

# Status of the Computer Network Security Activities of the People's Republic of China

*E. Kozik*

*Penn State University, Great Valley, Malvern, PA 19355*

*Ph: (610)648-3200 Fax: (610) 648-3377 E-mail exk6@psu.edu*

## **Abstract**

Around 221 BC the Qin Dynasty began building the Great Wall in an effort to keep out the Mongol invaders. It did not work. In 1997, the People's Republic of China is building an electronic wall to keep out undesirable Western electronic transmissions. This second wall also will not work, say many China experts. But the Chinese government believes it has to try. China's main security concern is the INTERNET. To counteract the free-wheeling INTERNET, in February 1996 the Ministry of Public Security published constrictive regulations on INTERNET use. Though China has about 20 INTERNET Service Providers and, at least, six links connecting to the global INTERNET, the flow of information is regulated. These regulations force all international networks to run through limited channels set up by the Ministry of Posts and Telecommunications (MPT). Additionally, all users of international networks must register with MPT. The government believes that Chinese values are not compatible with Western freedoms. Publicly, officials have stressed the need to protect state secrets and shield the Chinese people from undesirable political and pornographic materials. These regulations forbid networking activities that harm the state and prohibit the use of the INTERNET for "producing, retrieving, duplicating and spreading information that may hinder public order." Consequently, all international traffic--inbound and outbound--is filtered through government agencies and, eventually, through controlled information ports supported by Chinese-built firewalls. To achieve China's goal, it will be necessary to have total cooperation and support from the INTERNET users, a difficult goal to achieve indeed.

**Keywords**

China's INTERNET security, security technology, network design, firewalls, encryption, network encouragement, governmental constraints.

**Chinese INTERNET and Telecommunications Infrastructure**

The development of China's INTERNET has many operating constraints and infrastructure problems. Like computer network developments elsewhere in the world, research and educational institutions have been the early users. In 1998 the first China Academic Network (CANTET) was established. CANET can exchange e-mail with INTERNET, using X.25 technology via a gateway in Karlsruhe University, Germany. China established its second INTERNET e-mail link to the outside world at the Academy of Science (CAS) Institute of High Energy Physics (IHEP) nine years ago. Its first international INTERNET link was established in 1993, again at IHEP with a direct link to Stanford University. Since then, the INTERNET has experienced a torturous growth in China.

Although the INTERNET is still a very young technology in China, already powerful government forces are at work seeking to exert command control over the flow of information within the Chinese portion of the INTERNET and between the Chinese portion and the rest of the global INTERNET.

Since INTERNET success depends on the underlying China Information Infrastructure (CII), the use of current telecommunications technologies, language encoding ability, and the integration of computer network operations will frame its developmental problems and operating activities. For instance, given that government controls all the mass media in China (newspapers, broadcast stations, films, recordings), it should be no surprise that they are now "regulating" the INTERNET. China's security infrastructure also is equipped to selectively monitor telephone calls and faxes. The Chinese government has even banned paging companies from "editing and disseminating news" in the message function of their pagers. China's multifaceted, ideological control interest is still important to the government's *modus operandi*.

In addition to the constraining regulations, most INTERNET use in China is limited to simple e-mail. Few users currently have high-speed modems or multimedia computers needed to take advantage of the Web. And since most of the Web's pages are in English, a language gap exists for many users. But better computers and faster modems are making their way into the marketplace, and a new Beijing-based group called the INTERNET Media Consortium for Asian Electronic Commerce is studying how to provide Chinese translations through new Web browsing software.

These operating constraints and published regulations will likely slow the growth of the INTERNET within China. Currently, some Chinese professionals think that

their academic research network called CERNET is more important for China's development than INTERNET. Xing Li, a professor at Tsinghua University in Beijing and Vice-Director of the China Education and Research Network, is a strong supporter of CERNET'S importance. Li says economic growth may indeed slow down for a while but that the reasons have more to do with the lack of money than with constraining regulations. Also, electronic network services are expensive for Chinese institutions to use and too expensive for use by the average Chinese.

Many people believe that China is following a familiar governmental control pattern that will result in a major slowdown in INTERNET usage. The government's point-of-view is that time, skills, and more information technology experience in building their great electronic wall are needed in order to protect the people from undesirable Western influences.

Not everyone is convinced this electronic wall can hold for very long. It would be, for China, difficult to enforce such a control structure without a capable monitoring and auditing system to keep track of the INTERNET transactions. Attempting to monitor, filter or audit an ever-expanding and changing electronic commercial universe with millions of Web sites and hundreds of millions of pages is an exercise in futility and, surely, a non-workable policy. Chinese professionals believe that such potential enforcement may be more effective at scaring the users than the use of filtering techniques to catch the abuser. Intercepting, then deciphering and then tracing the origin of millions of e-mail messages is operationally difficult, if not economically impossible. Ultimately, China knows that it must rely on the Western inputs of scientific and information security technological transfers and must use such transfers in expediting the development of innovation systems in its drive to compete in world markets. Science and information technology developments are vital to economic development, and only by making itself market-oriented can the commercial sector boost productivity which, in turn, should help the Chinese people. But what China wants is a market economy with socialist characteristics. After all, this country is called the "People's Republic of China."

## **Expansion of the Chinese Networks**

China certainly wants to expand the use of their many electronic networks. There are four main nationwide networks currently being developed. They are the CHINANET, CERNET, Scientific and Technological Information Network and the Ministry of Electronics' industrial electronics network. Much government support is extending or will begin to extend the capability of these sector, regional and cross-regional networks. Central and local governments are assisting in the construction of these many networks and information control ports. Government

and business firms want to promote and expand the use of information resources in order to enhance their industrial and social developments.

The key government organization behind these network developments is the Ministry of Post and Telecommunications (MPT). In addition to supporting the four major networks were possible, MPT also operates several data networks. The China National Public Data Network (CHINAPAC) is an X.25 network. CHINAPAC has access nodes in all areas covered by the telephone network. CHINAPAC can be accessed at leased line speeds up to 64 Kbps as well as through the public telephone network. MPT also operates a Digital Data Network (DDN). Built in 1994, the DDN supposedly provides data services from 30 Mbps to 2Gbps with more than 3,000 nodes. The DDN is considered the backbone of China's information highway plans.

It appears that the Chinese government is concentrating on funding telecommunications projects that lead to more centralized government planning. These projects are referred to collectively as "Golden Projects." These Golden Projects rely mostly on MPT's public network circuits, CHINAPAC, DDN, and CHINANET, for transport. A partial list of currently active Golden Projects is presented below:

### **The Golden Projects**

1. Agricultural comprehensive management and service information system (Golden Agriculture Project)
2. Nation-wide public economic information processing network (Golden Bridge Project)
3. Electronic monetary and modern payment system (Golden Card Project)
4. Foreign trade information sources network (Golden Customs Project)
5. National economic micro-policy making support system (Golden Policy Project)
6. Industrial production and circulation information network (Golden Enterprises Project)
7. Chinese education and scientific research computer network and human resource project (Golden Intellectual Project)
8. Electronic taxation system (Golden Taxation Project)

### **Communications**

Most of the above golden projects will use CHINANET or the INTERNET as their communications carrier.

The Chinese government prohibits foreign operation of the communications networks that support the Golden Projects. MPT officials cite national security reasons as their justification to ban foreign investment in operating these networks. A more compelling reason would suggest that any such foreign investment would

be in direct competition with the MPT. Nevertheless, product vendors such as Motorola, AT&T, Nortel, Nokia, Ericsson, and Siemens are making some marketing inroads in China. Only a few telecommunications service corporations such as Ameritech, McGaw, Singapore Telecom, and Siemens have managed to forge joint ventures in which they are defined not as information service providers but rather as engineering advisors. Such joint ventures offer little legal protection. In fact, there is no telecommunications law in China. The Chinese government issues edicts that substitute for law. The absence of such law bolsters the influence of the MPT as both the dominant telecommunications common carrier and the telecommunications regulatory agency.

Probably as long as all governments have been legislating policy, technological developments have created problems for policy makers. Consequently, it is difficult to anticipate the effect of INTERNET technology on China's policy making process. Regulatory, legislative, political, financial, social, cultural, and international issues abound in China's untested, transient INTERNET market and have posed difficult security tasks for users and Chinese policy-makers.

Developers of electronic security in China are usually the universities and the State-run research institutes. Under this system, these institutions, subsidized by the government, have conducted State-assigned research and network security development programs with little emphasis on the commercialization of their research. In addition, there is little cooperation or sharing of research and development (R&D) results between these institutions, which belong to and/or are managed by other different and powerful ministries.

Many presenters at the Network and Information Port Conference (Shanghai, 18-20, October 1996) stated that it is essential that these science and technology institutions become more integrated with Chinese economic development. A legal system that will facilitate imports of needed research and development technologies should also be established. The problem with their legal system is that China does not run the country by laws. They run the country by governmental dictated regulations which they call official policy.

In the Ninth Five-Year Plan (1996-2000), major effort and investment are being applied to integrate the development of information, biotechnology, pharmaceutical and new materials industries. Key emphasis will be place on the development of on-line electronic service networks that include social security support, international economic performance information, community services and value-added electronic commerce activities.

All this boils down to China's "Orwellian" plans to build all sorts of national and regional electronic networks. They have the CHINANET ([www.cnc.ac.cn](http://www.cnc.ac.cn)), CERNET ([www.net.edu.cn](http://www.net.edu.cn)), Science and Technology (STNET) network ([www.stn.sh.cn](http://www.stn.sh.cn)), Economic Information Network ([www.cein.cn](http://www.cein.cn)), and eight regional networks with the Shanghai network being the largest. The latter's several subnets include Shanghai Post Telephone and Telegram (PTT) network

(www.sta.net.cn), banking network, customs network and others. Among the other networks are Fudan and Jiao Tong University campus nets, Eastern China Education and Research net, Jing-Jiu railroad network which links Beijing with Hong Kong, tobacco network, UNICOM'S (China United Telecommunication Corporation) electronic commerce network--and on and on it goes.

The national government intends to support its control over those sector, regional and cross-regional networks through the use of information ports under the auspices of the Ministry of Post and Telecommunications. To meet the growing needs for information services, China has mapped out ambitious plans to establish federated, nationwide fiber communications network, using the CHINANET or, perhaps, the INTERNET as a backbone. In order to achieve this goal, China must speed up the construction of its information technology infrastructure. This effort requires much capital investment in the telecommunications industry. As stated earlier, foreign investors have been limited to selling "telecommunications products." Generating and providing telecommunications services has been reserved for Chinese firms and other governmental institutions. With few exceptions, foreign investors have been kept out.

Despite all the telecommunications business developmental opportunities, China has many financial and operating problems that have to be addressed. Among them are high development costs; backward infrastructure; bureaucratic in-fighting; lack of skilled personnel; increasing technological gaps; inadequate development of information databases; over-emphasis on hardware at the expense of software; market's and business's impatience with governmental delays; and government dictated regulations that are more concerned about protecting various Ministry's powerbases, and in maintaining their control, rather than in supporting economic development. In general, the lack of managerial foresight and coordination at both the policy level and the technical level among governmental bureaus, agencies, commissions, R&D institutions and universities has created many managerial and technological hurdles for the development of the desired, national integrated set of secure networks.

This in-fighting has created managerial disputes between Ministries, between major R&D institutions and between the central and local government agencies in regard to the needed network backbone technologies and their connection to local regional nets and subnets. Professor Xing Li of Tsinghua University reiterated these problems when he remarked that the technological development of networks and information ports is hindered by ingrown, inefficient, cumbersome bureaucracies, plus overstaffed institutes, laboratories and universities whose primary concern is maintaining power. There is also a common complaint about "power control," the shortage of funds and the brain drain resulting from Chinese students who study abroad but who do not return. To help resolve these problems, many Chinese professionals are encouraging the government to set priorities for

information technologies developments, based on market demands rather than the counsel of state planners.

Professor Li has stated that China realizes that the freedom of information flow is important for economic development and that CERNET is a form of infrastructure designed to address the exchange of information, which, it turn, will help overcome some of the problems listed above which are handicapping China's development.

### **The Current Chinese Government's Policies on Building Electronic Networks**

The Chinese government is aware of the need of developing backbone computer networks as a means of integrating the sector, regional and cross-regional networks. By supporting backbone developments, the government can be instrumental in enforcing its control by providing the initial funding, operating regulations, and standards for these networks. The Chinese government then can maintain power control over computer and information networking by: 1) limiting network services (e.g. banning certain groups), 2) limiting users (e.g. providing access to only academic institutions, certain businesses, etc.) and/or 3) monitoring, filtering or auditing traffic (e.g. eavesdropping).

In February 1996, the Chinese government issued a directive regulating the use of the INTERNET as a backbone. According to the regulations, all international computer transactions must use the inward and outward port channels provided by the MPT or if they intend to be linked to other networks abroad. Currently, there are six ports operating. All the existing interactive networks, after registration, will be subject to close supervision by the MPT, the Ministry of Electronics Industry, the State Education Commission and the Chinese Academy of Sciences. Special software will be installed at these information ports to filter out data from overseas sources known to offer pornography and "counter-revolutionary" or subversive ideas. In the meantime, all interactive networks operations must be approved by the Ministry of Public Security. Although this information flow control structure is technically questionable, the Chinese officials intend to try to impose their will on such network operations. In this way, the government can do what it wants in monitoring the international transmissions or shut them down.

The catch-twenty-two is that the Chinese government really wants to get their country connected with the Western world but to do this in their own way. Beijing recognizes that advanced technology transfer is a prerequisite for a modern economy and cannot be contained within its national borders. The issue is that government wants to have cyberspace and ideological control. By linking with the INTERNET, they do not expect absolute free flow of information. The Chinese policy is to encourage economic development, introducing Western capital and

advanced technology while resisting foreign influences. In the process, they wish to retain tight political and ideological control.

As a result, rather than try to choke off INTERNET access, the regulations instead appear to be steering the flow of electronic information through these officially controlled ports so that it can be better monitored. This technique is viewed as a bid to control the INTERNET flow. Thus, the State-run and private Internet Service Providers (ISP) are concerned about the future of China's on-line industry, because all INTERNET users are required by the state to register with the Ministry of Public Security.

The Chinese government realizes that it cannot fully control the information flow on the Net, but it surely can force users into self-censorship. This strategy may partially work in the short run. These commercial and private ISPs have no recourse but to pledge to exert self-censorship in their business network operations or to be shut down.

Chinese policy makers are guided by political, economic and social concerns in their policy formulation process. At this stage in China, those concerns, unfortunately, have been more political than economic. In contrast to the concerns in Western countries about public access to general information and the improvement of health care and education, the concern in China concentrates more on ensuring efficient government planning and control plus facilitating the operation of large state corporations. In China, the instruments of mass communication are mobilized by the central government to aid in the tasks of nation building. The media, therefore, is expected to support central authority, not challenge it. Freedom of the press should be restricted according to the development needs of the society as defined by the government.

As stated, in China the policy-making process is not only directed by political considerations but also by cultural concerns. The Chinese culture values obedience to authority and homogeneity more highly than individual rights. For example, privacy is never an issue in China but is a major concern in the West. For example, the core of the outcry against the Communication Decency Act in the USA boils down to the privacy issue which is not a prime concern in China. The government concern is command control, for they believe Western democracy will generate chaos in China.

The Chinese government believes that international information flow control can be enforced by the key monopolistic, national backbone network called CHINANET. CHINANET is a national public computer network administered by MPT's Data Communication Bureau (DCB). CHINANET's backbone uses a three-layer topology. The increase from three to six high-speed links to the global INTERNET will hopefully reduce the congestion currently being experienced. In an ambitious bid to take the lead in the country's information highway construction, the MPT is building a 31-node nationwide backbone network. In addition to the two existing 256 Kbps international links in Beijing and Shanghai,



the CHINANET backbone will have one additional international line at Guangzhou. Even before the completion of the CHINANET backbone the State Council declared MPT the official leader in China's international connections business.

CHINANET is China's commercial ISP operated by the government via the MPT. Individuals are able to purchase INTERNET accounts directly from CHINANET. CHINANET international links to the INTERNET uses DDN (Digital Data Network) and CHINAPAC (China National Public Data Network) circuits to form its domestic network.

In addition to the CHINANET, there are a handful of private commercial companies now beginning to offer individual access to the INTERNET. Recent regulations have allowed new private ISPs to connect to INTERNET via CHINANET if minimum quality of service standards are met. Connecting private ISPs to the centrally administered CHINANET enables government authorities to monitor, audit and potentially censor INTERNET services and content offered by these new private ISPs. Private ISPs not only need CHINANET for their international connectivity but also to coordinate the following technical requirements in order for interoperability to take place: 1) network access point NAP; 2) INTERNET exchange establishment (IX); 3) network information center (NIC) services; 4) network operation center (NOC) services; and 5) domain naming system (DNS) standardization.

One firm that is trying to enhance China's economic development is UNICOM. UNICOM is a mainland based company that is attempting to develop the wireless technologies as a means of addressing China's growing demand for basic communication services. UNICOM is using radio services such as cellular and paging networks to service fixed locations or limited areas. These wireless loops are easier and cheaper to install and the investment in this technology is increasing. MPT has adopted Motorola's high-speed flex system as China's national cellular standard. Many Chinese have developed codes to communicate messages through the use of pagers. That is, a code of 72 is understood to mean "bring home a packet of tea." A longer code could contain other business or undesirable political messages that someone wants to communicate. As stated earlier, the Ministry of Public Security wants to prevent this type of message disseminations.

China buys such foreign wireless technology because it has very little choice. It does not, however, currently permit foreign companies to own or operate communications networks—even on a joint-partnership basis. Foreign companies, however, may provide selected services, with MPT's permission. They must pay the government for this privilege. As stated, networks are controlled by government entities such as MPT, Ministry of Electronic Industries and others. An exception is UNICOM which is a network service supported by a composite group of ministries and the military and is an anomaly. Their controls are enforced because the government wants the network operations to reflect their ideological

policies. The question is: "Can the government enforce such a policy and still unleash the Chinese abilities and capabilities to compete with the West?" many Chinese professionals believe there is trouble ahead because, in technological transfers, much still needs to be achieved.

For instance, CERNET is still under construction. Its hopeful goal is to link all the universities, along with many secondary and elementary schools, into an integrated operation. The China Academic Science Network (CASNET) wants to link all the major research institutes, some of which will be INTERNET Service Providers. CHINANET, the commercial INTERNET Service Provider operated by MPT, is in the process of building a high speed nationwide network and is a major ISP. In addition, MPT hopes to build a post office banking network for all of China.

These governmental efforts are receiving some support from the West. For example, SPRINT is involved with Jiangsu Provincial Data Telecommunication Bureau to help connect users to the INTERNET. IBM, in conjunction with Jiao Tong University of Shanghai, is helping to build a fiber network in support of video conferencing services to certain government agencies. Digital Equipment is helping to develop a multimedia network for Guangzhou.

### **The Use of Firewalls and Networking Security**

The reader should note that there is much work and capital going into the development of these many, many individual electronic networks. It does not appear, however, that sufficient effort is expended to make these nets technically secure. This is because of lack of skills and money. Eventually, this security problem will become self-evident. Then money will be found and skills will be developed. The government's serious intent, however, is to provide secure operations by building a national firewall system for all computer networks with INTERNET access throughout China. As stated earlier, they intend to control international access to China by using a limited number of information ports. Such ports will enforce an access control policy between China's networks and the INTERNET. They will be reinforced by Chinese-built firewalls. For information warfare reasons, the government does not permit the use of Western built firewalls in their electronic wall. The Chinese motivation for building such a national firewall system is rooted in its ideology of service to the state, which is regarded as more important than individual freedoms.

INTERNET firewalls allow MPT, the network manager, to create centralized information ports that act as "choke points" which help keep unauthorized users such as hackers, crackers, vandals and corporate spies from using or abusing the Chinese networks.

Firewalls can help prevent potentially vulnerable services from entering or leaving the Chinese networks. In addition, they can provide protection from

various types of routing attacks. INTERNET firewalls simplify security network management, since network security is concentrated on the firewall systems rather than being distributed over the many network sites.

When designing an INTERNET firewall system, a number of decisions must be addressed by the Chinese government and MPT as the network manager. As stated, MPT is the organization that is responsible for network security enforcement. It has published a set of policies and subsequent regulations that enforce the implementation of those policies. These focus on:

1. Legal aspects of security laws which essentially deal with penalties for non-compliances.
2. Management responsibilities for enforcing the law which deals with the responsibilities of network owners and users.
3. Technical issues and concerns which deal with the creation of standards and the resolution of technical problems.

For risk management purposes, the Ministry partitions the security process into four classifications. They are: 1) most confidential, 2) very confidential, 3) business sensitive and 4) open aspects. It is unclear what policy/law/regulation pertains to which classification.

For example, an INTERNET firewall does not stand alone - it must be part of Public Security Ministry's overall security enforcement policy. This policy must be based on an understanding of the needs of risk management, risk analysis and risk assessment. If the user organization does not have a clear understanding of the desired security perimeter defense and the implementation of the appropriate policy, the selected INTERNET firewall can be circumvented to expose the other Chinese networks to attack.

Many Chinese professionals are aware of these limiting issues and operating concerns but lack the power to influence the Ministries which are in control.

Nevertheless, some Chinese professionals are working on building INTERNET firewalls, based on such models as single-homed bastion host, dual-homed bastion host and screened subnet configuration. It is too early to tell which firewall model will be adapted and become the standard. In any case, a need exists for integrating firewall operations with anti-virus software and content monitoring by network managers. This is necessary because the borders between intranets and INTERNET is becoming less distinct.

A firewall itself must be designed to prevent undesirable penetration. If a firewall's defense is compromised, not only is its protection ability eliminated but the firewall's defense can be turned against its network owner. The most cost-effective way to ensure secure operation is to use a trusted security perimeter defense approach as support to the firewall. Firewalls have traditionally been built on the bastion host processors, routers or gateways using the UNIX operating system. Such a system offers standards for security extensions as well as having

the largest and most extensive set of available tools. There is no doubt that China is trying to build a secure Chinese-UNIX called COSIX (Chinese Operating System based on UNIX-version 2.4). This is consistent with the development of a Chinese firewall which would require a trusted bastion host platform. The cost of such a firewall system is expensive. Depending on its complexity and the number of networks protected, the costs can vary between \$4,000 and \$30,000 per installation. The primary advantage for the Chinese in building their own UNIX is that they will have complete control over the end-product firewall proxy scanning features, a national major network security objective.

China is proceeding with the building of their electronic wall and is being reinforced by firewall technology. There is no one correct answer for the design, deployment or evaluation of China's INTERNET firewalls. It all depends on what security policies China wishes to enforce, that is, the technical skills of their security professionals, acceptable costs and the threats perceived. Most security design, answers/solutions must incorporate the operating and/or the environmental constraints involved.

The Chinese INTERNET, CHINANET, CERNET and other telecommunications network infrastructure is a bit of an enigma. China has deployed all sorts of technology currently available and yet has a low level of national user penetrations. It is a highly regulated monopoly, yet has strong competition from local and foreign sources. It has no national policy of universal telecommunications service, causing many barren service areas. Yet there are some areas that have advanced state-of-the-art approaches to network management. The implications from controlled access to INTERNET which the Chinese people will eventually need to have for business reasons is a handicap. Can this enigmatic approach to network management survive and still compete with the West?

In essence, there is a strong need for the Chinese government to address the required electronic network capital planning needs, information security architecture and risk management in order to become an integral part of the 1996-2000 Ninth Five-Year Plan.

### *Conclusion*

The Chinese government can be brutal and authoritarian in its command economy type of management. But China is not, currently, an absolute totalitarian society. The country is undergoing enormous transformation in economic, technological and social change which, in turn, is improving life for millions of people. Political changes marked by speed and scale are bound to follow the international and local use of telecommunications technology. These networking systems are creating much business and personal benefits for the Chinese professionals and for the average person. Therefore, political command control over the people is slowly changing and more economic and social benefits are bound to follow. This is

because communist ideology is losing support which, in turn, permits the Chinese entrepreneurial people to operate more like semi-capitalists. China's current political institutions are being affected by the mounting pressure created by this rapid economic growth plus the people's desire for more business freedoms. The government's concern is that Western-style freedoms will lead to much disorder and, perhaps, chaos in Chinese society. Consequently China's governmental institutions are trying to maintain control over these issues, but it is a losing battle.

### *References*

The source material used in preparing this paper is based on discussions with people from the following organizations plus review of the listed publications:

- Ministry of Public Security (Computer Management and Inspection Bureau, Beijing)
- Tsinghua University, Beijing
- China National Computer Software and Technology Service, Beijing
- Ministry of Posts and Telecommunications and Data Communications Technology Research Institute, Beijing
- Shanghai Computer Society, Shanghai
- Jiao Tong University, Shanghai
- Shanghai - CAST Software Corporation and Shanghai Institute of Computing Technology
- Shanghai Stock Exchange
- Guangzhou Chinese Computer Federation and The Science and Technology Institute
- Guangzhou Bank of Commerce and Industry
- Ministry of Public Security "Temporary Rules of People's Republic of China on the Management of International Networking of Computer Information Networks, Beijing, PRC, 12 February, 1996

### *Publications*

- 3 Com Corporation, "Internet Firewalls and Security", Technical Paper, Santa Clara, CA, 1996
- Zhang Gendu, Gao Chuanshan, Zhang Shiyong, "Survey of Network Interconnection and Information Integration", Shanghai International Computer Conference Proceedings, 1996 pp. 17-61
- William Yurcik and Zixiang Tan, "The Great (Fire) Wall of China: Internet Security and Information Policy Issues in the People's Republic of China", Paper presented at the Telecommunications Policy Research Conference, Solomons Island, MD, October, 1996
- WEI WU, "Great Leap on Long March: Some Policy Issues of the Development of the INTERNET in China", AMIC Conference, Singapore, June 1-3, 1996