Chapter Two

GOVERNMENT COUNTERSTRATEGIES

BEIJING'S DILEMMA: CONTROL VERSUS MODERNIZATION

China faces a very modern paradox. The regime seems to believe that the Internet is a key engine of the New Economy, despite the burst of the Internet bubble and the dashed hopes of numerous Chinese "dotcom" companies, and that future economic growth in China will depend in large measure on the extent to which the country is integrated with the global information infrastructure. Economic growth is directly linked to social stability for the Beijing leadership, and absent communism or some other unifying ideology, maintenance of prosperity has become the linchpin of regime legitimacy and survival. Since economic growth has required modernization of China's relatively poor communications infrastructure, China has quickly become one of the world's largest consumers of information-related technologies. Moreover, Chinese leaders view the development of information technology, particularly the Internet, in China as an indispensable element of their quest for recognition as a great power. In the words of a recent *People's Daily* article, "The degree of development of information networking technology has become an important yardstick for measuring a country's modernization level and its comprehensive national strength."[1]

At the same time, however, China is still an authoritarian, single-party state with a regime whose continued rule relies on the sup-

[1] Commentator's article, "Using Legal Means to Guarantee and Promote Sound Development of Information Network," *People's Daily*, July 12, 2001, in FBIS, July 12, 2001.

pression of antiregime activities. The installation of an advanced telecommunications infrastructure to facilitate economic reform greatly complicates the state's pursuit of internal security.[2] The challenge for the regime, as Nina Hachigian puts it, is to "prevent this commercial goldmine from becoming political quicksand."[3]

Faced with these contradictory forces of openness and control, China has sought to strike a balance between the information-related needs of economic modernization and the security requirements of internal stability.

THE NATURE OF THE CHINESE INFORMATION SECURITY ENVIRONMENT

From public statements, policies, and actions, it is clear that the Chinese regime is anxious about the possible consequences of the country's information-technology modernization, in particular, the increasingly complex and challenging information security environment. The problem can be analyzed along two dimensions, one foreign and one domestic. The foreign dimension involves concerns about technology importation. Paranoia in China about "backdoored" foreign software and hardware is ubiquitous, bolstered by well-publicized cases involving user-ID tracking features of the Pentium III chip,[4] Windows 98,[5] and Windows 95,[6] as well as suspicions

[2] For a comprehensive rendition of this argument, see Andy Kennedy, "For China, the Tighter the Grip, the Weaker the Hand," *Washington Post*, January 17, 1999.

[3] Nina Hachigian, "China's Cyber-Strategy."

[4] Intel, the maker of the Pentium III chip, has admitted that each chip has a unique serial number that can be tracked as the user navigates the Internet. For a sample of Chinese analysis on the subject, see Cao Xueyi, "Here Comes the Wolf, Raise Your Hunting Rifle—Be Alert to Computer Network Security," *Jiefangjun bao*, August 25, 1999, p. 5, in FBIS, August 25, 1999.

[5] Microsoft has now verified that its Windows 98 operating system generates a unique identification number. As the user navigates the Internet, the operating system sends data to a Microsoft web site, where a database of user information is compiled. For a typical Chinese reaction, see Liu Youshui and Zhang Wusong, "High-Tech Development and State Security," *Jiefangjun bao*, January 11, 2000, p. 6, in FBIS, January 11, 2000.

[6] The Australian Navy allegedly discovered that their copies of Windows 95 were transmitting user information to Microsoft without the users' knowledge and subsequently accused Microsoft of attempting to steal naval secrets and undermine

that encryption products of U.S. origin have been deliberately weakened in a back-room export control deal with the U.S. National Security Agency.[7] Government officials, especially those in the security apparatus, seem convinced that foreign intelligence services are using or plan to use these "hidden dangers" (Chinese commentators also call them "time bombs") to the detriment of China.[8] According to one prominent Chinese information-security specialist:

> [D]uring the current phase of large-scale importation and use of foreign information equipment, we do not independently possess secure information systems, objectively speaking. For us, this is undoubtedly a great potential threat.[9]

This concern, coupled with the widespread belief that the U.S. military used back-doored hardware and software to advantage against Iraq and Serbia, has created the overall impression in Beijing that the importation of foreign equipment undermines Chinese national security and has led to calls for protectionist measures against foreign IT companies.[10]

The domestic dimension of the problem has been clearly articulated by the top leadership in China. Internal stability has been one of the state's top goals for the past few years and remains a crucial regime concern today.[11] Indeed, recent outbreaks of worker unrest sparked

Australian national security. For an understandably sympathetic Chinese spin on the incident, see Chen Ting and He Jing, "Pay Attention to Phenomenon of 'Information Colonialism,'" *Jiefangjun bao*, February 8, 2000.

[7] This assertion, a common theme in the Chinese press, is repeated in Xu Xiaofang and Dan Aidong, "Serious Challenge to Information Network Security," *Jiefangjun bao*, July 20, 1999, p. 6, in FBIS, July 20, 1999.

[8] The label "hidden dangers" is used in "Ensuring PRC Military Network Security," *Xiandai junshi*, October 11, 1999, pp. 35–36. The phrase "time bombs" is found in Xu Xiaofang and Dan Aidong, "Serious Challenge."

[9] Teng Yue, "China Should Handle Information Security Independently," *Wen wei po*, July 12, 1999, p. A7, in FBIS, July 27, 1999.

[10] Perhaps the most complete rendition of this argument, including analysis of alleged information warfare against Iraq and Serbia, can be found in Cao Xueyi, "Here Comes the Wolf."

[11] For articulations of this viewpoint over the past several years, see, for example, "Jiang Zemin Stresses Rural Stability at NPC Panel Discussions," *Xinhua*, March 5, 2002, in FBIS, March 5, 2002; "Zhu Rongji: Reform Requires Social Stability, State Security," *Xinhua*, March 5, 2000; "Jiang, Zhu Speak at Politics and Law Conference,"

by layoffs from failing state-owned enterprises (SOEs), and the expectation that such incidents are likely to become increasingly common in the wake of China's World Trade Organization (WTO) accession, have apparently intensified Beijing's concerns about social unrest and internal stability.[12] The government fears that hostile organizations, either foreign or indigenous, will use the new information technologies to agitate the population and undermine the regime. The following quote from the Public Security Bureau's official newspaper illustrates the regime's long-standing anxiety:

> As reform and the opening up [of] policy deepen, the problem of hostile elements at home and abroad using computer information systems and international networks to carry out infiltrations and sabotage will deteriorate.[13]

The cited possibilities are numerous. Chinese officials often warn that the information infrastructure could be used to disseminate information that is "harmful to social stability."[14] More alarming is the possibility that the new systems could be used to divulge state secrets or, worse still, to coordinate organized political action among antiregime forces.[15] Recent scandals involving the use of the Internet by the banned Falungong organization, the discovery of a high-ranking spy within the military,[16] the use of the Internet by antiregime dissidents, including the CDP, and a series of high-profile disclosures

Xinhua, December 23, 1998, in FBIS, December 24, 1998; and "Jiang Stresses Stability, Unity," *Xinhua*, December 18, 1998, in FBIS, December 18, 1998.

[12] For an excellent series of reports on the latest outbreaks of labor unrest, see John Pomfret, "With Carrots and Sticks, China Quiets Protesters," *Washington Post*, March 22, 2002; "China Cracks Down on Worker Protests," *Washington Post*, March 21, 2002; and "Thousands of Workers Protest in Chinese City," *Washington Post*, March 20, 2002.

[13] Sun Wen, "Use Computer to Fight Crime and Pornography," *Renmin gongan bao*, February 8, 1996, p. 3, in FBIS, February 8, 1996.

[14] Zhao Ying, "Information Security Issues," *Jingji guanli*, No.5, May 5, 1998, pp. 16–17.

[15] Willy Wo-Lap Lam, "Big Push to Maintain Stability in 1999," *South China Morning Post,* January 5, 1999.

[16] Hua Chen, "PLA Spy Major General Liu Liankun Has Extensive Interpersonal Relationships and Strong Backing and His Execution Was Enforced by the Ministry of State Security," *Ming Pao*, September 19, 1999, p. A12, in FBIS, September 19, 1999.

of "state secrets" by the domestic media[17] have only served to heighten anxiety among government policymakers.

COUNTERSTRATEGIES

Beijing has employed two broad types of counterstrategies to deal with the potential threat of Internet use for dissident and other anti-regime activity. The first, which could be dubbed "low-tech solutions for high-tech problems," draws upon the state's Leninist roots and tried-and-true organizational methods. The second, "high-tech solutions for high-tech problems," embraces the new information technologies as an additional tool of state domination. The mixture of the two has proved to be a potent *yin* and *yang*, deterring most antiregime behavior and neutering whatever remains.

Low-Tech Solutions for High-Tech Problems

The low-tech solutions employed by the Chinese authorities include the use of informers and surveillance, arrests of Internet dissidents, promulgation of regulations, and, in some cases, the physical shutdown of network resources.

Informers and Surveillance. Most dissidents known to the authorities in China are subject to varying levels of intrusive surveillance, especially during sensitive political anniversaries or visits by sympathetic foreign dignitaries.[18] In late 1998, for example, the PRC authorities reportedly placed 150 dissidents on an intensive watch list. At least half of these dissidents, described as "dangerous" in internal directives, had affiliations with the banned CDP. The tightening of surveillance was allegedly prompted by the dissidents' ability to form an effective national network, which was particularly alarming to the authorities.[19]

[17] For one version of the Chinese response to these leaks, see "Jiang Zemin Orders State and Military Security Departments Guard Against the Leaking of State Secrets Via the Internet," *Ming Pao*, September 22, 1998, p. A14, in FBIS, September 22, 1998.

[18] See U.S. Department of State, *China Country Report on Human Rights Practices, 2000*, February 21, 2001, especially pp. 15–17.

[19] Willy Wo-Lap Lam, "Beijing Orders Close Watch on 150 Dissidents," *South China Morning Post*, December 24, 1998, p. 1.

Interviews suggest that this “nationalization” of previously localized movements was greatly aided by the Internet, which allowed dissidents to easily transcend physical borders and obstacles. Yet there is little evidence to suggest that Internet monitoring is a crucial part of the overall surveillance operation.[20] Instead, the authorities most often reportedly become aware of new dissidents or new activity by veteran dissidents through informers and other traditional means. Once a dissident or Falungong member has been identified as a person of particular interest, however, the authorities have the capability to monitor his or her electronic communications, including use of the Internet (see the discussion of e-mail monitoring and filtering below).[21]

Arrests and Seizures. The evidence suggests that once dissident activity has been identified, the security apparatus is more interested in obtaining physical evidence than digital evidence. Searches and arrests are often conducted in the middle of the night to achieve maximum surprise. Western officials and human-rights monitors say that during searches of any political suspect’s home or office, the first thing Chinese security agents seize these days is the computer, hoping to find on the hard drive incriminating evidence such as incoming or outgoing e-mail messages to co-conspirators.[22] Examples of this technique are numerous:

- In October 1998, Qin Yongmin was taken in for questioning, and police confiscated his computer and three fax machines.[23]
- On October 26, 1998, police detained the three leaders of the China Development Union (Peng Ming, Gan Quan, and Chang

[20] Some dissidents reportedly travel by train or bus to hold clandestine meetings with their colleagues in other cities, in part because they fear that the authorities routinely monitor their online communications. Ironically, the attempts of these activists to conceal their activities frequently play into the hands of the domestic and foreign intelligence services. Indeed, interviews indicate that communicating in person rather than electronically frequently leaves dissidents trapped in the Public Security Bureau’s nationwide surveillance net.

[21] Interviews, PRC officials, Chinese dissidents, and Falungong practitioners, June–August 2000.

[22] Kevin Platt, “China’s ‘Cybercops’ Clamp Down,” p. 6.

[23] “Veteran Dissident Qin Yongmin Detained Again,” *Agence France Presse*, October 27, 1998.

Qing), confiscating computers and documents from their headquarters.[24]

- CDP leader Wang Youcai was detained on November 2, 1998, and formally charged on November 30, 1998. Wang was sentenced in Hangzhou Intermediate Court on December 21, 1998, to 11 years in jail for allegedly conspiring with foreign forces to overthrow the Chinese state. The specific charges against him included e-mailing 18 copies of the CDP constitution and declaration on the party's founding to dissidents and human-rights activists in the United States and Hong Kong[25] and accepting $800 to buy a computer.[26] Officers from the Hangzhou Public Security Bureau discovered the e-mail messages when they searched Wang's home and questioned him about the founding of the CDP in late June 1998.[27] The timing of these events supports the argument that PRC authorities rely primarily on traditional low-tech measures—in this case, a physical search of Wang's residence following his founding of the CDP—to uncover evidence of "subversive" Internet use. Specifically, the date the authorities claim to have uncovered Wang's e-mailing is the same as that of the raid on his apartment.
- In February 1999, Wang Ce, a prominent exiled democracy activist who clandestinely returned to China in 1998, was sentenced to four years in prison on charges of "abetting subversion" by giving CDP co-founder Wang Youcai $1,000 to purchase a computer.[28]

[24] Willy Wo-Lap Lam, "China Development Union Leaders Arrested, Told to Close," *South China Morning Post*, October 27, 1998, p. 9.

[25] "Hangzhou Court Verdict on Wang Youcai," Hong Kong Information Center, December 21, 1998, in FBIS, December 21, 1998. The court also noted that the Public Security Bureau found an e-mail message from a "hostile overseas organization" that had provided funding to Wang.

[26] Scott Savitt, "China's Internet Revolution," *Asian Wall Street Journal*, December 21, 1999, p. 10.

[27] According to the court verdict, "the public security organs testified that they found on the Internet and in 'Netscape Mail' of the defendant's Toshiba Satellite Pro 430 CDT on 26 June 1998 some 18 e-mail copies of the 'constitution' and 'declaration' sent by the defendant to overseas recipients on 25 June 1998."

[28] Authorities also charged Wang Ce with "illegally entering the country."

- In February 1999, Xu Wenli’s wife, He Xintong, demanded the return of some unlisted items among the 300 items seized from their home during three police searches. The missing items included two computers, two printers, two telex machines, a photocopier, and numerous cassettes and CDs.[29]
- On June 19, 1999, 15 police stormed into Zhu Yufu’s home and hauled him and another CDP member, Han Shen, away. The police searched his home for two hours, taking away a computer, an address book, and numerous documents.[30]
- On June 29, 1999, Gao Hongmin, deputy chairman of the Beijing-Tianjin branch of the CDP, was taken from his home by police, who also removed his computer and documents.[31]
- In August 1999, the wife of Wu Yilong (Shan Chenfeng) reportedly was detained. The authorities confiscated a computer, an address book, a fax machine, books, and other items.[32]
- In September 1999, Qi Yanchen, an employee of the Hebei branch of the China Agricultural Development Bank and a member of the China Development Union (CDU), a banned pro-reform intellectual group,[33] was arrested for his involvement in a variety of “subversive” online activities. These reportedly included posting portions of his unpublished book, “China’s Collapse,” on overseas Chinese-language BBS. The book explored themes including social instability in China and warned that the ruling CCP needed to enact political reform or risk turmoil.[34] He was also accused of publishing articles under the pseudonym “Ji

[29] “Wife Demands Return of Confiscated Items,” *Agence France Presse*, February 18, 1999.

[30] “Hangzhou Security Bureau Detains Five More Dissidents,” Hong Kong Information Center of Human Rights and Democratic Movement in China, June 19, 1999.

[31] “Two Democracy Party Members Detained,” *Agence France Presse*, June 29, 1999.

[32] U.S. Department of State, *Human Rights Report for 1999*.

[33] Peng Ming founded the CDU in early 1998. Beijing declared the organization illegal in October 1998 and subsequently sentenced Peng to 18 months of reeducation through labor on charges of soliciting a prostitute.

[34] “China Charges Dissident Author with Subversion,” Associated Press, December 22, 1999.

Li" in *VIP Reference* and of receiving copies of *VIP Reference*.[35] According to other reports, his arrest may also have been related to his involvement with *Consultations*, an environmentalist on-line magazine associated with the CDU. Qi had been under police surveillance since 1998. At the time of his arrest, his computer, fax machine, printer, books, manuscripts, and notes, as well as copies of *VIP Reference*, were allegedly confiscated.[36]

- In November 1999, Zhejiang Province CDP members Wu Yilong, Mao Qingxiang, Zhu Yufu, and Xu Guang received sentences of 11, 8, 7, and 5 years, respectively, on charges that included using e-mail to communicate with "reactionary organizations abroad" and posting CDP materials on overseas Chinese-language BBS.[37] Authorities confiscated a computer belonging to one of the four dissidents when they detained them earlier in the year.
- In March 2001, state security officers in Beijing detained Yang Zili, a software engineer and outspoken critic of the CCP who maintained a website called "Yang Zili's Garden of Ideas." They also detained his wife, Lu Kun. The agents confiscated Yang's computer, books, and other items. Lu was subsequently released, but Yang reportedly remains in detention.[38]

Finally, the authorities have a clear track record of arresting possible dissidents for Internet-related offenses. The first person imprisoned in the PRC for "subversive" use of the Internet was Lin Hai, a computer software engineer and Internet entrepreneur from Shanghai, who was charged with subversion and was sentenced to two years in prison on January 20, 1999, for providing a total of 30,000 e-mail addresses to "overseas hostile publications." Authorities charged that Lin, using the on-line pseudonym "Black Eyes," began transmitting

[35] "Chinese Internet Writer Faces Trial for Subverting State Power," e-mail press release from *VIP Reference* editor Richard Long, May 22, 2000.

[36] U.S. Department of State, *Human Rights Report for 1999*. See also "Chinese Intellectual Detained for Alleged Internet Crimes," *Inside China Today*, www.insidechina.com/news, September 6, 1999.

[37] "Four CDP Founders Given Stiff Prison Sentences," Hong Kong Information Center for Human Rights and Democracy, November 9, 1999, in FBIS, November 9, 1999.

[38] For a detailed account of the detention, see Lu Kun, "My Experience in a Beijing Detention Center," April 13, 2001, available on the Digital Freedom Network website at http://www.dfn.org/voices/china/lukun-detention.htm.

the e-mail addresses of Internet users in Chengdu, Guangzhou, Shenzhen, Zhuhai, Zhanjiang, Huizhou, Shantou, Qingdao, and Shanghai to *VIP Reference* and *Tunnel* in September 1997. In January 1998, Lin sent more e-mail addresses to the editors of *VIP Reference* in response to their specific requests for the addresses of Internet users in Nanjing and Beijing.[39]

Lin argued that he transmitted the e-mail addresses solely for commercial reasons, but the court rejected his defense on the basis of his e-mail correspondence with *Tunnel* and *VIP Reference*, which suggested that he had political motivations.[40] Lin believes that the Public Security Bureau found out he had sent the e-mail addresses to the online magazines through e-mail filtering and then traced the e-mail address he used, which was hosted by a Chinese ISP.[41] However, available evidence is not sufficient to determine conclusively whether authorities initially discovered Lin’s activities through technical monitoring or through more traditional means, such as the use of informants.[42]

Many observers said that Lin’s sentencing reflected Beijing’s growing unease about the potential of the Internet and e-mail to aid dissidents’ efforts to organize, contact “overseas hostile forces,” and disseminate uncensored information within China. The sentence was apparently intended to deter other would-be “cyber-dissidents” from

[39] “Court Verdict on Dissident Lin Hai,” Hong Kong Information Center, January 20, 1999. Police originally detained Lin in March 1998. The charges brought against him also included forwarding copies of *Da Cankao* to a former classmate in Beijing and telling him how to subscribe to the magazine via e-mail.

[40] According to the authorities, in one message, Lin wrote, “Your electronic periodical is indeed a high-class magazine carrying an independent voice. Although I hate the tweeters of the CPC, I am alone and there is nothing I can do.”

[41] Interviews, March 2002.

[42] Evidence presented by the prosecution at Lin’s trial included two PCs, one laptop, and one modem; e-mail correspondence between Lin and editors of *Tunnel* and *VIP Reference*; e-mail correspondence between Lin and a former schoolmate; “relevant reports” from “data communication bureaus” in Guangzhou, Shenzhen, Zhuhai, Shantou, Zhanjiang, and Huizhou, the Shanghai Telecommunications Bureau, the Beijing Zhongxi Electronic Engineering Technology Developing Company, the Sichuan Public Information Industry Company, Limited, and the Shandong Qingdao Information Industry Company, Limited; an “Internet User Application Card” from the Shanghai Telecommunications Bureau; other unspecified written evidence; and “witnesses’ statements.”

using the Internet for subversive purposes. For unknown reasons, Lin was released early, in September 1999.[43] Despite his ordeal, Lin subsequently told the Associated Press that he was looking for new Internet-related business opportunities because "this business is very hot at the moment," but he allowed that "whether or not I can continue in this line of work depends on the political environment."[44] In 2000, Lin apparently reopened his web site, which advertised a list of more than 1,000,000 mainland e-mail addresses as well as a variety of information-technology services.[45] He ultimately left China and is now living in the United States.

In June 2000, police in Chengdu, Sichuan, arrested and charged with subversion the operator of a mainland web site that posted news about dissidents and the 1989 Tiananmen massacre. Huang Qi, who operated the www.6-4tianwang.com site, was seized by police on June 3, 2000, and held at a detention center in Chengdu. His wife, Zeng Li, who was taken away the same day, was released. Minutes before he was arrested, Huang posted messages on the chat room of his web site, saying that four policemen had come to take him away.[46] The web site was originally launched in June 1999 as the first in China dedicated to helping people find relatives abducted by traffickers. It was shut down in March 2000 over reports concerning the human rights of Chinese laborers working overseas. It was reopened in April 2000 with the help of a U.S.-based Chinese group.[47]

Many more Chinese dissidents, Falungong practitioners, and others have been charged with crimes related to political use of the Internet. Over the past two years, at least 25 people have been detained in

[43] See "PRC's Cyber-Dissident Released from Jail Early," Hong Kong *Agence France Presse*, March 3, 2000; and "China Grants Early Release to Cyberdissident," Associated Press, March 3, 2000. Lin's early release was not widely reported in Western media until March 2000. He was apparently reluctant to discuss with reporters the circumstances surrounding his early release, telling *Agence France Presse* only that "the real reason, nobody knows."

[44] "China Grants Early Release to Cyberdissident," Associated Press, March 3, 2000.

[45] The site, home4u.china.com/technology/internet/hopy/, is no longer accessible.

[46] Josephine Ma, "Police Charge Web Site's Founder with Subversion," *South China Morning Post*, June 8, 2000.

[47] Josephine Ma, "Defiant Cyber-Surfers Play Cat-and-Mouse Game," *South China Morning Post*, June 8, 2000.

China for their use of the Internet, according to the Digital Freedom Network.[48] Representative cases include the following:

- Six Falungong practitioners, four of whom were graduate students in engineering and sciences at Beijing's elite Qinghua University, were sentenced in December 2001 to prison terms of from three to 12 years for disseminating Falungong materials on the Internet.[49]
- That same month, Wang Jinbo, a member of the CDP in Shandong Province, was convicted of subversion and sentenced to four years in prison for e-mailing articles calling for the reversal of the official verdict on the 1989 Tiananmen democracy movement to overseas dissident groups.
- In September 2001, a Hunan Internet user was sentenced to three years in jail for e-mailing articles critical of the government to friends.
- A Chinese reporter affiliated with the CDP was sentenced in August 2001 to reeducation through labor for trying to recruit new members for the banned opposition party in Shanghai and posting pro-democracy articles on web sites.
- Li Hongmin of Hunan was detained in June 2001 for e-mailing excerpts from the Chinese version of the *Tiananmen Papers,* which was swiftly banned in China, to several friends.

[48] Digital Freedom Network, "Attacks on the Internet in China: Chinese Individuals Currently Detained for Online Political or Religious Activity," available on the DFN website at http://www.dfn.org/focus/china/netattack.htm. See also Digital Freedom Network, "Attacks on the Internet in China: Internet-Related Legal Actions and Site Shutdowns Since January 2000," available at http://www.dfn.org/focus/china/shutdown.htm.

[49] "Six Falungong Academics Jailed," *South China Morning Post,* December 24, 2001. The Falungong members had also distributed printed materials on the streets in Beijing, and it is not clear how the authorities initially discovered their activities. If this case followed the usual pattern, the police may have arrested the Falungong members after receiving a tip from an informant or learning that they were distributing the leaflets. The authorities probably confirmed that they were using the Internet to transmit similar materials only after arresting them and confiscating their computers. The possibility that the police observed and traced their online activities, however, cannot be discounted on the basis of the evidence available. In all of the incidents listed here, as in this case, it is not known how the authorities discovered the Internet activities of the individuals who were jailed or detained.

- In October 1999, Zhang Ji, 20, a student at Qiqihar University in Heilongjiang, was arrested and charged with "disseminating reactionary documents via the Internet." Zhang had reportedly transmitted news of the crackdown to Falungong members in the United States and Canada.[50]

It should also be noted that the authorities appear willing to charge dissidents with "subversive" uses of the Internet that are inherently nonpolitical in nature, primarily as a tactic to silence them or smear their character. In January 2000, Public Security Bureau officers arrested Wang Yiliang, a dissident writer from Shanghai, for his participation in an unauthorized literary association. The authorities searched his home and found pictures of nude women downloaded from the Internet on his computer, which they subsequently used to sentence him to two years of reeducation through labor for "possessing pornographic articles."[51]

Promulgation of Regulations. One of the most effective lines of defense in China's Internet security strategy is the use of bureaucratic regulations to shape the market environment and the incentives of key participants in ways favorable to the state's interest. Since 1995, the Chinese government has promulgated a blizzard of rules covering nearly every aspect of the Internet market. In particular, the 1997 Public Security Bureau regulation entitled "Computer Information Network and Internet Security, Protection and Management Regulations" places most of the onus for monitoring, reporting, and preventing antiregime use of the Internet on domestic providers. At the level of international gateways, units that oversee international connections of networks "must assume responsibility for the Internet network gateways as well as the security, protection, and management of the subordinate networks" (Article 10), including technical security measures, education and training, and user registration. Below the gateway level, networks should, within 30 days of the opening of a network connection, carry out the proper registration procedures with a unit designated by the Public Security Bureau of the province, autonomous region, or municipality directly under the

[50] "China Charges Student on Falungong E-mail," Reuters, November 8, 1999.

[51] "Guizhou Poet Ma Zhe Has Been Sentenced to Five Years' Imprisonment on Subversion Charge," Hong Kong Information Center, March 14, 2000.

Central Government people's government. They are also required to give information to their local Public Security Bureau on the units and individuals that have connections to the network, as well as to keep the Public Security Bureau informed of any changes in the information about units or individuals using the network. Interviews in Beijing also confirm that the Public Security Bureau frequently requests information on customer databases from ISPs.[52] If a violation occurs, the ISP is required to assist the Public Security Bureau in investigating the incident and criminal activities involving computer information networks. Like network security, responsibility for maintaining database security resides with the ISPs, and violations by users result in cancellation of the ISP's business license and its network registration (Articles 20–23). As a result, ISPs have implemented certain self-censoring policies to avoid the wrath of the authorities. According to a January 24, 2000, Reuters story, ISPs pay employees known as "Big Mamas" to lead "armies" of volunteers who patrol chat rooms and bulletin boards, ferreting out risky political commentary, foul language, and unwanted advertisements.

The 1997 regulations also circumscribe the acceptable uses of the Internet by the users themselves. Users are required to register with the Public Security Bureau, filling out an application form that links their personal information with their network account information (it is important to note, though, that this rule is almost universally ignored). Once online, users are not permitted to use the Internet to create, replicate, retrieve, or transmit information with the following goals:

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, or spreading rumors destroying the order of society.

[52] Interviews, Chinese and Western executives, January 2000.

6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, or murder.
7. Inciting 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. Engaging in other activities against the Constitution, laws, or administrative regulations.

Moreover, the rules also bar anyone from using computer networks to "harm national security, disclose state secrets, harm the interests of the State, of society or of a group, the legal rights of citizens, or to take part in criminal activities" (Article 4).

A more recent regulation (State Council Order #273, "Regulations on the Management of Commercial-Use Encryption") attempts to supplement the existing Internet rules by strictly regulating the importation of encryption products, which the authorities fear might be used by dissidents, foreign spies, and other insurgent elements to hide their Internet-based activities from the prying eyes of the authorities. The authorities ultimately backed down from this regulation. Ironically, the fears of the security apparatus about encrypted e-mail currently appear unfounded, although this situation could change as e-commerce and other encryption-heavy applications become more widespread. Interviews suggest that few, if any, people in China—either citizens or foreigners—are using encryption to conceal the content of their communications, and this is especially true for dissidents.[53] In the words of one interviewee, "Why would I use encryption? Why would I want to call attention to myself?" Indeed, the reluctance to use encryption appears to dovetail with the widespread perception that the government is monitoring e-mail and other electronic communications for keywords, despite the seemingly insurmountable technical challenges of searching so much traffic without bringing the network to a grinding halt.

[53] Interviews, Chinese and Western sources, January 2000. Similarly, none of our contacts ever mentioned dissident use of steganography, a technique that can be used to conceal information by hiding text messages in images and audio or video files.

The Ministry of Public Security also allegedly sought to restrict the use of the Internet by dissidents prior to June 4, 2000. In June, the Ministry allegedly issued Document #33, calling on the Computer Management and Supervision Departments of the Public Security Bureaus in various localities to strictly manage Internet users and restrict them from browsing “reactionary” information. After receiving this circular, Public Security Bureaus in some provinces and cities held emergency meetings to coordinate control measures. They called on ISPs to place more overseas web sites on the list of blocked sites and demanded that web cafes be placed under strict control. For example, the Ministry of Public Security authorities in Baoding City, Hebei Province, issued new regulations for 100 Internet cafes in the city. The regulations announced a “point system,” whereby a cafe “allowing a customer to browse ‘reactionary’ information will be deducted 10 points.” If a cafe loses 30 points within a single year, its license will be suspended for one year.[54]

The authorities have continued to issue rules and regulations in response to perceived Internet-enabled challenges to the regime. In November 2000, the Ministry of Information Industry issued regulations governing the management of Internet bulletin board sites and chat rooms. The regulations mandated that operators of any of these types of “electronic public notice services” must register with the authorities, obtain a permit, enact measures to control content, and maintain records of all postings for 60 days. In addition, the regulations forbid Internet users from posting on such sites any information that endangers state security, harms national reunification, runs counter to the provisions of the PRC Constitution, exposes state secrets, undermines national unity, spreads heretical beliefs, disrupts social order, or is otherwise banned. Moreover, the regulations stipulate that ISPs must delete postings that fall into any of these forbidden categories and must report them to the authorities.[55]

[54] “Eight Reactionary Activists from Jilin Who Were Imprisoned Before Call for Reversing the Verdict on the June 4th Incident and for Government Compensation,” Hong Kong Information Center for Human Rights and Democracy, June 3, 2000, in FBIS, June 3, 2000.

[55] “China Enforces Control of Electronic Public Notice Service over the Internet,” *Xinhua*, November 6, 2000.

Several bulletin board sites have been closed for violating the regulations. In September 2001, for example, authorities temporarily shut down a popular BBS hosted by the Huazhong University of Science and Technology in Wuhan, after students posted articles about the 1989 Tiananmen Square crackdown. "Everybody knows universities aren't quiet places, but it's still too sensitive for students to talk about this on the Web," a local official told Western journalists. "Articles on the June 4 incident are a serious breach of state regulations on Internet information," he said.[56] In addition to issuing rules concerning BBS, Beijing also promulgated regulations in November 2000 that require popular sites like Sohu.com and Sina.com to carry only news content that has been approved by state-run media organs.

The most recent regulations on the use of the Internet were promulgated by the Ministry of Information Industry in January 2002. These regulations require ISPs to maintain detailed records about their users, install software to record e-mail messages sent and received by their users, and send copies of any e-mails that violate PRC law to the appropriate Chinese government departments.[57] Like many of the previously issued regulations, the January 2002 regulations place the burden of policing Internet use squarely on the shoulders of Internet industry companies.

In March 2002, the official *People's Daily* reported that more than 100 Chinese Internet industry executives signed a voluntary "self-discipline" pact aimed at promoting "the healthy and orderly development" of the Internet in China through "protection of intellectual property, network security and the elimination of deleterious information from the Internet."[58] The agreement pledges the com-

[56] "Student Net Site Closed over Talk of Tiananmen," Reuters, September 6, 2001. The *Baiyun huanghe* bulletin board site (bbs.whnet.edu.cn) was reopened after the university's Communist Party Committee expunged the messages about the Tiananmen crackdown, replaced student webmasters, and required all users posting messages to register under their real names. The authors last accessed the site in January 2002.

[57] For more on the latest regulations, see "China Sets New Net Rules," *South China Morning Post*, January 21, 2002.

[58] For the English version, see "China's Internet Industry Wants Self-Discipline," *People's Daily Online*, March 26, 2002, available at http://english.peopledaily.com.cn/200203/26/print20020326_92885.html; for the Chinese version, see Chen Jian, "*Zhongguo hulianwang xingye zilu gongyue zhengshi qianshu*" [Chinese Internet

panies of China's Internet industry to abide by all laws, regulations, and policies governing the development and management of the Internet, including those concerning online news. The signatories also promise to prevent the online publication or transmission of information that is "harmful to state security or social stability, violates laws and regulations," or is deemed "superstitious or obscene." In addition, they pledge to scrutinize the information users publish online and quickly remove any "harmful information" posted on their web sites that could have a "negative influence" on Chinese Internet users. The agreement also stipulates that portals will not link to web sites that contain "harmful information."[59]

When regulations and the threat of arrest are not enough, Beijing has shown that, at least under what it perceives to be pressing circumstances, it is willing to resort to more disruptive measures.

Physical Shutdown of Network Resources. In serious crises, the Chinese government has consistently been willing to shut down networks temporarily in order to gain control. The first harbinger of this trend occurred during the anti-Japanese demonstrations of 1996 that were sparked by perceived violations of the territorial sovereignty of the contested Diaoyutai/Senkaku Islands. When Chinese students used e-mail to organize anti-Japanese demonstrations, Chinese officials responded by shutting down computer bulletin boards on some campuses.[60] More recently, after the April 1999 Falungong gathering in Beijing, the government reportedly ordered one ISP to suspend e-mail service for two days. In the run-up to June 4,' 2000, the Ministry of Public Security reportedly sought to slow down or shut down China's free and anonymous e-mail sites, 163.net and 263.net. The

Industry Self-Discipline Pact Formally Signed], *Renminwang*, March 26, 2002, available at http://www.people.com.cn/GB/it/49/149/20020326/695393.html.

[59] For the full text of the agreement in Chinese, see "*Zhongguo hulianwang xingye zilu gongyue*" [Chinese Internet Industry Self-Discipline Pact], *Renminwang*, March 27, 2002, available at http://www.people.com.cn/GB/it/49/149/20020327/695927.html. The pact also includes provisions on competition in the Internet industry and Internet user privacy issues, among other matters. Interestingly, it also contains a provision that says the signatories will propose recommendations for legislation and policy initiatives related to the development and management of the Chinese Internet industry.

[60] Steve Mufson, "Chinese Protest Finds a Path on the Internet," *Washington Post*, September 17, 1996, p. A9.

owners of 163.net, Liang Liwei and Leng Wanbao, said that they could neither send nor receive e-mail beginning on June 1. The government's reasoning for the repeated use of this tactic is neatly summarized by Pan Weimin, an electrical engineering graduate from Fudan and the head of operations for PaCity Computer Company: "When push comes to shove, the authorities don't have to restrict themselves to imposing a NetWall around China. They can use tried and true traditional methods: one administrative order from on high and everything can be shut down. It's simple and effective."

High-Tech Solutions for High-Tech Problems

In addition to traditional methods of control, the Chinese authorities have also made use of high-tech countermeasures, such as blocking websites and e-mail, government-sponsored hacking, monitoring and filtering of e-mail, and online propaganda, denial, deception, and disinformation.

Blocking Web Sites and E-mail. One of the most common, and perhaps most quixotic, methods employed by Beijing to stem the flow of antiregime information into China consists of the blocking of web sites and e-mail. Authorities at various times have blocked politically "sensitive" web sites, including those of dissident groups and major foreign news organizations, such as the Voice of America, the *Washington Post,* the *New York Times,* and the BBC.[61] In early 1999, Hong Kong–based activist Lau San Ching helped establish a web site commemorating the victims of Tiananmen (www.june4.org), and Beijing quickly blocked access to the site.[62] In April of the same year, stunned party bosses responded to the gathering of thousands of Falungong members in central Beijing by ordering the arrest and

[61] The *New York Times* web site was unblocked in 2001 after its reporters raised the issue with Jiang Zemin during an interview. The site remained accessible from China as of the completion of this study in January 2002. In addition, we note that the blocking is rather inconsistent—materials blocked on one web site often remain accessible on other sites. For example, the *Foreign Affairs* web site was blocked in early 2001, presumably to prevent Chinese Internet users from reading an article on the *Tiananmen Papers* that appeared there. But at the same time, the offending article was still readily accessible via a link from the Council on Foreign Relations web site, which was not blocked.

[62] Liu, "The Great Firewall of China."

prosecution of Falungong leaders and members and the blocking of access to the group’s international constellation of web sites.[63] The authorities even dispatched censors to screen all Chinese web forums and bulletin boards and erase any favorable remarks about Falungong founder Li Hongzhi, whom they denounced as a charlatan and a doomsayer.[64]

Most of the government’s attempts to prevent the viewing of banned web sites use multiple layers of filtering, ranging from the ISP to the network carrier to the nontechnical aspects of web surfing in China (e.g., registration with the police, observation by Internet cafe workers). The technical blocks themselves are carried out at the ISP or international-gateway level and involve the alteration of network routing tables. According to interviews, the four major ISPs regularly exchange information about which sites they are blocking. At the network-carrier level, CERNET apparently uses only CISCO routers with ACR (access-control routers), and site restrictions are set by the Ministry of Education. Most national-level blocks are placed by China’s International Connection Bureau (ICB), a set of computers belonging to state-owned China Telecom. Software at that level is programmed to reject requests for access to banned sites. China blocks sites only if a large enough number of users access them. Blocking can be done only intermittently because the software does not have enough computing power to block every objectionable site all the time. By blocking a site intermittently, the government hopes users will simply assume that the site isn’t accessible.[65] In addition, blocks on web sites are often temporarily removed when high-level foreign delegations visit China. During the October 2001 Asia-Pacific Economic Cooperation (APEC) meeting in Shanghai, for instance, Beijing permitted access to several web sites that are normally blocked, including those of the *Washington Post* and CNN. This was presumably intended to avoid embarrassing international media reports and to burnish China’s image in order to make a good impression on visiting world leaders. As soon as President Bush and

[63] Ibid.

[64] Ibid.

[65] Julie Schmit and Paul Wiseman, “Surfing the Dragon: Web Surfers Find Cracks in Wall of Official China,” *USA Today*, March 15, 2000, p. 01B.

other world leaders left Shanghai, however, the web sites were once again blocked.[66]

While access to sites of groups such as Human Rights Watch/Asia and Human Rights in China are routinely blocked, Beijing has also shown a willingness to block prominent nondissident sites for hosting "anti-China" material. After *Tiananmen,* a magazine published by exiled Tiananmen student leader Wang Dan, was posted on a Stanford University server, Beijing responded by blocking all Stanford-hosted sites.[67] The California Institute of Technology was allegedly pressured by Beijing to remove a Falungong site from its servers. When the request was rejected, access within China to the university's entire web site was blocked for several months.[68]

One site that has been repeatedly blocked by the Beijing authorities is that of *China News Digest* (CND), a volunteer group of overseas Chinese clearly unsympathetic to the regime. An account of how the CND site was blocked is offered by its founder, Wei Lin:

> Our site was among the first batch of 100 or so web sites being blocked. Some time after that, there were reports about some sites actually being removed from the Chinese government's blacklist. Earlier this year [1998], readers in China were able to access our site because we changed our ISP and consequently the IP address for our web server changed. This lasted until 5 June 1998, then the China traffic suddenly dropped. We had linked to the June 4th Beijing Massacre photo archive from our top page, which had increased our hits from 2000/day to 4000/day. Our ISP was nice enough to let us change the web server IP once again. But our server log showed that every time we changed the IP address, the traffic from China would last for a day or two during the month of June before the new IP is blocked again. We can pretty much assume that they are using the latest software on the routers when available and applicable. They do not have any technology lag other than possibly the export restriction from the U.S. government regarding encryp-

[66] This is done even for some relatively routine visits by less-senior foreign officials, reporters, and other guests.

[67] Scott Savitt, "China's Internet Revolution," *Asian Wall Street Journal*, December 21, 1999, p. 10.

[68] "Top U.S. Institute Won't Bow to Dictatorship," Central News Agency, February 20, 2000.

> tion. They have implemented classless interdomain routing (CIDR). Commercial ISPs connect to the state-owned backbones, ChinaNet and ChinaGBN, [and] many of them implement private networks and users access the Internet via proxies. The method used to block sites outside of China is, because the government allows only a few backbone networks to exist and to have their own international links, to put the access-control list on all border routers (which appear to be CISCO routers). This is very efficient because it blocks based on [the] packet source’s IPs and normally those sites cannot change their IPs easily. Based on our experience in early June 1998, CERNET and CASNET blocked us first, ChinaNet a day later, GBN some time later.

Wei closed by noting that since ChinaNet and ChinaGBN are both part of the merged information superministry, the sequenced delays in adding the blocking would suggest that, administratively, their networks are not fully merged.

Despite these types of efforts to block sensitive sites, however, CND is at the forefront of the promotion of one of the most potent weapons used in fighting web-site blocking: proxy servers.[69] The CND web site contains a guide to using proxy servers to circumvent firewalls or Internet censorship, as well as a call for volunteers to provide CND with additional proxy services.[70] A CND web page (http://proxy.cnd.org/) contains detailed instruction on the use of proxies, including various techniques for configuring web browsers. For its users, CND currently provides four official proxies, each of which uses a dynamic IP address:

1. http://cnd-d.cnd.org:8000/http://www.cnd.org
2. http://proxy2.cnd.org:8000
3. http://proxy3.cnd.org:8000
4. http://anon.free.anonymizer.com/http://www.cnd.org

[69] A proxy server sits between a client application, such as a web browser, and a real server. Proxy servers are also used to improve performance or filter requests. For more information, see www.webopedia.com.

[70] See www.cnd.org. CND seeks volunteers who have system privileges on UNIX servers or on PCs running Linux, and it notes that individuals who work at universities and have cable modems or DSL service are particularly desirable volunteers.

The fourth proxy exploits one of the most popular "anonymizer" web services, allowing users to surf the web in relative privacy. The CND site also points users to other proxy lists, available in abundance by searching portals such as Yahoo! or Webcrawler for the term *proxies*.

New York–based Human Rights in China (HRIC) has also published an article describing the use of proxy servers to access blocked web sites in its quarterly *China Rights Forum*.[71] Available evidence is fragmentary but suggests that many mainland Internet users are capable of accessing a variety of blocked sites. Xiao Qiang, executive director of HRIC, says that many sites that are blocked by PRC authorities, including those of HRIC and CND, still receive numerous visits and e-mail messages from web surfers on the mainland.[72] Statistics provided by CND on its web site confirm that some mainland users can access the site even though it is blocked.[73] CND also advises readers who have difficulty accessing their site from within China that they can receive CND publications via e-mail, using accounts at www.usa.net, www.hotmail.com, www.yahoo.com, and other free web-based e-mail services.[74] In addition, Zhang Weiguo recommends that PRC readers use proxy servers to access his *New Century Net* site, which the Chinese authorities began blocking about a year after its establishment. According to Zhang, as of 2000, new proxy addresses could generally be used for about two months before they were discovered and blocked, but this is reportedly no longer the case, as the Chinese authorities have redoubled their efforts to block access to popular proxy servers (this is discussed in further detail below).

As a result of these efforts and the gaps in the implementation of blocking on the Chinese end of the system, most sensitive sites are

[71] "Proxy Servers," *China Rights Forum*, Human Rights in China, fall 1998.

[72] Erik Eckholm, "China Cracks Down on Dissent in Cyberspace," *New York Times*, December 31, 1997.

[73] According to CND's access statistics for Friday, June 9, 2000, for example, at least six mainland Chinese users (defined as visitors with .cn domain names) accessed the main CND page, and at least 16 reached one of CND's two mirror sites, presumably by using proxy servers. A mirror site is a replica of an already existing site, used to reduce network traffic (hits on a server) or improve the availability of the original site. For more information on mirror sites, see www.webopedia.com.

[74] "Some Special Notes for Network Users in CN Domain (Mainland China) or Accessing to the Internet from Behind Firewall (Need a Proxy?)," CND web site.

available to the Chinese population, or at least to those Internet users who are willing to devote some time and effort to accessing them. Among these, a number of avowedly pro-democracy web sites, human-rights web sites, and Tibet-related web sites, including that of the Tibet government-in-exile, continue to be accessible even without the use of proxy servers.[75] The authors’ own limited empirical studies in Internet cafes in major Chinese cities, usually involving 100 to 200 political and media sites, reveal little consistent blocking of even the most sensitive sites. More surprising, the vast majority of terminals in these cafes, including those populated exclusively by locals, were preconfigured with the necessary proxy servers in Australia or elsewhere to circumvent the “Great Firewall.”

Beginning in early 2001, however, the Chinese authorities stepped up their efforts to block access to well-known proxy servers and privacy protection sites. Companies offering privacy protection services (e.g., Safeweb, SilentSurf, and Anonymizer) are now engaged in a daily game of measure and countermeasure with the authorities in China and other countries that try to restrict access to particular web sites.[76] For example, the Safeweb site was blocked by Chinese authorities beginning in late February 2001.[77] At around the same time, SafeWeb received funding from the International Broadcasting Bureau, which oversees the Voice of America, to enhance the services it offers to Chinese users who want to access blocked web sites.[78] The result was a peer-to-peer application, Triangle Boy, released in April 2001, aimed at enabling Chinese Internet users to access all websites blocked by the authorities.

[75] U.S. Department of State, *Human Rights Report for 1999*.

[76] See for example, Jennifer 8. Lee, “Punching Holes in Internet Walls,” *New York Times*, April 26, 2001.

[77] Recent research suggests that this version of Safeweb, which was taken out of service in November 2001, may not have provided the degree of anonymity it promised its users. Researchers from Boston University and the Privacy Foundation assert that Safeweb’s security vulnerabilities would “allow adversaries to turn Safeweb into a weapon against its users, inflicting more damage on them than would have been possible if they had never relied on Safeweb technology.” See David Martin and Andrew Schulman, “Deanonymizing Users of the Safeweb Anonymizing Service,” February 11, 2002, p. 1. The full report is available online at http://www.cs.bu.edu/techreports/pdf/2002-003- deanonymizing-safeweb.pdf.

[78] Jennifer 8. Lee, “U.S. May Help Chinese Evade Net Censorship,” *New York Times*, August 30, 2001.

Despite claims that Safeweb's Triangle Boy system would allow Chinese Internet users unfettered access to blocked sites,[79] however, the Chinese authorities reportedly have had a relatively easy time blocking the system. Computer-savvy Internet users have reported that they are unable to access Safeweb's Triangle Boy servers, and the authors were also unable to use the system on two recent trips to the PRC. One major problem with the current system is that of communicating the IP addresses of Triangle Boy servers to people in China without the authorities also finding out and quickly blocking access to the sites. Currently, Safeweb sends out an e-mail containing the information in response to user requests. Personnel from the Ministry of Public Security's Computer Monitoring and Supervision Bureau simply request the information through e-mail as often as necessary and block the IP address on the routing table.[80] After only a few months, Beijing's blocking of the addresses caused an 80 percent decline in the use of Triangle Boy by Chinese web surfers, according to a Western media report.[81] "Now it is basically impossible to use it," laments an article posted on a Chinese-language web site dedicated to promoting freedom of speech on the Chinese Internet.[82] This article and other postings on Chinese-language web sites indicate that since the Chinese authorities intensified their efforts to block access to Safeweb's Triangle Boy network, some mainland Internet users have turned to another peer-to-peer application, the Chinese version of Freenet, which can be used not only to search for and exchange documents, but also to access blocked web sites. Nevertheless, it appears that, for the moment at least, Beijing has the up-

[79] See Safeweb's "White Paper: Triangle Boy Network," available on the Safeweb web site, www.safeweb.com. The paper asserts: "Triangle Boy is our answer to Internet censorship. Triangle Boy defeats all attempts to prevent users from accessing sites on the Internet." Safeweb expects that it will become more and more difficult for the Chinese security services to block access to its network over time as the number of Triangle Boy machines increases. The use of dynamic IP addresses by some Triangle Boy machines, according to Safeweb, "makes the censors' task even more daunting and the likelihood of success even slimmer." For now, it appears that Beijing has the upper hand in its battle with Safeweb, but as these points illustrate, this could change in time.

[80] Interviews, Western computer technicians, January 2002.

[81] Pamela Yatsko, "China's Web Censors Win One—For Now," *Fortune*, December 24, 2001.

[82] *"Guanyu Ziyouwang"* [About Freenet], December 11, 2001, available at www.internetfreedom.org/gb/articles/1042.html.

per hand in the web-site blocking battle. In the words of one activist who recently visited the mainland, "The authorities have become much better at finding and blocking proxies in China; I was there for eight days and experienced eight days of Internet blackout."[83]

In sharp contrast to web sites, e-mail and e-mail publications are difficult to block, although the PRC government attempts to do so at times by blocking all e-mail from overseas ISPs used by dissident groups. The Voice of America Chinese-language e-mail news server was blocked beginning in April 1999, except for a brief period in July of that year. Beijing has responded to the spamming of *Xiao Cankao* by blocking all e-mails from the ISP from which the messages originate.[84] As noted earlier, at the height of the summer 1999 crackdown on Falungong, the government ordered an ISP suspected of being a conduit for the group's international coordination activities to suspend e-mail service for two days. In the run-up to June 4, 2000, the Ministry of Public Security reportedly sought to slow down or shut down China's free and anonymous e-mail sites, 163.net and 263.net. As noted earlier, the owners of 163.net, Liang Liwei and Leng Wanbao, said that they could neither send nor receive e-mail beginning on June 1.

Despite these government efforts, opponents of the regime have enjoyed significant success in overcoming e-mail blocking. Indeed, as argued earlier in this report, the spamming campaigns of *Xiao Cankao* and *Da Cankao,* originating from a different e-mail address every time, are among the most successful dissident Internet strategies. Even the CND listserv e-mails, which originate from the same site, have enjoyed relatively easy access, due in part to the advice offered by CND on how to overcome e-mail blocking. In particular, its staff recommends that mainland users obtain free Web-based e-mail accounts, such as www.usa.net, www.hotmail.com, www.mailcity.com, www.yahoo.com, or www.rocketmail.com. After sending mail/subscribe messages to CND from these sites, users are free to check

[83] Interview, Chinese activist, March 2002. As peer-to-peer applications become more widely used in China, however, the advantage now enjoyed by the authorities may shift back to those Internet users who are interested in viewing banned web sites.

[84] Frank Langfitt, "Taking Dissent Online in China; E-mail: In the Age of the Internet, Chinese Leaders Are Finding It Harder to Contain Free Speech," *The Baltimore Sun*, May 11, 1999, p. 2A.

their e-mail on the web, with no fear of receiving e-mails that must traverse Chinese government-controlled routers.

Hacking. There is some evidence to suggest that the Chinese government or elements within it have engaged in hacking of dissident and antiregime computer systems outside of China. Given the inherently indeterminate nature of the source of most computer network intrusions, it is often difficult if not impossible to establish official culpability for hacking attacks without additional evidence. Governments, usually by design, can therefore claim a reasonable measure of plausible deniability in these cases. The Chinese-origin hacking attacks that occurred against Taiwan in August 1999 and against Japan in February 2000 are examples of incidents in which government culpability, either limited or complete, is difficult to determine solely on the basis of the intrusion data.

Stronger evidence exists to support the conclusion that the Chinese government or elements within it were responsible for one or more of the China-origin network attacks against computer systems maintained by practitioners of Falungong in the United States, Australia, Canada, and the United Kingdom. After the exposure of the role of certain Chinese security agencies in the attacks, the later, more sophisticated intrusions were believed to have been carried out by cut-outs, making it more difficult to ascertain the extent of government involvement. This was especially true of the attacks that occurred in winter and spring 2000.

Summer 1999. In mid-July 1999, the Chinese government authorities began a nationwide crackdown on the Falungong organization, claiming that it was a “dangerous cult.” News of the crackdown spread quickly, due in large measure to the organization’s extensive use of advanced information technologies and its network of Internet sites around the globe. These sites provided real-time accounts of crackdowns in some Chinese cities, based on e-mails and other communications from Falungong members. As the story was gradually picked up by the global media, these sites, many of which were shoestring operations run by group members, understandably began to strain under the increased hits they received. While this slowdown in service was an expected consequence of worldwide attention, some of the sites began to suffer from anomalous crashes. When the system administrators of these servers examined the situation in detail, some realized that their networks were suffering from a sophisticated series of computer network attacks. The July 1999 attacks against Falungong sites in four countries (one in Britain, two in Canada, one in Australia, and two in the United States) bear greater scrutiny.

The evidence of a Chinese government-directed information operation against Falungong is strongest in the U.S. case. On July 14, 1999, Falungong practitioner Bob McWee of Middletown, MD, established www.falunusa.net, with the express purpose of mirroring the files of existing Falungong sites in Canada (www.falundafa.ca and www.minghui.ca) and the United States (www.falundada.org).[85] On July 20, 1999, the two Canadian sites began to suffer a degradation of network performance, because of Chinese-origin hacking attacks. As a result, they began re-routing connection requests to their mirror site, FalunUSA. Between July 21 and 23, the U.S. site began to have similar difficulties. Specifically, it was suffering from a type of attack known generally as a denial-of-service attack, in which the target machine is flooded with incomplete requests for data and eventually succumbs to the attack by crashing. Backtracking a similar attack on July 27, 1999, revealed the source IP address of the attack to be 202.106.133.101, an Internet address in China. Examination of the Asia-Pacific Network Information Center (APNIC)[86] database entry for this address revealed the ownership information shown in Figure 1.

The name of the organization, “Information Service Center of XinAn Beijing,” sounded innocuous enough, but the street address told a very different story. The address, #14 East Chang’an Street (listed in Figure 1 in transliteration as “Dong Chang An Jie 14”) in Beijing, is that of the Ministry of Public Security, China’s internal security service—the organization most embarrassed by the unexpected appearance of thousands of Falungong practitioners outside the

[85] Svensson, “China Sect.”

[86] APNIC is the Internet registry organization for the Asia-Pacific region. For more information on APNIC, see http://www.apnic.org.

```
Inetnum:    202.106.133.0 - 202.106.133.255
Netname:    ISCXA
Descr:      Information Service Center of XinAn Beijing
Country:    CN
Admin-c:    WH42-AP
Tech-c:     HJ36-AP
Changed:    suny@publicf.nta.net.cn  19990716
Source:     APNIC

Person:     Wang Huilin
Address:    Dong Chang An Jie 14 Beijing 100741
Phone:      +86-10-65203827
Fax-no:     +86-10-65203582
Nic-hdl:    WH42-AP
Changed:    suny@publicf.bta.net.cn  19990716
Source:     APNIC


Person:     He Jian
Address:    Dong Chang An Jie 14 Beijing 100741
Phone:      +86-10-65203789
Fax-no:     +86-10-65203582
Nic-hdl:    HJ36-AP
Changed:    suny@publicf.bta.net.cn  19990716
Source:     APNIC
```

Figure 1—Original APNIC Database Entry

central leadership compound, Zhongnanhai, in April 1999, which led to the MPS leadership being criticized and purged. In addition, the MPS Computer Monitoring and Supervision Bureau has important responsibilities related to the Internet in China, including computer network security and management of ISPs.

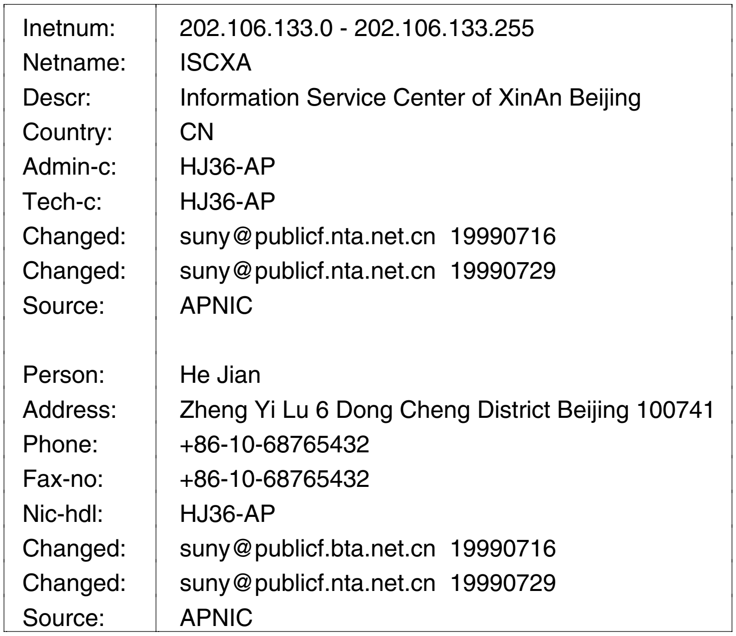
Of course, given the ambiguities of information warfare created by the structure of the Internet itself, intrusion-detection logs alone are usually not sufficient to identify whether the true source of an attack is the organization in question or simply a third party that has hacked into the MPS network and used it as a base to launch attacks. Four crucial pieces of evidence, however, strongly suggest that the MPS was the real culprit in the attacks against Falungong sites. First, the network had been established shortly before the information operations began and was divorced from other explicitly identified MPS networks in other parts of Chinese cyberspace, such as the domain spaces belonging to the MPS web page (www.mps.gov.cn). Second, the name of the organization in the database—Information Service Center—suggests an intent to deceive outsiders about its actual affiliation. Third, at least one Western media source claimed to have called the telephone numbers listed in Figure 1 and was told by the person answering the phone that the numbers belonged to the Ministry of Public Security.[87] A later call by the same news organization to the telephone operator at the ministry confirmed that the numbers belonged to the MPS Computer Monitoring and Supervision Bureau.[88] The fourth and most telling piece of evidence resulted directly from the impending exposure in the Western media of the network’s governmental affiliation. Probably as a result of the increasing media attention, especially an imminent article by Michael Laris in the *Washington Post*,[89] the information in the APNIC database was altered on 29 July 1999, as seen in Figure 2. Most important, the owners of the network space changed the damning street address of the owner of the network from #14 East Chang’an Street to #6 Zhengyi Road (listed in Figure 2 in transliteration as Zheng Yi Lu 6).

If the ministry’s network had itself been the victim of an attack and was thus wrongly accused as the perpetrator of the attacks on the Falungong site in the United States, why go to the trouble of changing the database information to an address other than MPS headquarters? And was it a coincidence that the network information was changed on the eve of an exposé in a major Western newspaper of the MPS’s alleged role in the attack? Most damning, the new street address (No. 6 Zhengyi Rd) is the address of the Ministry of Public Security’s No. 3 Research Institute, which is responsible for com-

[87] Svensson, “China Sect.”

[88] Ibid.

[89] Michael Laris, “Beijing Turns the Internet on Its Enemies: Sect Members Abroad Claim State Harassment,” *Washington Post,* August 4, 1999.



```
Inetnum:    202.106.133.0 - 202.106.133.255
Netname:    ISCXA
Descr:      Information Service Center of XinAn Beijing
Country:    CN
Admin-c:    HJ36-AP
Tech-c:     HJ36-AP
Changed:    suny@publicf.nta.net.cn  19990716
Changed:    suny@publicf.nta.net.cn  19990729
Source:     APNIC

Person:     He Jian
Address:    Zheng Yi Lu 6 Dong Cheng District Beijing 100741
Phone:      +86-10-68765432
Fax-no:     +86-10-68765432
Nic-hdl:    HJ36-AP
Changed:    suny@publicf.bta.net.cn  19990716
Changed:    suny@publicf.nta.net.cn  19990729
Source:     APNIC
```

Figure 2—Altered APNIC Database Entry (July 29, 1999)

puter security. The evidence cited earlier, along with this last attempt to further disguise the true owner of the network, strongly suggests that the perpetrator was caught with its "hand in the cookie jar."

Of course, the fact that the attacks might have originated from an MPS network does not automatically imply that they were sanctioned by the ministry leadership or their superiors in the senior party leadership. One possibility that must be considered is that the attack was carried out by a "rogue element" within the MPS, without approval from anyone. After the exposure of a rogue's efforts, a natural reaction would be to cover up the network's ministry affiliation by changing the APNIC data. One might question whether the ministry would be able to find the perpetrator, conduct an investigation of his actions, and implement a technical fix so quickly, but as improbable as that seems, it is not impossible.

One final footnote to the July 27, 1999, attack against FalunUSA.net: The manner in which the MPS allegedly brought down the site contains a fascinating twist. The denial-of-service attack was a classic “SYN flood” attack and appears to have been designed to make it appear as if Falungong was conducting information operations against the U.S. Department of Transportation (DOT).[90] In the July attack, the MPS network sent a SYN to the FalunUSA site with an incorrect return address, namely, a server controlled by DOT. A network engineer at DOT contacted Bob McWee and the operators of the other Falungong sites to find out why www.falundafa.org, www.falunUSA.net, and www.falundafa.ca were sending unauthorized packets to a DOT server, according to Everett Dowd, deputy director of telecommunications in the DOT Information Technology Operations office.[91]

Why, out of the millions of possible IP addresses, did the MPS choose an address belonging to DOT? One plausible hypothesis is that the perpetrator wanted a “two-fer”: crash the Falungong site, but also make it look as if the Falungong site was engaged in information operations against a U.S. government site. At the time of the attack, the entire Chinese governmental propaganda apparatus was in high gear, branding Falungong a “dangerous cult” and a “terrorist organization.” What better way to demonize Falungong than to make it appear that the organization was hacking sites run by the U.S. government? Indeed, system administrators at DOT initially thought they were under a different type of denial-of-service attack (a SYN-ACK flood) from the Falungong site, since all they could see on their end was a series of SYN-ACK requests entering their system from FalunUSA.net for no apparent reason. Only later did the DOT personnel realize that the Falungong site had simply been the unwitting accomplice of a third party.

[90] Any successful connection between two servers on the Internet requires a three-way “handshake” before information can be exchanged. First, Machine A sends a SYN to Machine B, which responds to Machine A with a SYN-ACK. Machine A then closes the loop by sending Machine B an ACK. The success of this exchange requires that all of the packets contain correct address information; otherwise, they will go to the wrong places. A SYN flood exploits this dynamic. In such an attack, Machine A sends a SYN with an incorrect return address to Machine B, which logically responds by sending its SYN-ACK not to Machine A but to Machine C. Since both Machine B and Machine C have a limited number of slots in their buffers for these sorts of unanswered queries, they both eventually suffer from buffer overflow and crash.

[91] Associated Press, August 6, 1999.

Attacks on Falungong sites in England and Australia during late summer 1999 bear some interesting similarities to the intrusions in the United States, particularly with regard to the source IP addresses of the perpetrators. The U.K. Falungong web site (http://www.yuanming.org.uk) was set up on July 20, 1999, by Zhu Bao, a Falungong practitioner living in Dublin, Ireland.[92] By July 23–24, 1999, the site had come under continuous attack from China-origin IP addresses. At the beginning of the attacks, the intruders disabled the server.[93] Later, they deleted all the original files and replaced them with the text of an article from the *Xinhua* News Agency entitled "The Person and Affairs of Li Hongzhi," falsely listing the author of the article as a member of the "Falungong Research Society." The article says that Li

> is not the "highest Buddha" who brings salvation to suffering people, but an evil person who has had an extremely disastrous effect upon society. Li is not bringing salvation to practitioners, but is in fact leading them to a disastrous and miserable end, and Falungong is doing enormous harm to both the mental and physical health of people.

Falungong's U.K.-based service provider (NetScan, www.netscan.co.uk) confirmed that the intruders had obtained their root password.

In a separate attack, Li Shao of Nottingham publicly reported on July 26, 1999, that his Falungong site was attacked by hackers operating from a Chinese IP address.[94] Falungong sources claim that the British police linked the address to the Information Service Center of XinAn in Beijing, discussed above, but no independent confirmation was possible.[95]

In Canada, two Falungong sites (www.minghui.ca and www.falundafa.ca) were attacked by hackers, and both eventually succumbed. The ISPs for these sites, Bestnet Internet of Hamilton, Ontario, and Nebula Internet Services of Burlington, Ontario, re-

[92] Jonathan Dube, "China Ate My Web Site," ABCNEWS.com, August 6, 1999.

[93] The details of this attack are derived from Falungong, "Report," p. 23.

[94] Svensson, "China Sect."

[95] Falungong, "Report," p. 87.

ported that their networks were attacked on July 30, 1999, by Chinese government servers because they hosted sites run by Canadian followers of Falungong, including Jason Xiao, the system administrator of www.falundafa.ca.[96] According to the director of Bestnet Internet, Eric Weigel, the hack attempts originated with "Chinese government offices in Beijing." Weigel stated that the specific originating addresses belonged to the Beijing Application Institute for Information Technology (BAIIT) and the Information Center of XinAn Beijing.[97] No IP addresses were furnished by the newspaper accounts, but BAIIT's networks can be found between 203.93.160.0 and 203.93.160.255. Possible government connections are suggested by the P.O. box mailing address provided by BAIIT in the APNIC database, as P.O. boxes are often used in lieu of street addresses by Chinese government and military hosts. By contrast, the government affiliations of the Information Center of XinAn Beijing are much clearer, as discussed in greater detail earlier in this chapter.

Nebula Internet Services reported that the same sites had attempted to crash its servers, using similar types of attacks. According to Nebula representatives, the assault went on for more than a month, coinciding with the timetable of the government crackdown on the sect. Unlike Bestnet, which had more-advanced equipment and was able to withstand the attacks with little loss of service, Nebula's systems were crippled by the hackers, and the company was forced to shut off its service. The owner of two Canadian Falungong sites (perhaps the same sites discussed above), Jillian Ye of Toronto, claimed that her sites had been under attack every day for several months and that the problems had gotten progressively worse until she finally moved the sites to a more secure server.[98]

Fewer similarities exist between the attacks described above and those against Falungong servers based in Australia, but the timing of the Australian attacks (in late summer 1999 and mid-spring 2000) coincides to a significant degree with attacks in other countries. An Australian practitioner of Falungong established a Falungong mirror

[96] Peter Goodspeed, "Falung Gong, Beijing Wage War over Internet," *National Post*, November 2, 1999.

[97] Oscar Cisneros, "ISPs Accuse China of Infowar," *Wired News*, July 30, 1999.

[98] Svensson, "China Sect."

site (http://falundafa. au.cd) in March 1997 on a Windows NT server.[99] On September 6, 1999, computer attacks originating from a Chinese IP address forced this site to shut down.[100] The victims reported to the police that the intruders tampered with their e-mail system. The system administrator of the site noticed that the infiltrators were able to manipulate the cursor on their screen, which suggests that the attackers were using a hacker tool known as Back Orifice[101] to penetrate the site. Beginning in September 1999, Australian police undertook constant monitoring of the site.

Spring 2000. The first of the renewed attacks against Falungong servers occurred on March 11, 2000, coinciding with the meetings of the National People's Congress in Beijing. The hack, which used a denial-of-service technique known as a "smurf" attack, brought down the main server in Canada (www.minghui.ca), as well as three mirror sites (www.falundafa.ca, www.falundafa.org, and www. minghui.org).[102] Since smurf attacks are quite effective in masking the identity of the attacker, no useful source information could be gained from the logs of the intrusions.

Attacks on Falungong servers reached a crescendo in mid-April 2000, when five sites—three in the United States (www.falunUSA.net, www.falundafa.org, www.truewisdom.net) and two in Canada (www.

[99] Interview, Falungong practitioner, June 2000.

[100] "Falungong Hot on Jiang's Trail," *Agence France Presse*, September 7, 1999.

[101] The hacker tool Back Orifice was developed by the Cult of the Dead Cow (CDC).

[102] Smurf attacks employ a two-step procedure. First, hackers scan the Internet for vulnerable servers or host computers. Ideal target systems have relatively wide bandwidth and few IP addresses, characteristics found in servers operated by universities (.edu) and nonprofit organizations (.org). The networks of these servers are often composed of subnetworks. Usually, a request sent to the main IP address is answered by every computer on the local network. In other words, if the local network has 40 subnetted computers, one request will result in 40 replies. These types of servers can be used as "Internet request amplifiers" or "slaves" for a smurf attack. Hackers will assemble large numbers of these slaves for an impending attack, hoping to direct all of their bandwidth toward a single target server.

In the second step, hackers issue the signal to the slaves. Attackers forge a ping command that appears to be coming from the target computer. For every fake ("spoofed") ping they send, the victim is flooded with many (40, in our example) replies. A dial-up user with 28.8 kbps of bandwidth exploiting this technique on our illustrative network could generate (28.8 × 40) or 1152.0 kbps of traffic, about 2/3 of a T1 link. The smurf attacks that brought down eBay and Yahoo! used much larger sets of networks.

minghui.ca and www.falundafa.ca)—were smurf-attacked simultaneously.[103] The timing of the attacks coincided with two sensitive political events: (1) the impending vote in the United Nations Human Rights Commission on a UN resolution condemning Chinese human-rights abuses, including persecution of Falungong; and (2) the one-year anniversary of the April 25, 1999, gathering of Falungong practitioners outside the central leadership compound in Beijing.

Falungong system administrators received a variety of warnings about the impending attack. Around April 6, Falungong received an e-mail warning that the Public Security Bureau had paid two network security companies to hack the group's sites abroad. After the first wave of attacks, Falungong system administrator Li Yuan received an anonymous tip on April 12 confirming the situation. "We received an anonymous e-mail from a Chinese computer expert on April 12 warning us that the police computer security bureau had offered to pay a computer company money to hack into our sites," said Yuan.

According to the Maryland-based system administrator for FalunUSA, the attacks themselves began around April 9 or 10. The intruders attacked the IP addresses of the sites, not the domain names, and likely got into the system using security holes in the ftp command. Once inside, the attackers replaced most of the original network command files (e.g., *ls*, *df*, and *find*) with versions of these files that contained "trojan horses" for later penetration. The system administrator reports that after he discovered and dismantled the hackers' efforts, intruders attempted to log on to his server, using ftp and SSH commands, but these probes were rebuffed.

In Australia, the attacks started again between March and May 2000, with the most serious attack coming on May 22. The Australian server was crashed by hackers around 3 a.m. on May 22, rebooted the next morning, and hacked again one hour later. It was not rebooted a second time until 7 or 8 p.m. Logs of these attacks and the addresses of the attacking sites were unavailable for analysis, but the Australian system administrator said that the intruders used an exploit known as IISATTACK, and their IP addresses could be traced to Hong Kong,

[103] "Web Sites of Falungong Hit," *Agence Prance Presse*, April 14, 2000.

England, and the United States. The system administrator asserted that the attacks in 2000 were far more sophisticated than those in 1999, and the attackers were able to easily exploit the server's remote logins, which were later disabled by its owners.

Monitoring and Filtering. Foreign visitors to China and domestic dissidents have long been aware that the Chinese government is engaged in widespread monitoring of communications. According to the 2000 State Department China human-rights report:

> [The Chinese] authorities often monitor telephone conversations, fax transmissions, e-mail, and Internet communications of citizens, foreign visitors, businessmen, diplomats, and journalists, as well as dissidents, activists, and others.[104]

The extent of this monitoring, however, is frequently overstated, as the sheer scale of the necessary effort is beyond the resources of the security apparatus. This is especially true of electronic communication.[105] Members of the security apparatus suggested in interviews that they recognize the technical difficulties—or, rather, the impossibility—of wide-scale e-mail monitoring, regardless of encryption. While research in keyword searching applications continues, even its advocates realize that a network system would grind to a halt if keyword searches were attempted on a nationwide or even a regional basis, given the enormous volume of electronic communication.[106] Public security sources confirm that selective, often *post hoc*, monitoring, combined with traditional surveillance methods, is a preferable and far more effective strategy.[107]

Fragmentary evidence exists to support the notion that the security services possess and are actively developing limited monitoring and

[104] U.S. Department of State, *China Country Report on Human Rights Practices, 2000*, February 23, 2001, p. 15.

[105] Recently, the apparently modest results of U.S. efforts to track terrorists through the Internet have illustrated the difficulties of conducting online surveillance against users who seek to evade detection by communicating with each other via anonymous e-mail accounts accessed at Internet cafes, sometimes using strong encryption. See, for example, Susan Stellin, "Terror's Confounding Online Trail," *New York Times*, March 28, 2002.

[106] Interviews, Western executives, January 2000.

[107] Interviews, PRC officials, January 2000.

filtering capabilities. The anonymous author of an article entitled "China's Main Methods of Supervising and Controlling the Net and Countermeasures," which was recently published on a Chinese-language dissident web site, asserts that there are two types of methods used by the Chinese authorities to monitor and control e-mail communications: filtering software (*guolu ruanjian*) and selective examination (*choucha*) of users' electronic mailboxes.[108] This is confirmed by a number of other sources. In a published interview, a computer engineer claiming to be employed by the Public Security Bureau asserted that his organization monitors information aimed at "undermining the unity and sovereignty of China" (i.e., references to Tibetan independence or the Taiwan question), communications that attempt to propagate new religions, and dissident publications by filtering for selected keywords.[109] Human Rights Watch reported that in May 1998, the Ministry of Labor and Social Security installed monitoring devices at the facilities of ISPs that can track individual e-mail accounts.[110] In January 2000, Liu Ming, the younger sister of student leader Liu Gang, wrote an indictment against the Changchun City Public Security Bureau, which was then disseminated abroad via the Internet by Leng Wanbao, a noted dissident in Changchun City, Jilin Province. Leng was picked up and interrogated for three hours by the police, who knew about the activity immediately.[111] A Heilongjiang Harbin University student, Zhang Ji, was arrested for disseminating "reactionary information via the Internet." He was alleged to have been sending e-mail messages to Falungong web sites in the United States and Canada, as well as downloading information from those web sites and relaying it to fellow Falungong practitioners. Falungong sources in the United States believe that police copied the e-mail addresses of Falungong net users, and their e-mail passwords were obtained from mainland ISPs. As a result, the U.S. Falungong sources believe that all e-mail from Falungong practi-

[108] *Zhongguo dui wangluo de zhuyao jiankong fangfa he duice* [China's Main Methods of Supervising and Controlling the Net and Countermeasures], www.internetfreedom.org/gb/articles/1012.html.

[109] Geremie Barme and Sang Ye, "The Great Firewall of China," *Wired 5.06*, June 1997.

[110] U.S. Department of State, *China Country Report on Human Rights Practices, 1999*.

[111] "Report on PRC Controlling Dissidents' E-mail," Hong Kong Information Centre for Human Rights and Democratic Movement in China, January 19, 2000, in *FBIS*, January 19, 2000.

tioners that passes through 163.net and 263.net is now monitored by the Chinese government. Falungong practitioners in China also claim that the Public Security Bureau has intensified its efforts to identify Internet users who try to access the group's overseas web sites.[112] Finally, the Committee to Protect Journalists asserted in its 1999 report that the Ministry of State Security has an entire department devoted to tracking dissidents and their writings on the Internet.[113]

Chinese Internet users have responded to these efforts with a variety of protective countermeasures.[114] One of the simplest, but most effective, consists of logging onto the Internet anonymously at one of the Internet cafes that are by now ubiquitous in many Chinese cities. Chinese-language Internet postings advise mainland users on appropriate security measures for covering their tracks at Internet cafes.[115] In some cases, it is also possible to exploit gaps in the monitoring technology. For instance, some net companies use software to identify occurrences of a leader's name in online postings so they can remove any unfavorable comments, but chat room visitors reportedly dodge that restriction by putting a space between characters or using nicknames.[116] Other users protect themselves by discretion. Before June 4, 2000, the discussion of Tiananmen issues quieted down significantly. Frequent visitors to popular chat rooms reportedly posted warnings asking fellow chat room visitors to avoid leaving sensitive messages about June 4 on the Internet. On June 1, some messages in chat rooms claimed that Internet portals had re-

[112] Craig S. Smith, "Sect Clings to the Web in the Face of Beijing's Ban," *New York Times*, July 5, 2001.

[113] "State Tracks Dissidents Online," Associated Press, March 24, 2000.

[114] See, for example, Shi Lei, "*Xinxi bailinqiang: tupo zhonggong wangluo dianzi youjian fengsuo* (*zhiyi*)," [The Information Berlin Wall: Breaking the Chinese Communist Party's Net and E-mail Blockade (Part One)], November 2, 2001; and Shi Lei, "*Zhonggong ruhe guolu he jiecha wangluo dianzi youjian: tupo zhonggong wangluo dianzi youjian fengsuo* (*zhi er*)" [How the Chinese Communist Party Filters and Monitors the Net and E-mail (Part Two)], November 2, 2001, available on the web site of the Home for Global Internet Freedom at http://www.internetfreedom.org/gb/articles/997.html.

[115] "*Wangba shangwang de yixie anquan wenti*" [Some Security Problems of Going On-Line at Internet Cafes], internetfreedom.org/gb/articles/979.html.

[116] Julie Schmit and Paul Wiseman, "Surfing the Dragon: Web Surfers Find Cracks in Wall of Official China," *USA Today*, March 15, 2000, p. 01B.

ceived warnings from police to delete messages about the 1989 movement, as well as messages about the recent murder of Beijing University student Qiu Qingfeng.[117]

Finally, users have sought safety in numbers. After Chen Shui-bian's inauguration speech in May 2000, Chinese BBS were overflowing with critiques and commentaries, many of which disagreed with the PRC government's policy and conduct. The BBS on the *People's Daily* web site became a particularly intense hotbed of comment, overwhelming the ability of the censors to deal with it, though they were able to prevent the posting of the text of Chen's speech.[118] This was an interesting choice of priorities, highlighting the extent to which the government seeks to deny the population access to primary sources of information that would allow them to form opinions other than those generated by the propaganda apparatus.

Propaganda, Denial, Deception, and Disinformation. The deceptive practices of the Chinese government on the Internet take a number of forms. The first is *denial,* in the strict sense of the word. In October 1998, the PRC government-controlled Chinese Society for Human Rights, which represents China in its expanding human-rights dialogue with other countries, launched a web site (www.humanrights-china.org) to promote Beijing's official line on the subject and deny the accounts of Chinese human-rights abuses alleged by nongovernmental organizations. The site contains government documents in Chinese and English, including articles from the state-run media, legislation, and lectures from a symposium on human rights that Beijing hosted.[119] (U.S.-based "hacktivists" successfully penetrated this site in late October 1998, replacing its front page with an impassioned attack on the Chinese government's repressive policies and a trenchant criticism of the site's poor network security.[120])

[117] Josephine Ma, "Cyber-Crackdown Fails to Silence Protesters," *South China Morning Post*, June 2, 2000.

[118] Michael Dorgan, "Chinese Censors Losing Online Race," *San Jose Mercury News*, May 22, 2000.

[119] "China: We're Only Human," Reuters, October 26, 1998.

[120] For an account of the hack, see "China Cyber-Cops Partially Block Hacked Web Site," Reuters, October 29, 1998. For the Chinese response to the attack, see "Hacker Attacks Society for Human Rights Studies Web Site," *Xinhua*, October 29, 1998, in FBIS, October 29, 1998.

The second deceptive tactic is *passive disinformation about third parties.* For example, as part of the campaign against Falungong, the Chinese Academy of Social Sciences (CASS) has established a web page to combat cults and expose their evil intentions and activities. The web site is divided into six topics, including theories of Marxism, atheism, and materialism, as well as analysis and exposure of the Falungong cult and a general survey of cults in other countries. Its content is similar to the overall anti-Falungong propaganda campaign that has been waged relentlessly by Beijing since August 1999. CASS claims that as of May 10, 2000, the site had received over 500,000 hits.[121]

The third deceptive tactic is *active disinformation,* including harassment and character assassination. One victim of such harassment, Frank Siqing Lu, claimed that after the suppression of the CDP in late November 1998, public security offices used the names of local dissidents to page him and leave return numbers that were either nonexistent or numbers for hotels, karaoke bars, and hospitals. Public security officials also allegedly bombarded his fax machine with large numbers of blank pages.[122]

Similar tactics are reported by Falungong members both in China and abroad. There is some evidence to suggest, for instance, that individuals have been redirecting e-mails from China to send fake articles by Li Hongzhi to Internet users in China, using a flaw in Internet mail protocols that is easily unmasked. On February 28, 2002, a Falungong practitioner in Beijing received an e-mail from editor@minghui.ca, the legitimate address of one of the main Falungong sites in Canada. The message contained a fake Li Hongzhi article. Closer inspection of the e-mail header reveals that the message actually originated from IP address 202.106.227.134, which is located in Beijing, not Canada.[123] An additional harassing technique reported

[121] "China Establishes Web Page to Combat 'Cults,'" *Xinhua*, May 10, 2000, in FBIS, May 10, 2000.

[122] Maureen Pao, "Information Warrior," *Far Eastern Economic Review*, February 4, 1999. See also "PRC Said Interfering in Information Center's Work," Hong Kong Information Center of Human Rights and Democratic Movement in China, January 8, 1999, in FBIS, January 8, 1999.

[123] The full header of this e-mail can be found in http://hrreport.buhuo.net/book2e/eb210-1.html#3.

by Falungong practitioners abroad is e-mail bombardment. According to interviews, the personal e-mail of group members, as well as the official Falungong e-mail addresses, is regularly saturated with hundreds or thousands of bogus messages (as many as 20,000, in some cases), making it impossible to use the Internet for reliable communication. Similarly, Falungong web pages are repeatedly saturated with bogus requests from IP addresses that do not exist, preventing other users from visiting the pages.[124]

Members of the overseas dissident community, which has been riven by personality and ego clashes, appear united in their belief that the Chinese government is spreading rumors and planting false agents in their midst, with the goal of furthering dividing the already notoriously factionalized movement. In October 1999, Wei Jingsheng told a Taiwanese news agency that the Beijing government is using the Internet to spread rumors intended to "sow seeds of discord" among organizations of mainland Chinese dissidents.[125] Interviews in June 2000 with members of prominent dissident groups confirm these perceptions. If the Chinese government is indeed pursuing this strategy, it is succeeding beyond its wildest dreams. Dissident bulletin boards and chat rooms are regularly filled with accusations and counteraccusations, primarily revolving around the question of which dissidents are actually paid agents of the Ministry of State Security. It is generally impossible to ascertain conclusively the true identities of the posters of such messages, making it relatively easy for the Chinese security services to engage in clandestine disinformation operations of this type.

MEASURING SUCCESS

Numerous possible metrics exist for measuring the government's success in thwarting the political use of the Internet by domestic and external forces, but one salient fact stands out: There are currently no organizations inside or outside China using the Internet to mount a credible threat to the survival of the regime. Indeed, the 1999 State Department human-rights report asserted that by the end of 1998,

[124] *New York Times*, September 9, 2000.

[125] "Internet Used to Promote Freedom of Expression in China," Taiwan Central News Agency, October 2, 1999.

there were no organizations posing a legitimate threat to the regime, regardless of their means of communication:

> By year's end [1998], almost all of the key leaders of the China Democracy Party (CDP) were serving long prison terms or were in custody without formal charges, and only a handful of dissidents nationwide dared to remain active publicly. Tens of thousands of members of the Falungong spiritual movement were detained after the movement was banned in July; several leaders of the movement were sentenced to long prison terms in late December and hundreds of others were sentenced administratively to reeducation through labor in the fall.[126]

The situation did not improve in 1999, 2000, or 2001. Indeed, by most measures, it has since deteriorated. As a recent State Department report on human rights in China observed, "only a handful of political dissidents remained active" by the end of 2000.[127]

FUTURE TRENDS

Does Beijing's relative success in controlling dissident use of the Internet indicate that the Internet will have only a limited effect on China's political landscape? Some analysts argue that, at least in the short to medium term, the spread of the Internet will tend to benefit authoritarian regimes at the expense of dissidents and prodemocracy activists. As Kalathil and Boas observe, for example, China and other authoritarian states have responded effectively to the dissident challenge by implementing a combination of reactive measures, including blocking web sites and jailing activists, and proactive policies, such as distributing propaganda online and offering e-government services.[128] This has enabled China to minimize the Internet's potential as an instrument for "subversive" activity while simultaneously strengthening the position of the regime. "The

[126] U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, *China Country Report on Human Rights Practices, 1999*, February 25, 2000.

[127] U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, *China Country Report on Human Rights Practices, 2000*, February 23, 2001, p. 2.

[128] Shanthi Kalathil and Taylor C. Boas, "The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution," Carnegie Endowment Working Papers, No. 21, July 2001, pp. 1–10, 15–18.

Chinese state,” Kalathil and Boas write, “has shown that it can use the Internet to enhance the implementation of its own agenda.”[129] Indeed, authoritative pronouncements in the state-controlled media have called for more-extensive use of the Internet in “guiding opinion.” An August 9, 2000, *People’s Daily* commentator’s article, for example, called for the strengthening of “positive propaganda and influence on the Internet” to enable the government’s “ideological and political work” to become “more inclusive and influential.” The commentator went on to note that official Internet sites “accurately and comprehensively publicize the Party line, strategies and policies, and consistently guide people with correct state opinion.”[130] Chinese scholars have also recognized the Internet’s potential as an effective tool for carrying out “political thought work” and disseminating propaganda.[131] China’s proactive efforts to use the Internet to bolster regime power, however, have thus far produced only limited results. For example, although Beijing has actively promoted a “government online” plan, a recent survey of e-government initiatives around the world found that China ranked eighty-third out of 196 countries.[132]

Measures of a more reactive nature will thus continue to occupy a dominant place in Beijing’s strategy for dealing with dissident use of the Internet. There is some evidence that Beijing’s technical countermeasures are becoming increasingly sophisticated. In future efforts to limit what Beijing views as the pernicious side effects of the spread of the Internet in China, however, the authorities will likely try to combine low-tech and high-tech measures. This evolving approach is illustrated by Beijing’s recent efforts to tighten its control over

[129] Ibid., p. 8.

[130] “Vigorously Strengthen the Building of China’s Internet Media,” commentator’s article, *Renmin ribao*, August 9, 2000, in FBIS, August 9, 2000.

[131] Xie Haiguang (ed.), *Hulianwang yu sixiang zhengzhi gongzuo gailun* [*Introduction to the Internet and Political Thought Work*], Shanghai: Fudan University Press, 2000.

[132] World Markets Research Centre and Brown University, “Global E-Government Survey,” September 2001. The United States placed first, followed by Taiwan, Australia, Canada, the United Kingdom, Ireland, Israel, Singapore, Germany, Finland, and France. The sophisticated e-government program of Taiwan stands in sharp contrast to the PRC’s “government online” project. For example, Taiwan President Chen Shui-bian has a weekly e-mail Internet newsletter, called *President A-bian’s E-Paper*. See www.president.gov.tw/1_epaper.iod.html. President Chen has also engaged in live, online chat sessions with Internet users in Taiwan.

China's nearly 100,000 Internet cafes.[133] During a nationwide sweep that began in April 2001, the authorities shut down more than 17,000 Internet cafes for allowing access to pornographic or "subversive" web sites, according to *Wen Hui Bao*, an official Shanghai-based newspaper. Some 28,000 more Internet cafes were ordered to install software that prevents users from accessing forbidden web sites and enables the establishments to monitor user activities.[134] While there is little information available about the software, other official media reports indicate that Internet cafes in major cities such as Xi'an and Chongqing have installed programs called "Internet Police" and "Internet Cafe Security Management System" to block access to banned content and make it easier for police to track users engaging in "subversive" activities online.[135] Beijing does not rely on software alone to control what users do in Internet cafes. Indeed, the authorities rely just as heavily on Internet cafe owners and employees to prevent visitors from viewing banned material on the Web. Because their interests lie in earning profits, not engaging in politics, the proprietors of many of the estimated 94,000 Internet cafes in China are willing to cooperate with local authorities.

While Beijing's countermeasures have been relatively successful on the whole, the current lack of credible challenges to the regime, despite the introduction of massive amounts of modern telecommunications infrastructure, does not lead inexorably to the conclusion that the regime will continue to be immune from the forces unleashed by the increasingly unfettered flow of information across its borders. While Beijing has done a remarkable job of finding effective counterstrategies to the potential negative effects of the information revolution, the scale of China's information-technology modernization would suggest that time is eventually on the side of the regime's opponents. Nina Hachigian predicts that "control over information will slowly shift from the state to networked citizens," leading to po-

[133] Some observers have speculated that the crackdown may have had more to do with the desire of the authorities to collect registration fees from delinquent Internet cafe proprietors than concerns about what Internet users were doing at the cafes.

[134] "17,000 Internet Bars Shut Down," *South China Morning Post*, November 21, 2001.

[135] "Internet Police Software Installed in 800 Xi'an City Internet Bars," *Xinhua*, August 7, 2001; see also "New Software Censors Web in Chongqing Net Cafes," *China Online*, August 14, 2001, which cites other official media reports.

tentially "seismic" changes.[136] Rising levels of economic development and concomitant demands for political participation on the part of a growing middle class are often cited as the primary motors of pluralization and liberalization, but recent statistical analysis found an even stronger correlation between democracy and the availability of networked communications technology,[137] suggesting that the Internet may prove over time to be a driving force for democratization. At least a few Chinese scholars are in agreement with the basic thrust of this assessment. In the words of one Chinese researcher, "It will be impossible to control this technology completely, even with filters and an army of trained digital agents."[138]

In the short to medium term, however, the multifarious close partnerships between the regime and the commercial Internet sector, institutionalized in a complex web of regulations and fiscal relationships, imply that the government will not lose the upper hand soon. The government's strategy is also aided by the current economic environment in China, which encourages the commercialization of the Internet, not its politicization. As one Internet executive put it, for Chinese and foreign companies, "the point is to make profits, not political statements."[139] Thus, the Internet, despite the rhetoric of its most enthusiastic supporters, will probably not bring "revolutionary" political change to China, but instead will be a key pillar of China's slower, evolutionary path toward increased pluralization and possibly even nascent democratization.

As dissident use of the Internet and regime countermeasures continue to evolve in China and other authoritarian countries, future research should not only update this unfolding story but should also place it in a comparative framework to help enhance our understanding of the political impact of the Internet in these countries. Comparing the political role of the Internet in a variety of authoritarian, quasi-authoritarian, and nondemocratic states in Asia—namely, China, Myanmar, Singapore, Vietnam, and Malaysia—would repre-

[136] Nina Hachigian, "China's Cyber-Strategy."

[137] Christopher R. Kedzie, *Communication and Democracy: Coincident Revolutions and the Emergent Dictator's Dilemma,* Santa Monica, CA: RAND, 1997.

[138] Chinese researcher, January 2001.

[139] Interview, U.S. businessperson, 2001.

sent a useful next step in this process. The research agenda could then be broadened to compare the situation in these countries with that in states outside the region, perhaps including Iran, Saudi Arabia, and Cuba, to produce more widely applicable conclusions about the political use of the Internet in authoritarian countries.