

The Great Firewall of China: Cyber-policing dissent

by David Banisar

In March, 2001, ordinary Chinese citizens used news websites and chat rooms to expose government attempts to hide the deaths of 38 children and four adults in an explosion in the south-eastern province of Jiangxi. Corrupt teachers, Communist officials, and businessmen had forced the children, some as young as eight, to hand-manufacture firecrackers to pay school fees. At first Premier Zhu Rongji blamed a suicidal villager for the tragedy. Nine days later, as outrage and facts spread across the internet, the premier was forced to make an extraordinary public apology.

Activists like those who pressured Premier Zhu are among more than 45 million Chinese internet users who are finding unprecedented opportunities to exchange ideas and information censored in traditional media. So while the Chinese Communist Party (CCP) views the internet as a boon to the country's rapidly developing economy, it also sees the web as a danger to its own control.

To counter that threat, while still allowing 100,000 internet cafés to bloom, Beijing has imposed a shrewd combination of technology, laws, and intimidation to create the world's most sophisticated system of electronic monitoring and censorship. The internet is only the latest mass media channel for unapproved, uncensored dialogue in China. Following in the footsteps of call-in talk radio programmes that flourished in China through the 1990s, ordinary citizens are going online in record numbers. Under the cloak of anonymity, they chat online about sex, scandal, and politics with a frankness once reserved for the dinner table. They report local corruption, accidents, and murders that public authorities would probably have succeeded in covering up.

'When private citizens in China first gained access to the internet in 1995,' said Xiao Qiang of the New York-based Human Rights in China, 'overseas Chinese dissident groups were actively using the internet as a communicating, organizing, and advocacy tool. We were already internet-savvy.' Many of the activists exiled after the 1989 Tiananmen Square crackdown plugged into this international network. Today dissident groups inside and outside of China regularly email newsletters to tens of thousands of Chinese citizens and maintain sophisticated websites, such as the Hong Kong-based China Labour Bulletin, founded by labour activist and former political prisoner Han Dongfang. The spiritual group Falun Gong used the internet to help rally some 10,000 practitioners for a silent vigil at the central leadership compound in April 1999.

Other totalitarian regimes, including North Korea and Myanmar, reduce the risk of damning revelations such as official culpability in the Jiangxi fire by simply banning the internet outright.

China, however, is trying to balance access and control. It limits 'subversive' use by combining traditional techniques – arrest, surveillance and harassment – with new blocking and surveillance technology.

And Beijing passes laws that would impress George Orwell himself. In the last five years, according to Amnesty International's report, State Control of the Internet in China, Beijing has drafted more than 60 rules on internet usage. Regulations now ban harming the 'honour' of China, disturbing 'state order', and revealing 'state secrets' –a crime that carries the death penalty. Beijing regularly shuts down internet service providers (ISPs) that don't comply, and dismantles domestic websites that discuss politics or other banned topics. In 2002 the government closed thousands of unlicensed internet cafés.

Party leadership, from hardliners to more liberal-minded reformers, endorses the controls. 'There's a liberal wing that thinks that, in general, the realm of public expression can be looser than it is and still help rather than hurt party rule,' said Andrew Nathan, professor of political science at Columbia University and author of numerous books on Chinese politics. 'But all are agreed on preventing forces from organizing to challenge the party. So there's enough agreement to undergird the basic policy of getting dissidents off the internet.'

Authorities mete out harsh punishment to offenders. Amnesty International has investigated the cases of 33 prisoners of conscience arrested for using the internet. These include two members of the Falun Gong movement who died in custody, according to AI's report, as well as activists and writers calling for political reforms. Essayist Chen Shaowen was arrested in September 2002 after publishing articles online about unemployment and inequalities in the legal system. The government charged him with 'subverting state power' and 'sending in numerous articles of all sorts, fabricating, distorting and exaggerating relevant facts, and vilifying the Chinese Communist party and socialist system.'

Others face severe consequences for exposing official ineptitude, corruption, or even public health problems – often at the local or provincial level. In April 2001 Wang Sen was arrested for 'libelling the police' after he exposed a medical centre in Dachuan for selling tuberculosis medicine that had been donated by the Red Cross. A year later in August 2002, Wan Yanhai used the internet to disclose that thousands of people in Henan had been infected with HIV after they donated blood at government-sponsored clinics. Detained in August 2002, he spent a month in jail before international pressure and his confession to revealing state secrets secured his release.

In 2002, the CCP propaganda department issued a directive against online stories that 'affect social stability', citing coverage of China's AIDS epidemic as an example.

Monitoring web sites

Chinese authorities have always kept close tabs on dissidents and others who challenge the CCP, and now they are adapting their methods to fit the technology. Beijing requires each web-site to monitor chat rooms and delete politically sensitive posts. In addition, ISP employees called 'Big Mamas' (Da Mama) lead teams of volunteers in ferreting out and removing messages that 'jeopardize state security', 'disrupt social stability', or 'spread superstition and obscenity'. They report offenders to the authorities and yank live discussions offline when users start criticizing the government.

To ensure that these companies are keeping up, some 30,000 state security personnel monitor websites, private emails, and chat rooms. 'People are used to being wary, and the general sense that you are under surveillance acts as a disincentive,' said one Public Security Bureau officer quoted in a Rand report. 'The key to controlling the net in China is in managing people, and this is a process that begins the moment you purchase a modem.'

Authorities have eager partners in the private sector, where self-censorship for profit abounds. Some 300 companies, including Yahoo China, have signed the 'Public Pledge on Self-Discipline'. It requires ISPs to record activity, scan for and remove subversive materials, and forward objectionable messages to the authorities.

When human eyes fail, technology picks up the slack. China now has a sophisticated system of tools that both block access and conduct automated surveillance. This 'Great Firewall of China' bars users from some 19,000 sites, according to the Berkman Centre at Harvard University. Most are political or religious. So while Chinese users can easily look at pornography online, they cannot access Amnesty International, Human Rights in China, Human Rights Watch, or sites relating to Tibet or Taiwan. The depth of the censorship is startling; Chinese web surfers cannot access the home pages of court systems in the United States, Australia or the UK. New filters triggered by terms such as 'Falun Gong' and 'human rights and China' restrict searches on the Google and Altavista search engines.

Nationwide digital surveillance

Western companies are only too willing to hone surveillance technology for China's use. Major companies, including Sun Microsystems, Cisco Systems, and Nortel Networks, are helping China develop 'Golden Shield', a system that would combine local internet surveillance with ID cards, databases, and video cameras, according to a report by the Canadian International Centre for Human Rights and Democratic Development. The report describes Golden Shield as 'a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance.' Once this technology is perfected, developers may find interested buyers in the United Kingdom, or perhaps with Washington's proposed Total Information Awareness Programme. Under a Bush administration proposal, the TIA office would develop technology allowing the government to collect information on an individual's medical history, travel, financial transactions, and other activities.

Meanwhile, China's Ministry of Public Security appears to be sponsoring an army of hackers to attack dissidents based abroad. Tibetan independence groups report an unrelenting barrage of e-mail viruses targeting their networks, including some traced back to Chinese government offices. Falun Gong websites run from outside China also have been hit by a breathtaking variety of attacks: daily, coordinated assaults on multiple ISPs housing Falun Gong websites; hundreds of e-mail viruses sent each day; and in a May 2002 case, a hacking incident that destroyed the entire site of a Falun Gong supporters' group.

'Their whole site just disappeared,' said Scott Chinn, webmaster for New York's Falun Gong. 'There's also a European Falun Dafa site which had its content replaced with articles from the People's Daily, which is a Communist Chinese newspaper.'

Chinese Internet users have artfully dodged each new advance in surveillance and blocking, only to face new impediments. They avoid filters on mass e-mails by frequently changing addresses and servers. They use proxy servers to reroute requests through unblocked sites. Most recently, they have adopted peer-to-peer technology, best known for programmes like Napster, to transfer political information in a way that makes them more difficult to track. But like a Spy-vs.-Spy cartoon, the government counters with new techniques to block new tactics used by dissidents, who then change their configurations to thwart the blocks, and so on.

Washington has funded some tools, such as SafeWeb, to counter Chinese censorship of Voice of America and Radio Free Asia. In October 2002, Rep. Christopher Cox (R-CA) introduced the Global Internet Freedom Act, which would provide \$50 million in funding for two years to combat internet censorship.

By all accounts, however, the Chinese government has managed to keep the average internet user on a tight leash. Optimists argue that the democratising nature of the medium will prevail because the CCP cannot control every facet of internet use. At the same time, however, there are plenty of customers around the globe for the surveillance and blocking technology used by the CCP, among them the United States.

From Amnesty Now, Spring 2003, pp. 24-26, a publication of Amnesty International, 322 Eighth Avenue News York NY 10001-4808. tallen@aiusa.org.

David Bansar is a visiting research fellow at the Cyberlaw Research Unit at Leeds University and deputy director of Privacy International, London, both in the United Kingdom.