



Rights & Democracy
International Centre for Human Rights
and Democratic Development

1100-1001, de Maisonneuve Blvd. East, Montreal, H2L4P9, Canada
www.ichrdd.ca ichrdd@ichrdd.ca

Review of China's Internet Regulations and Domestic Legislation

China's Internet regulations and legislation are guided by the principle of "guarded openness" - seeking to preserve the economic benefits of openness to global information, while guarding against foreign economic domination, and the use of the Internet by domestic or foreign groups to coordinate anti-regime activity. While researchers often refer to a national Internet strategy, there is in reality, no single "official" articulated strategy, written down and approved by the Chinese leadership. The research here is therefore, an aggregation of the interrelated Internet security policies and regulations pursued by the various bureaucracies.

In China, the security apparatus includes all those organizations responsible for internal or external security. The two most important are the Public Security Bureau (PSB), which is responsible for internal security, and the Ministry of State Security (MSS), which handles foreign civilian intelligence-gathering and internal counter-intelligence against foreign threats.

As China modernizes its telecommunications infrastructure, both organizations have evolved corresponding claims to regulating Internet security – the global character of the Internet makes it difficult to define the distinction between internal and external security. The stakes are high – for the government, as China integrates into the global economy, and for the would-be “cyber-dissident”, who ultimately faces the death penalty for illegal use of the Internet. The bureaucratic environment for information security is very complicated, characterized by on-going struggles over jurisdiction and authority.

The Public Security Bureau

The Public Security Bureau is in charge of maintaining China's civilian network security, both physical and on-line. The primary PSB unit charged with maintaining network security is the Computer Management and Supervision Bureau, which was founded as early as 1983. Its responsibilities are formally codified in "*Computer Information Network and Internet Security, Protection and Management Regulations*," which was approved by the State Council on December 11, 1997.

Under the 1997 regulations, the PSB is tasked with oversight of Internet Service Providers and all other commercial enterprises that have users with Internet access. According to Article 8, "units and individuals engaged in Internet business must accept the security supervision, inspection, and guidance of the Public Security Bureau." The PSB requires Internet companies to provide monthly reports on number of users, number of page views, and user profiles. ISPs are also required to assist the Public Security Bureau in investigating incidents involving law violations and criminal activities involving computer information networks. Like network security, responsibility for maintaining security lies with the ISPs, and violations by users will result in the cancellation of the ISP's business license and its network registration, fines, and possible criminal prosecution of both the company staff and the user (Articles 20-23).

As a direct result, ISPs have implemented a series of self-censoring policies, in order to avoid the wrath of the authorities. So-called "Big Mamas" (*da mama*) are paid ISP employees who lead "armies" of volunteers patrolling chat rooms and bulletin boards erasing unacceptable political commentary.

The regulations also define the acceptable uses of the Internet by the users themselves. First, users are required to register with the PSB, filling out an application form that links their personal information with their network account information. Under Article 13, users may not lend or transfer these accounts to others. Once online, users are not permitted to use the Internet to create, replicate, retrieve, or transmit certain kinds of information :

- (1) Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;
- (2) Inciting to overthrow the government or the socialist system;
- (3) Inciting division of the country, harming national unification;
- (4) Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
- (5) Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;
- (6) Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder,
- (7) Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
- (8) Injuring the reputation of state organs;
- (9) Other activities against the Constitution, laws or administrative regulations.

The PSB is empowered to control and set standards on information security products in China. The PSB first addressed the technology certification issue as early as February 1987, when the Standardization Management Committee was formed to deal with "criminal investigation technology, traffic control technology, computer application technology, and public security technology and equipment".

Under the 1997 law on network security, all information security products must first be evaluated at a PSB testing facility in Tianjin, currently unidentified. The Tianjin facility was mentioned in promotional materials for the 26-28 October 1999 "China International Information Security Exhibition," and the "Security China Exhibit" in November 2000. Both events were sponsored by the PSB. This ability to certificate Internet security products places the PSB in a unique position, inevitably leading to close relationships with foreign and domestic companies that market information security products. These affiliations are allegedly both direct and indirect, including outright ownership, de facto control, strategic alliance, or simply certification and approval oversight.

Building a Legal Framework

In the past year the Chinese government has rapidly built-up a legal framework on the foundation of the 1997 regulations. In less than one year, no fewer than three laws were passed, all of them extensive.

Legislation passed on October 1, 2000, deals with the involvement of foreign investments in the Internet sector and the control that operators have over their sites. It requires that any foreign companies wishing to invest in this sector obtain an authorization from the Ministry of the Information Industry. In addition, managers of Chinese sites are responsible for editing and censoring the content published on their sites, and, if not, risk fines or closings.

One significant new aspect of the law is that they are now required to report any infractions to the proper authorities. They must also be able to provide the authorities with the addresses of Internet users who have visited their site in the past sixty days. This new regulation also reinforces the prohibition of any "subversive" information on the Internet, particularly documents which incite "ethnic hatred, discrimination, feudal superstitions", spread "rumours that could lead

to social disorder or damage social stability", advocate Tibetan or Taiwanese independence, or have content containing "obscenity, pornography, violence or terrorism".

Important legislation was implemented on November 6, 2000, concerning the content of news sites and Chinese discussion forums. It specifies that sites can only publish information provided by public media, that is, content which has undergone censorship within the constraints of official state propaganda. News originating from foreign media sources can no longer be published on Chinese sites unless an official authorization has been obtained. In addition, web sites are held responsible for any "subversive" information they publish. These measures also concern discussion forums. Anyone who violates this new law, especially those responsible for web sites, face administrative sanctions, fines, or prison sentences, depending on the "seriousness" of their wrongdoing. This measure means that news portals, such as Sohu.com are now wholly dependent on China's official press.

On December 28, 2000 a law was passed stating that "spreading rumours, defamation or publishing harmful information, inciting the overthrow of the country's government, the socialist system or a division of the country" is now considered "cyber-crime" and "cyber-dissidence". It provides for prison sentences for "the promotion or organization of religious cults" and "leaking State secrets". In January 2001, the official news agency Xinhua announced that anyone involved in "espionage activities" such as "stealing, uncovering, purchasing or disclosing State secrets" using the web or by other means, risks the death penalty, or from ten years to life in prison.

The Ministry of State Security

The Ministry of State Security (MSS) is responsible for external civilian intelligence- gathering and internal counter-intelligence. The MSS was formed in June 1983, combining the external intelligence, counter-intelligence, and internal security functions of the PSB and the "*Investigation Department of the Chinese Communist Party Central Committee*". The MSS has been locked in an on-going bureaucratic struggle with the Ministry of Public Security ever since. The bureaucratic competition between the PSB and the MSS is most acute in the area of information security, where the distinction between external and internal security is unavoidably opaque.

The MSS has the clear mandate to thwart foreign efforts at undermining Chinese information security, but this frequently intersects with the PSB's role, for example, in domestic network security. Similarly, the MSS feels it has a monopoly on undermining overseas subversion plans, particularly in Tibet and Xinjiang, but the PSB oversees Internet Service Providers and other facilitators of contact with the outside. As a result, the two bureaucracies remain mired in a cycle of cooperation and conflict, with new clashes sparked by every new internal incident or relevant technological advance.

The State Secrets Bureau

One of the hallmarks of single-party authoritarian system are well-developed organizational structures for the protection of information deemed to be "state secrets." The regime in Beijing is no exception, possessing a sophisticated and interlocking set of secrecy-oriented units at all levels of the party. Of these, the most important is the State Secrets Bureau.

The State Secrets Bureau (SSB) is directly responsible for the protection of state secrets by all Chinese government and party organizations. Under the PRC Law on the Protection of State Secrets state secrets are defined as "matters that affect the security and interests of the state," including broad areas of national defense, diplomatic affairs, policy decisions on state affairs, national economic and social development, political parties and "other state secrets that the State Secrets Bureau has determined should be safeguarded."

In reality, however, many seemingly trivial pieces of information in China, such as company revenue numbers, are hidden under the cloak of "state secrets," and information has been known

to be retroactively declared a state secret to further the political agenda of an individual, unit, or the state itself.

The State Secrets Bureau has sought to extend its jurisdiction over Internet content. In January 2000, the bureau extended the State Secrets Law to the Internet. The new "*State Secrecy Protection Regulations For Computer Information Systems on The Internet*" explicitly prohibits computer information systems that contain state secrets from being directly or indirectly connected to the Internet or other public information networks. Second, the regulations prohibit the storage, processing, or transmission of state secrets over the Internet. Finally, individuals and units are prohibited from releasing, discussing, or transmitting state secrets on electronic bulletin boards, chat rooms, or Usenet groups. Operators of chat rooms will be held liable for their content. If they find something that is "*obviously wrong*", they must delete it, while if they find content that is suspicious, they should report it. Web site operators must undergo computer security checks, and those that have failed to implement safeguards against security breaches will be shut down. In addition, Web sites will not be permitted to hire "cyber reporters" to write stories for them, but must get content from China's state-controlled media since site operators may not publish previously unreleased information on the Internet without permission.

Conclusion

Analysts disagree about the impact that this blizzard of new legislation will have. Some say it will have relatively little effect since many Web site operators have long known that leaking state secrets on the Internet is going to be an illegal activity. Provisional regulations to this effect have been circulating since early 1998. Webmasters are already self-censoring, taking their political news from official media sources only, or steering clear of such content altogether and focusing instead on sports and entertainment.

Many believe the new rules to be unenforceable due to the high cost and impracticality of monitoring the exploding volume of information being exchanged via the Internet and tracing them to particular individuals. It may be technically possible to filter out keywords and read email, they say, but it will considerably slow down Internet communication and therefore development, to which the economic departments are likely to make strenuous objections. At the same time, many Chinese Web site operators have said that the regulations were inevitable and that in a sense they are useful for standardizing irregular practices and bringing order to the industry. Others however, assert that the regulations concerning cyber-reporting may be a disaster for some Chinese Internet portal sites, which depend on their own news reports and those from other providers for content.

Even where there is little direct impact from the new legislation, it will indirectly repress the atmosphere of lively on-line debate that characterised the early days of the Internet in China. In addition, the new rules are likely to hinder technical innovation, while the constantly shifting interpretations and contradictory implementations may frighten off foreign direct investment, undermining China's efforts to exploit the economic potential of the Internet.

Key Internet Legislation and Regulations issued in China since 1996

"PRC Interim Regulations Governing the Management of International Computer Networks"

PRC Interim Regulations Governing the Management of International Computer Networks (*Zhonghua renmin gongheguo jisuanji xinxi wangluo guoji lianwang guanli zanxing guiding*), *pub. Fazhi Ribao (Legal Daily)*, February 12, 1996, issued by State Council Order No.195, signed by Premier Li Peng on February 1, 1996.

"Management Measures of the PRC Regulations for the Safety Protection of Computer Information Systems"

Management Measures of the PRC Regulations for the Safety Protection of Computer

Information Systems (*Jisuanji xinxi wangluo guoji lianwang anquan baohu guanli banfa.*), pub. *Jisuanji Ji Wangluo - Falu Fagui (Computers and Internet -Laws and Regulations)*, Falu Chubanshe, Beijing: 1999, p. 99.

"State Secrecy Protection Regulations For Computer Information Systems on the Internet"
Regulations Regarding Management of State Secrets in Computer Information Systems and International Internet (*Jjisuanji xinxi xitong guoji lianwang baomi guanli guiding*)
January 25, 2000 (applied retroactively from January 1, 2000) issued by the Bureau for the Protection of State Secrets.

"PRC Telecommunications Regulations"

PRC Telecommunications Regulations (*Zhonghua renmin gongheguo dianxin tiaoli*), October 11, 2000, issued by State Council Order No.291, endorsed by Premier Zhu Rongji on September 25, 2000.

"Telecommunications Regulations Of The People's Republic Of China"

PRC Telecommunications Regulations (*Zhonghua renmin gongheguo dianxin tiaoli*), October 11, 2000, issued by State Council Order No.291, signed by Premier Zhu Rongji on September 25, 2000.

"Measures for Managing Internet Information Services"

Measures for Managing Internet Information Services (*Hulianwang xinxi fuwu guanli banfa.*), *Fazhi Ribao (Legal Daily)*, issued by State Council Order No.292; signed by Premier Zhu Rongji on September 25, 2000.

"Decisions of the National People's Congress Standing Committee on Safeguarding Internet Safety"

Decisions of the National People's Congress Standing Committee on Safeguarding Internet Safety (*Quanguo renda changweihui guanyu weihu hulianwang anquan de guiding*), *Fazhi Ribao (Legal Daily)*, December 30, 2000.

"Explanations on Certain Questions Concerning the Specific Application of Law in the Trial of Cases of Stealing, Making Secret Inquiries of or Buying State Secrets and Intelligence and Illegally Providing Gathered State Secrets and Intelligence for Units Outside the Country",

in "China: Supreme People's Court on Stealing State Secrets", BBC Monitoring, January 23, 2001, from report in Xinhua, January 21, 2001.
