent of users have been attacked more than 3 times. The main causes of viruses however, were pirated CD-ROMs and removable media. Over 8,000 respondents contributed to the on-line poll.¹²

However, the US–Chinese spy-plane incident in early 2001 sparked what many believed would be a hacker war between the United States and the PRC. In the end, it appeared to be a long-running exchange of web-site defacements (regarded by many as electronic graffiti – embarrassing but ultimately harmless) by actors operating independently of the authorities. Similar reprisals had occurred following the accidental bombing of the Chinese embassy during NATO operations against Serbia in 1999.¹³ The attacks escalated further when Chinese hackers attacked the US Department of Energy web-site, posting messages proclaiming Chinese superiority. The White House homepage was also hit by attackers (who appeared to originate from the PRC) and defaced with pro-Chinese messages. At the height of this 'War of Defacements', estimates suggested over 40 attacks daily.¹⁴

¹¹ "Over half of computers attacked by virus – survey", *China News* (26 July 2001): www1.chinadaily.com.cn/itchina/2001-07-26/22606.html (visited on 28 January 2002)

¹² "Over half of computers attacked by virus – survey", *China News* (26 July 2001): www1.chinadaily.com.cn/itchina/2001-07-26/22606.html (visited on 28 January 2002)

¹³ "Chinese Hackers Launch Retaliatory Web-Site Attacks", *Newsbytes* (26 April 2001): www.newsbytes.com/news/01/165102.html (visited on 28 January 2002)

¹⁴ "Pro-Chinese hackers hit Californian sites", *Ananova* (2 May 2001): www.ananova.com/news/story/sm_279613.html?menu= (visited on 28 January 2002)

In August 2001, the US DIA (Defense Intelligence Agency) awarded a contract to Veridian to monitor intrusions originating from a foreign country generally thought to be the PRC. The company was asked to correlate such attacks with real world events. Although DIA did not know at the time whether the attacks were sponsored by official agencies, a number of experts believed that some were.¹⁵ This was re-emphasised by the testimony of certain officials to the US Congress that confirmed Chinese development of computer-based tools intended to attack the United States.¹⁶ Chinese hackers are not averse to attacking other web-sites in addition to those of the United States. In August 2001, the Chinese hacking group 'the Red Hackers Alliance' hit a number of Japanese web-sites in response to the visit by Japanese premier Junichiro Koizumi to the Yasukuni shrine, which has proved to be a source of contention between the PRC and Japan. The motivation for the attack was popular dissatisfaction with the Japanese government, though it was not thought that official government bodies were at all involved in the incidents.¹⁷

Government Initiatives Aimed at Tackling Cyber-Security

For a long time, it was unclear which ministry actually held responsibility for controlling the internet in the PRC.¹⁸ In the autumn of 2000, twenty provinces set up a special police force to monitor Internet "crimes", with the task of curbing pornography and "maintaining order" on the Internet. Meanwhile, criminal statutes have been revised to allow for the prosecution of subversive activity on-line. Existing laws covering state security and secrecy allow the authorities to jail people for a wide range of Internet-related offences. But in October and November 2000, after years of internal debate, the government issued two sets of regulations that specifically govern ownership, content, and other aspects of Internet usage.

The first set of rules, issued on October 1, limits direct foreign investment in Internet companies, requiring them to register with the Ministry of Information Industry and apply for permission before issuing stock or signing any agreement with a foreign investor. Article 15 bans the dissemination of any information that may harm the unity of the country, endanger national security, or subvert the government. Promoting "evil cults" is similarly banned, along with material that "disturbs social order or undermines social stability." Other articles ban the distribution of pornography or "salacious material," along with anything that harms "the honour and interests of the state." Another regulation requires Internet café patrons to register with "software managers" and produce a valid ID card in order to log on.

Under the new rules, only state media are allowed to set up news sites, and only with permission from the State Council Information Office (SCIO), a Politburo-level agency tied to the Communist Party's

¹⁵ "Defense agency, Veridian to pinpoint foreign hackers", *Computerworld* (28 August 2001): www.computerworld.com/storyba/0,4125,NAV47_STO63380,00.html (visited on 28 January 2002)

¹⁶ "CIA Official Warns Congress of Cyberattack Danger", *IDG.net* (22 June 2001): www.idg.net/crd_idgsearch_3.html?url=http://www.thestandard.com/article/0,1902,27365,00.html (visited on 28 January 2002)

¹⁷ "Chinese hackers attack Japanese websites", *ireland.com* (visited on 15 August 2001): www.ireland.com/newspaper/breaking/2001/0814/breaking45.htm (visited on 21 January 2002)

¹⁸ Lin, Neumann A. "The Great Firewall": www.cpj.org/Briefings/2001/China_jan01/China_jan01.html (read 5 November 2001)

Propaganda Ministry. The Information Office handles content issues, while the Ministry of Information Industry looks after service and access issues.

An overview of appropriate laws is given by Gregor Urbas for the Asia Cyber-Crime Summit 2001:¹⁹

Offences	Laws and regulations
Illegal access	Regulations on protecting the safety of computer information (Order No. 147 of the State Council of the People's Republic of China, 18 Feb 1994)
Illegal interception	Computer information network and internet security, protection, and management regulations (State council approval 11 Dec 1997, promulgated 30 Dec 1997)
Data interference	1994 Regulations Warnings may be given, fines imposed, and illegal income confiscated in cases of deliberate input of computer virus or selling special safety protection products without permission.
System interference	1997 Regulations Prohibiting the use of internet to: harm national security, disclose state secrets, conduct illegal activity, etc. (Art. 4) punishable by state-relevant regulations (Art. 19); transmit information inciting illegality or overthrow of the government etc. (Art. 5) punishable by warnings, confiscation of illegal income and fines (Art. 20).
Misuse of devices	Prohibition of activities harming the security of computer information networks including: unapproved use of computer networks or resources, change of network functions, adding/deleting/altering stored data, etc.; creation or transmission of viruses, punishable as for Art. 5.
Computer-related forgery	
Computer-related fraud	
Computer child pornography	

On 28 December 2000, the 19th session of the Standing Committee of the National People's Congress passed a resolution²⁰ on maintaining the security of computer networks, making it a criminal offence to transmit over the Internet slander and rumours or harmful information, state, intelligence, or military secrets, incitement of ethnic hatred or discrimination, information in support of cults, advertising fake or substandard products or services, material damaging business reputation, material infringing intellectual property, false information on securities or futures trading, pornography or insulting/ defaming material.

In June 2001, there was the first publicised arrest of a Chinese hacker. A 21 year-old student was arrested on charges of intruding into a commercial computer system. According to news reports at the time, he obtained password and username information which was then sold onto around 1,000 other people.²¹ In November 2001, China began clamping down on a number of Internet bars and cafés that had failed to block web-sites deemed to be subversive or pornographic by the authorities. Over 17,000 venues were

¹⁹ Gregor Urbas, "Cyber-crime legislation in the Asia-Pacific region" in Broadhurst (ed), Proceedings of the Asia Cyber-crime Summit, University of Hong Kong (25-26 April 2001).

²⁰ Urbas, *ibid.*

²¹ "First Arrest of a Hacker Made in Beijing", Chinese Peoples Daily (1 June 2001): english.peopledaily.com.cn/200105/31/eng20010531_71479.html (visited on 28 January 2002)

closed for these reasons. There are over 94,000 such cafés in the PRC, and 4.5 million people use them to access the Internet. This may be the first time that news of such activity has become widespread.

Both these events are evidence that the PRC is beginning to take its responsibilities more seriously. Clampdowns began after the war of defacements between the PRC and the United States following the Hianang spy-plane incident in early 2001. Encryption rules were relaxed in March 2000, and consumer software with strong encryption was allowed into the country. Originally, a license was required for software or equipment containing encryption technology. According to the same edict, support for public key escrow was dropped.

Industry and Other Non-Government Activities Related to Dependability

In July 1997, the independent CCERT (China Education and Research Network Computer Emergency Response Team) became operational. Part of the China Education and Research Network (CERNET), CCERT's stated tasks are to prevent security violations in CERNET and deal with and respond to intrusions and emergencies.

Research and Development

In 1986, the PRC introduced the Torch Programme, under the leadership of the State Science and Technology Commission (now Ministry of Science and Technology, MST) to commercialise discoveries made by government research institutes and universities. The program provides facilities to serve as technology incubators.

The Torch Programme co-locates technology-rich enterprises in order to create new technologies through synergy. The State Science and Technology Commission has established 53 high-technology zones (resembling research parks in the United States), producing a revenue of EUR 64 million. Successful enterprises include Legend Computer, a PC manufacturer; Stone Company, which produces a popular word processing program; and the Founder Company, which produces typesetting software that is used worldwide.