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 de-

tail, 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 con-

tains 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.