The Architecture of Control: Internet Surveillance in China
James A. Lewis, Center for Strategic and International Studies
July 2006

Security concerns shape China's official internet and information technology strategies. These include concerns shared by many countries: promoting a strong and growing economy, providing information assurance, and defending against foreign intrusions into China's information space. Most importantly for the Chinese, information security includes a political element not found in many other nations – control by the party and the state over communications and the flow of information. The rapid spread of internet access and mobile communications pose a serious challenge to this goal. In response, China's security apparatus is reorienting its informational defenses. In the past, the emphasis was on blocking access - the "great firewall." In the future, the emphasis will be on the monitoring and surveillance of online activities.

China's primary objective in internet security is political – preventing IT from eroding the regime's authority. Information security is defined in China as "a comprehensive concept understood in a broad sense, and it involves political, economic, cultural, ideological, media, social and military level or field." It includes "data, system, network, infrastructure."[1] Chinese officials worry about the potential of the Internet to contribute to the loss of state secrets, offer new avenues for organizing dissent and opposition, and spread "harmful information." This makes controlling access to "harmful network information" and the ability to monitor and intercept communications top priorities.[2]

For China's leadership, one particular set of events demonstrated the risks of not securing networks. This was the use of the Internet by Falun Gong to bypass existing security monitoring and organize demonstrations within China in 1999. Demonstrations occurred simultaneously in thirty cities, including Beijing, and involved thousands of demonstrators. The Internet was one of the primary tools used to organize the demonstrations. In this, the Chinese faced a problem shared with other nations' security services: the ability of diffuse groups of opponents without much in the way of hierarchy or organization to take advantage of the global commercial communications infrastructure to organize, win support, and carry out operations. The Falun Gong demonstrations made China's political leadership and security services realize that they faced a new and potentially damaging vulnerability.

China's internal security apparatus is extensive and China's intelligence and security services have far-reaching domestic powers. Their missions include not only conventional counterterrorism, counterespionage, and what we would call critical infrastructure protection, but a political role that reflects the continuing (albeit diminishing) absence of a clear line between state and party in China. A heritage of security practices from an earlier era emphasizes secrecy, vigilance, and action against both foreign intruders and internal dissent. China appears to apply these security policies and practices to new technologies and the behaviors they produce. Directed by the State Council, there is an interlocking series of efforts by competing ministries to build a layered approach to network and information security. It includes:

--   An encompassing structure of Internet regulation that expands existing security regulations and applies them to Internet users, Internet cafes, ISPs, and other network service

providers. These regulations give the state the authority to compel actions or behaviors.

--   A complementary set of regulations that gives Beijing the authority to regulate software, in particular network security and encryption software.

--   Government organizations and personnel with an Internet security/control mission, including the Ministries of Culture, Information Industries, Public Security, and State Security.

--   A strong technological component that uses network architecture, human intervention, and software tools for monitoring online activity and interfering with access to information.

--   A system of voluntary compliance and self-regulation among the larger private networks and service providers to complement the already high degree of control in state-operated systems.

--   A long-term effort to move to reliance on indigenously developed software that would have the benefits of both greater control by Beijing and less potential for malicious activities by foreign intelligence services.[3] The development of indigenous software is a crucial element of China's planning on how to manage security risks created by the Internet.

Regulation
Much of what China has done in regard to Internet security is an effort to extend existing control mechanisms into the new medium and to preserve, to the extent possible, political control. Erosion is unavoidable, but Beijing probably hopes that it can preserve enough control so that a combination of economic growth, nationalist appeals, and a slow increase in the government's openness and accountability will avoid any destabilizing tendencies from the new information technologies.

China has perhaps the most extensive set of regulations for the Internet of any major economy.[1] The Ministries of Public Security, State Security, Information Industries, and Culture are the primary regulators of the internet and have issued broad, overlapping, and at time ambiguous regulations. Provincial and local government rules reinforce national regulations. Beijing and China's provincial governments have relied much more heavily than other nations on regulation and licensing of Internet activities, including access, content, the use of encryption and, potentially, even the kind of software that can be used.

The absence of privately-owned infrastructure simplifies security tasks. The Chinese government uses its control of Internet access, network operations, and the domain name system to advance its security agenda. Government control of the Domain Name System (DNS) allows officials to identify companies and organizations using the Internet and make adherence to security regulations a condition for DNS services.[2] There are also reported instances where

---

[1] China's laws and regulations fall into hierarchical categories: laws enacted by the Standing Committee of the National People's Congress; administrative regulations issued by the State Council; local administrative regulations issued by local governments of provinces, autonomous regions, or municipalities reporting directly to Beijing; the final category includes administrative regulations and rules issued by ministries and local governments.

[2] China shared the experience of many countries in the late 1990s that pursued a solution to online authentication

government personnel change the domain name server record of forbidden sites to reroute users to approved material.[4] At the same time, growing privatization has led China to begin to replace direct state control with regulation as a mechanism for achieving policy goals.

Prior to the 1993 "Golden Bridge" Project, China connected to the Internet through government research institutions. The State Council was careful to put Internet regulations into place in 1994, before allowing commercial access to the Internet (which began in early 1995). Since that time, China has implemented an additional sixteen regulations that relate to Internet security. Chinese Internet regulations serve two primary functions. First, they give Ministries the authority to regulate networks, software, online behavior and content through administration rulings and other mechanisms. Equally as important, they apply existing security legislation and regulations to the Internet. The regulations extend Ministries' existing responsibilities into cyberspace, with the result that perhaps a dozen ministries and agencies have Internet regulatory functions that sometimes overlap. The regulations often do not require specific actions to improve cyber security, nor do they reference security standards such as BS 9779. Instead, they impose a general requirement to make networks secure, list a set of behaviors that are not allowed, and assign broad responsibility for enforcement to an agency or agencies.

China wrote its first network security regulation in February 1994. The "Regulations on Protecting the Safety of Computer Information Systems of the People's Republic of China" authorized computer security functions for the Ministries of State Security and Public Safety and the National Administration for the Protection of State Secrets (NAPSS). The State Council published additional regulations in February 1996; the Ministry of Public Security issued its own implementing regulations in 1997; regulations from the National Administration for the Protection of State Secrets were published in January 2000; and the National People's Congress approved Internet edicts in December of 2000.

Although most of the Internet regulations are in the form of edicts rather than legislation, China amended its criminal laws in 1997 to deal with hacking and other Internet crimes. This legislation was expanded in 2000 when the Ninth National People's Congress issued the "Decision on Ensuring Internet Security" which created criminal penalties for computer crimes. This criminalized a number of activities when conducted on the Internet, including fraud or the use of false information for financial purposes. An APEC Survey suggests that China is on par with most other Asian countries in terms of the scope and effectiveness of its cyber crime legislation.[5] A few cases have been reported where China has imposed the death penalty for some cyber intrusions, but this sentence seems to have derived from the nature of the crime (robbing a bank) rather than from the use of the Internet.[6]

A surprisingly large number of Ministries, subsidiary agencies, and State Council bodies exercise oversight for Internet activities and information technologies. They include the Ministries of Public Security, State Security, Information Industries, Foreign Trade and Economic Cooperation, and the Ministry of Culture. The responsibilities of these Ministries in regard to IT

---

based on Public Key Infrastructure (PKI) technologies, Like these other countries, however, China has found that PKI has not provided an adequate solution for authentication for reasons of cost, interoperability, and complexity of operation.

and the Internet overlap, and competition among Ministries for bureaucratic turf or for commercial advantage for Ministry-owned companies helps to shape Chinese Internet regulations.

China's 1994 network security regulation made the Ministries of Public Safety and State Security and the National Administration for the Protection of State Secrets (NAPSS - formerly the State Secrets Bureau) responsible for network security. These two agencies, along with the Ministries of Information Industries and Culture, are the primary regulators of the Internet. MPS bears primary responsibility for securing national computer systems, monitoring Internet use, and acting against cyber crime. All Internet users must register with the MPS, and the Ministry's Internet Products Testing, Evaluation, and Authentication Center works with the PLA-affiliated State Secrecy Bureau and other organizations involved with state security to certify for the sale and use of hardware, software, and data security products. MPS is responsible for Internet monitoring, and Public Safety Bureaus throughout China are responsible for oversight of China's tens of thousands of Internet cafes and their users.

China's Internet regulations incorporate key provisions of the 1993 State Security Law that gives the Ministry of State Security (MSS) the authority to take action against individuals whose conduct harms the PRC state security. Portions of the State Security law are incorporated without change in Internet regulations. The most important provisions include prohibitions against subversion or the overthrow of the socialist system, providing state secrets to an enemy, or engaging in sabotage. The Ministry has the discretion to decide when an activity falls into one of these prohibited categories, giving it very broad authority. MSS also has, like the PLA, research institutes that work on network security technologies. MPS and MSS reportedly are more likely to compete than cooperate in some aspects of Internet security such as monitoring efforts to access forbidden websites.

NAPSS is the implementing organization for the Party's Committee for the Protection of State Secrets, which is part of the Central Committee. NAPSS is responsible for classifying secret information. NAPSS has worked with the Ministry of Public Security to counter the Internet and potential leaks. It forbids the release, discussion, or transfer of state secrets via e-mail, chat rooms, electronic bulletin boards, or newsgroups. Web sites may not publish unreleased news on the Internet without permission. NAPSS holds site operators liable for content on their sites and requires them to either delete or report suspicious information to it. NAPSS also requires web site operators to implement safeguards against network security breaches. Additionally, it requires registration of encryption software by private companies and monitors its use.[7]

The Ministry of Information Industry (MII) was created in 1998 by merging the former Ministry of Post and Telecommunications and the Ministry of Electronics Industries. MII is responsible for constructing and managing secure networks for the party, government, and the military, and for guaranteeing information security. MII has oversight of the network, not content. It uses control over Internet Service Providers to block objectionable website and postings from a central location in Beijing where, according to some reports, it has as many as 30,000 employees dedicated to Internet monitoring. The Ministry of Culture (MOC) regulates Internet content. MOC regulations ban internet activities that are harmful to the reunification of the nation and integrity of the country's sovereignty and territory; undermine national unity; disclose state

secrets; advertise obscene or superstitious material or exaggerated violence; and defame or insult people.

The government can also use its control of the domain name system in China to enhance security. A Ministry of Information Industries Ministerial regulation issued on August 1, 2002 sets out a number of requirements for regulating the national domain name system. Section 10 requires authorization from the MII for high-level DNS management activities. Section 12 lays out a number of requirements for entities engaged in providing domain name services, including a requirement to have put in place unspecified "information security" safeguards, along with other unspecified MII conditions for operation.

Section 19 of the DNS regulation repeats China's internet content restrictions and specifies that they apply to DNS service providers and also to "any organization or individual" using a domain name issued in China. It forbids the inclusion of certain content in registered domains, including those that jeopardize national security; leak state secrets; intend to overturn the government or disrupt state integrity, national honor, and national interests; violate the state religion policies or propagate cult and feudal superstition; spread rumors, disturb public order, or disrupt social stability; spread pornography, obscenity, gambling, violence, homicide, terror, or instigate crimes; or commit libel against others and infringe upon other people's legal rights and interests. A catch-all clause at the end also forbids anything else prohibited in any other law or regulations. Section 20 caps all the other requirements by stipulating that DNS registrant applicants must observe all other Internet laws.[8]

Technology
Western attention is drawn to anecdotal reports of internet users being scolded by monitors for attempting to access forbidden sites or of connections suddenly and irreparably terminated. Given the steadily growing number of internet users in China, human surveillance is inadequate and the Chinese government has placed a new emphasis on the development of IT solutions, particularly the use of software tools to automate the tasks of surveillance and interception.

The government at first appears to have hoped that State control of the internet backbone, combined with address blocking technologies, would be enough to limit the informational risk created by the Internet. This was the era of the "Great Firewall of China," which attempted to block certain IP addresses using firewalls and proxy servers operating at the government-controlled connections to networks outside of China. A number of Chinese and western hackers take the Great Firewall as a challenge and have successfully designed software or techniques that allow Chinese internet users to bypass it.[9]

In response, Beijing has placed increased importance on automatic monitoring and surveillance, and on the extensive use of filtering and monitoring software. Many of these are conducted under the aegis of the Golden Shield Project, one of several "Golden Projects." The Golden Projects are telecommunication and information infrastructure modernization initiatives that began in 1993. The fifteen initiatives included e-commerce and e-government programs. Golden Shield, begun in 2000, seeks to expand the regime's ability to engage in political and security monitoring for domestic security purposes, including the wide use of video surveillance of public spaces and an expansion and automation of Internet surveillance and

telecommunications interception capabilities. Golden Shield is similar in concept to many of the national technical means developed or being developed by western nations for use in foreign intelligence, except that it is aimed at China's domestic population.[3]

Golden Shield software aims to increase domestic security forces' surveillance and access to communications and their control of information in China. The development of software for surveillance, voice recognition, interception, switching, and decryption is the reverse side of China's efforts to build a domestic IT industry. While its security services have traditionally depended on the use of large numbers of personnel to monitor the civilian population and communications, the "informatization" of China and the heavy use of information technologies for communications by China's population have led China to seek to automate security processes. In a traditional division of labor in signals intelligence between acquisition and assurance, Golden Shield's acquisitions programs are complemented by national programs to provide information assurance by developing indigenous software and hardware, particularly an operating system and CPUs. These measures provide information assurance by reducing the potential for foreign access.

Effective automated communications monitoring software is particularly crucial for Golden Shield to succeed. If rumors that security agencies employ 30,000 Internet monitors are correct, each agent would need to cover ten to twelve cyber cafes.[4] In addition, the need to monitor text messaging from mobile phones and PDAs adds millions of new messages every day to the surveillance burden – one official estimate showed 240 billion SMS messages sent in 2003.[10] Even with assistance from personnel at the leading Chinese Internet Service Providers (ISPs) and telecom companies, this is a crushing burden where the only possible hope for success is to automate surveillance.

Several Ministries subsidize Chinese IT firms to build software for remote access, management, and automatic monitoring of networked computers. A number of these Chinese products are already deployed. The Ministry of Public Safety (MPS) has ordered cyber cafes throughout the country to install "Filter King," "Internet Cafe Management Specialist," "Mei Ping," and other remote management and monitoring software.[11]

Human rights groups have charged that Golden Shield also depends on the expertise of western technology companies.[12] Golden Shield is much more ambitious in its technology and scope than previous efforts and will involve western technology even if there is no assistance from western companies. Western companies have either denied these accusations or refused to comment. China is unlikely to be comfortable in depending on western suppliers for these sensitive technologies.

Surveillance and Self-Regulation
China's regulation of Internet activities complements an already large and powerful internal security apparatus. While some elements of this apparatus are losing effectiveness (such as the work units and neighborhood committees that once oversaw most peoples' lives), Beijing

---

[3] It is reasonable to assume, however, that technologies developed for Golden Shield, such as voice recognition, will probably also be used to automate and modernize China's sigint capabilities.
[4] This takes the conservative estimate of 110,000 cybercafes in China and assumes three shifts for monitors.

appears to be working on a technology-based approach to internal security. Building new tools for surveillance and control is an important element of the national emphasis on and commitment of resources to high tech research and development and to creating a strong IT industry.

Identity management requirements imposed on internet users reinforce self-regulation. Regulations promulgated in 1994 require internet service providers and internet users to register with their local Ministry of Public Security Bureau. Patrons of Internet cafes must register with the café operator, using their national identity cards for each session. Since few Chinese Internet users regularly use some form of electronic authentication, the authorities are forced to rely on paper credentials. This complicates the use of monitoring software.

As a complement to regulation and agency oversight, Chinese authorities see self-regulation and self-discipline as a key part of their cyber security strategy. They have pushed some of the monitoring burden onto Internet Service providers (ISP) and cyber cafes by making it a condition of their approval to operate. They have also obtained from more than thirty ISPs who are members of the Internet Society of China (an entity sponsored by government ministries that is not part of the larger, international Internet Society) a "Public Pledge on Self-Discipline" that commits ISPs and others to control content and to cooperate with security forces. The four-page pledge commits ISPs to monitor and block foreign websites, accept supervision and criticism "from the public," and (in what sounds suspiciously like regulatory language changed at the last minute to a voluntary pledge), to allow the "administering agency" to investigate violations and revoke membership. China's Xinhua news service reported that ISPs have also agreed to block twenty categories of content that are listed in the text of an agreement with the government.

Conclusion

> "Problems concerning information security have turned out to be a major obstacle in the development of the national economy."
>> Xu Guanhua, Minister for Science and Technology.

An emphasis on security should not minimize the importance of other motives in Chinese regulatory activities. Pursuit of commercial advantage is one of these, and it is likely that some officials do not see commercial advantage and improved security as mutually exclusive. A September 2003 requirement from the State Council that Ministries must buy domestically-produced software in the next acquisition cycle aims to provide both incentives to the local software industry and to reduce the use of foreign software that the Chinese fear may contain back doors.[13] While there is a clear security motive, there is also a desire to give Chinese firms an advantage. Often, the Ministries issuing regulations own or have invested in the firms they seek to aid, and at times Ministries will issue competing regulations to give "their" companies an advantage not only over foreign firms, but over firms "owned" by other ministries.

It may be that China relies on a degree of bluff in its efforts to secure the Internet. By emphasizing monitoring and by publicizing draconian punishments for those caught violating their Internet edicts, security agencies may hope to give the impression of an effective and far-reaching system that will deter people from challenging them. However, China is making a major effort to find technological solutions to the problem of internet monitoring. China's

extensive internal security apparatus and limited protections and rights for its citizens give it a much greater ability than any other country to monitor Internet activities. China's internet monitoring effort is performed by human watchers, both in government agencies and in ISPs, by monitoring software installed in cyber cafés, at Internet Service Provider facilities, and elsewhere, and by indirect government control of the telecommunications infrastructure and international connections. These factors give the Chinese government a considerable degree of insight into Internet activities. However, these advantages have proven to be insufficient to provide the level of control Beijing wants or to improve network security.

End Notes

[1] Private communication, Chinese technology Institute staff, May 2004

[2] Cheng Ying, "All quarters cooperate fully to construct the network security system to become the Political Consultative Conference people in attendance mutual recognition," New China net, March 9

[3] Yang Gu, Guangming Daily, Wednesday, June 30, 1999, "Ministry of Information Industry (MII) Advises Government Agencies on Prudent Use of PIII" http://jya.com/cn-p3-peril.htm; Sumner Lemon, "Intel, Microsoft Under PRC Press Attack," ComputerWorld Hong Kong, July 6, 1999 http://www.cw.com.hk/News/n990706001.htm

[4] Julia Scheers, Net Dissidents Jailed in China, Wired News, February 24, 2004, http://www.wired.com/news/politics/0,1283,62391,00.html?tw=wn_story_mailer

[5] APEC Survey of Cybercrime Legislation for China, 2002, http://www.apectelwg.org/apec/comple/clecb/ChinaSurvey.doc

[6] BBC, "China Plays Net Nanny," February 12, 1999, http://news.bbc.co.uk/1/hi/world/asia-pacific/278452.stm

[7] Bureau for the Protection of State Secrets (State Secrets Bureau), http://www.chinaonline.com/refer/ministry_profiles/secrets-3-s.asp; Amnesty International, "States Secrets Legislation Open to Abuse," http://www.amnesty.org/ailib/intcam/china/china96/secret/secret2.htm; Penny Lai, Christine Tsai, Agnes Yip, "e-Commerce Laws in China and Hong Kong: Integration or Separation?" Cyberlaw and Telecommunication Policy in Greater China, City University of Hong Kong, http://newmedia.cityu.edu.hk/cyberlaw/gp16/intro.html

[8] China Daily, New Regulation Eases domain Access," December 13, 2002 http://service.china.org.cn/link/wcm/Show_Text?info_id=51041&p_qry=china%20and%20internet%20and%20information%20and%20center

[9] Paul Festa, "Cracking the great firewall of China," May 20, 2003, CNET News.com http://news.com.com/2100-1028-997101.html?tag=fd_top; Niall McKay, "China: The Great Firewall," Wired, December 1, 1998, http://www.wired.com/news/politics/0,1283,16545,00.html

[10] South China Morning Post, "Great Firewall has little chance of stopping messages," July 7, 2004, Http://www.wirelessweek.com/article/NEa0705405.7iw?verticalID=110&vertical=Wireless+Internet

[11] Information Centre for Human Rights and Democracy, Hong Kong

[12] See Greg Watson, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," International Centre for Human rights and Democracy Development, http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html#ToC15,

[13] ZDNet, China blocks foreign software use in gov't," September 3, 2003, http://www.zdnet.com.au/news/software/0,2000061733,20277354,00.htm