



On The Cover/Top Stories

Cracks In the Wall

Richard C. Morais, 02.27.06

With engineering help from half a dozen Western firms, the Chinese Communist Party has erected a huge apparatus to censor free speech. A ragtag crew of hacker dissidents may succeed in tearing it down.

In a windowless room in New York City a computer engineer with owlsh glasses--call her "Jenny Chen"--peers at a color-coded bar graph on her PC screen. Her group is launching attacks on the Chinese wall of censorship that blocks access to sites discussing verboten topics like civil rights and democracy. The graph displays how many Chinese that month evaded the country's censorship to condemn the Chinese Communist Party.

Chen, a Beijing-born woman of about 40, runs her own it businesses. Her group, and like-minded "hacktivists" (as they call themselves) spread around the globe, are chipping away at the Golden Shield, the term that describes the filtering system that censors the Internet and e-mail of China's 110 million Internet users. The invaders slip contraband words and ideas in and out of the country via such means as mass e-mails, proxy servers that aren't yet blacked out and code words that aren't yet on government blacklists.

Arrayed in battle against the hackers are the Chinese Communist Party and an assortment of Western firms that provide the hardware, software and search services that make the Chinese Internet run: Cisco, Google, Microsoft, Nortel Networks, Sun Microsystems and Yahoo. These companies are in a bind. They can't do business in China except on terms dictated by the Chinese authorities, and that means zapping Web traffic that strays too far from the party line. But if they comply, they become, in the eyes of dissidents, collaborators with an oppressive regime. The Internet firms have been squirming this month. They've been poked by U.S. Representative Christopher Smith (Republican--New Jersey) and his Global Human Rights subcommittee, forced to publicly answer questions about their operations in China. The companies' oft repeated defense: We must comply with local laws; we think it's better for Chinese citizens to be getting filtered access to the Web than none at all; and we hope for more openness in the future.

One case troubling human rights activists is that of Shi Tao, a reporter for the *Dangdai Shang Bao* (*Contemporary Business News*) of Hunan, who forwarded, ultimately to foreign Web sites, his account of political directives to Chinese journalists forbidding the coverage of the fifteenth anniversary of the Tiananmen Square massacre. The Paris-headquartered free-speech advocate Reporters Without Borders, citing court records, says Yahoo's subsidiary fingered Shi by handing Chinese authorities the digital fingerprints of Shi's e-mail. The evidence led to the journalist's ten-year prison sentence last year.

Reporters Without Borders fumes on its Web site: "It is one thing to turn a blind eye to the Chinese government's abuses and it is quite another thing to collaborate." Don't try to access that site from a computer in Beijing. If you do, you'll just get a blank page.

On Dec. 31 Microsoft shut down Zhao Jing's popular blog, penned under the pseudonym Michael Anti. Zhao, who writes from Beijing, had fiercely criticized the firing of an editor at a progressive newspaper in Beijing. Microsoft says it had to shut down the blog based on the "explicit government notification" it received. "[The U.S. Internet companies] argue they have to follow local laws," says Corinna-Barbara Francis, China analyst for Amnesty International in London. "But when Microsoft took down the Michael Anti blog--what was the law they were following? Chinese laws protect freedom of expression and freedom of the press. And the Yahoo case hits home really hard. We have asked Yahoo whether they were presented with a court order; the company has not said that it was. So it seems Yahoo simply went along with a political request." Yahoo says it did have a legally binding request and only responded to what it was legally compelled to provide.

Google is under attack for allowing its Chinese site to be hijacked by the authorities. Type the Chinese characters for "Falun Gong" (prominent among China's many outlawed spiritual movements) into google.cn, search the "entire Web" and you get 626,000 hits of Communist Party propaganda about an "evil cult" that makes its believers go insane and commit suicide. A footnote at the page bottom, easily overlooked, tells Chinese surfers their search wasn't complete. Meanwhile, a Falun Gong search in Chinese characters on Google in the Free World comes up with 4 million links of all sorts, from supportive to hostile. Says Congressman Smith: "Many Chinese have suffered imprisonment and torture in the service of truth--and now Google is collaborating with their persecutors."

Censorship is quite an industry in China. Every village has spies to watch neighbors; the mail and the poster boards are

watched, say expat Chinese. Recently reporter Wu Xianghu died from a police beating after his newspaper exposed illegal bicycle fees collected by the police. It is said (by dissidents) that China has 40,000 Web police hard at work just in Beijing, looking over the shoulders of Web users and composing lists of banned words that cause a Web search to freeze up or a site to automatically be blocked. They have quite a challenge, not just because e-mail traffic in China is running at 300 million a day (based on China's own statistics), but because they are aiming at a moving target. They block not only "Tiananmen Square" but also chat-lingo substitutes like "Tsquare" and "June 4," the date of the incident. Block documents with repeated instances of "June 4" and you have a new problem: How does a law-abiding construction firm insist in e-mail that concrete forms have to be in place on June 4?

The censors have on their side not just industriousness but the long arm of a police state. Reporters Without Borders says that at least 50 Chinese citizens are behind bars for breaking the rules with their cyberdissent. The group counts another 32 print and broadcast journalists who have met the same fate. The dissidents, though, have a big thing in their favor, and that is the dispersed nature of the Internet. There are 800 million Internet users on the globe, and potentially any one of them can serve up offending documents. Something like 35 million Chinese live abroad, beyond the reach of the thought police. (*But they're not home free. See www.forbes.com/home_asia.)* They have news-thirsty friends and relatives back home.

The government can issue a decree to Google, and it will be obeyed. How does it go after Wikipedia? This is the lay encyclopedia, authored by anyone who wants to chip in. It's available in 100 languages, and its documents are on almost 100 servers spread across the globe. It has no income source in China to protect.

The English version of Wikipedia includes a 12-page illustrated article on the Tiananmen Square protests. Wikipedia is blocked in China--except to computer users who have downloaded proxy technology like Tor, a software program that gets them outside China by sending them to linked proxy servers, one encrypted hop at a time. States the Wikipedia Web site: "Many sysops and other users from mainland China have remained very active on Wikipedia using these means."

By throwing up their hands at trying to sort the innocuous Wikipedia info from the political and choosing to block the site in toto, the censors have created new enemies--the citizens who used the encyclopedia for academic work. In a short time, say China-watchers, the government has made millions of ordinary citizens into document smugglers.

Remarkable what a little suppression can do to turn a small disgruntled group into a large, angry mob. Consider the history of the religious movement Falun Gong. Unexceptional on its face, Falun Gong looks to outsiders like a cross between tai chi and Buddhism. But about seven years ago the Chinese authorities decided that, with 70 million adherents, it had become a threat to their rule. The police began a campaign to imprison and torture the practitioners. It made the believers into martyrs.

Now Falun Gong is the focal point for a whole dissident movement. The practice is, appropriately, a postmodern religion that operates in the digital world: It has never had significant church real estate nor run formal fundraising activities but is driven entirely by volunteers organized over the Internet. Now expatriate members are all over the world, bombarding their homeland with e-mails, chat rooms, phone calls and faxes. Many but not all of these messages randomly list multiple proxy Web sites that can be used to slip through the Golden Shield to access news and information from the Free World. These ever-changing proxy addresses rain down on China so quickly that the Internet police can't blacklist them quickly enough. Some proxy addresses last only minutes before they are obsolete, others several days. Some use encryption (of the sort used to protect charge card numbers) to thwart the censors. "The amount of information going into China is staggering," says Alan Adler, a Tenafly, New Jersey businessman who raises money for this hacking effort through a nonprofit outfit called Friends of Falun Gong.

UltraReach Internet Corp. and Dynamic Internet Technology are just two commercial American companies moving information back and forth through China's Golden Shield for Falun Gong and other news, human rights and U.S. government organizations. UltraReach is press shy, but monthly traffic statistics we've seen suggest its proxy Web sites averaged 2 million visits and 460 million hits a month in 2005.

Dynamic Internet Technology of North Carolina got its start with a pilot project for the U.S. government in 2002 and today discreetly claims on its site that it offers customized, low-cost and reliable Internet solutions "under challenging circumstances." Voice of America and the New York-headquartered Human Rights in China are also DIT customers. William Xia, DIT's chief executive, claims "hundreds of thousands of regulars" use its services daily. But DIT and UltraReach are just the tip of the Falun Gong's hacking efforts. "We never put all our eggs in one basket," says hacktivist Chen. "We work from multiple places, use many different systems and technologies, and we back each other up in many different ways. We've learned this the hard way."

The task should become easier as more censorship-evading technologies come online. Psiphon, for example, is a product developed by the Citizen Lab at the University of Toronto that creates a "closed" proxy system among, say, trustworthy family members both in and out of China. Tor, meanwhile, created by tech pundit Roger Dingledine, "is a network of virtual tunnels" numbering undetected through the Internet. Its early development was funded by both the U.S. Navy and the Electronic Frontier Foundation. In the last 11 days of January, says Dingledine, a quarter of a million copies of the Chinese-language version of Tor were downloaded from the Tor Web site. "The idea is similar to using a twisty, hard-to-follow route in order to

throw off somebody who is tailing you--and then periodically erasing your footprints.”

The mobile phone is another way of getting information in and out of China. China's highest profile human rights lawyer at the moment is Gao Zhisheng, and one night in mid-January, he says, a car with brown paper covering its license plate tried to run him down--while the military police were watching. In the scrape the paper fell off the car's license. Gao survived and immediately wrote everything down in a text message, including the license plate number, and sent the text to another lawyer in Beijing, pleading, "Please help to send this message to the Internet." The text message went around the world.

Julien Pain, running the Internet Freedom desk at Reporters Without Borders in Paris, says Chinese families effectively used their mobile phones and text messages to spread the word about SARS. The censors have responded with cell phone filters. But how many eavesdroppers does it take to keep tabs on 390 million cell phone users? Unless the government is prepared to shut down the mobile phone industry, it will have to contend with rumors, news and whispered plans for tomorrow's street demonstration.

The Falun Gong have under way a multimedia campaign to distribute *Nine Commentaries on the Communist Party*, a scathing series of "exposés" about the Chinese Communist Party. DIT says it passed 2 million "scrambled" (mild encryption) electronic copies through the Golden Shield; sometimes DIT hides heavily encrypted material in a river of seemingly legitimate encrypted commercial data entering China. The book was promoted with 100 million e-mails, 12 million snail mails, 10 million faxes and some 50 million phone calls. During the last 14 months, claims Falun Gong, the *Nine Commentaries* campaign has inspired 7 million disenchanting members to renounce the party. That sounds exaggerated, but Dynamic Internet Technology's digital logs display party renunciations arriving at DIT's proxy Web sites at the rate of over 30,000 a month. Heilongjiang, a remote province bordering Russia, suddenly has become a hotbed of hacking refuseniks. Why? Last November an explosion at a chemicals factory--followed by a classic Chinese cover-up--resulted in a toxic spill that poisoned the Songhua River and left millions of the province's citizens without water.

Could the party's hold on China indeed be imperiled--not years down the road, after the kind of gradual transition to capitalist democracy that many outsiders hopefully expect, but by a precipitous upheaval of the sort that demolished the Soviet bloc? Not likely--but it could happen.

"The bloggers in China are really angry," says Amnesty International's Francis. "Virulent. Let's say, hypothetically, the Chinese government was out of power in five years--these people will remember that Microsoft took [the blogger Zhao] down."

What are Google's and Microsoft's and Yahoo's strategies? Beset on one side by a mob of freethinking, pro-democracy bloggers who denounce them and on the other by the totalitarian government censoring them, the companies issue only guarded statements about the Internet war. So we don't know exactly what Google's Eric Schmidt, Microsoft's Bill Gates and Yahoo's Terry S. Semel are thinking. But it could be something close to this: that the censorship is not just asinine but doomed to failure; that Western companies can make a show of cooperating with the authorities while leaving in place plenty of loopholes for the dissidents to exploit; and that the complete collapse of the censorship regime can't come soon enough.

Sidebars

[Hardline Hardware](#)

[Controlling Leaks](#)

[You Don't Say](#)

[Standing Up](#)

-