WIRED

WIRED MAGAZINE: ISSUE 15.11

The Great Firewall: China's Misguided — and Futile — Attempt to Control What Happens Online

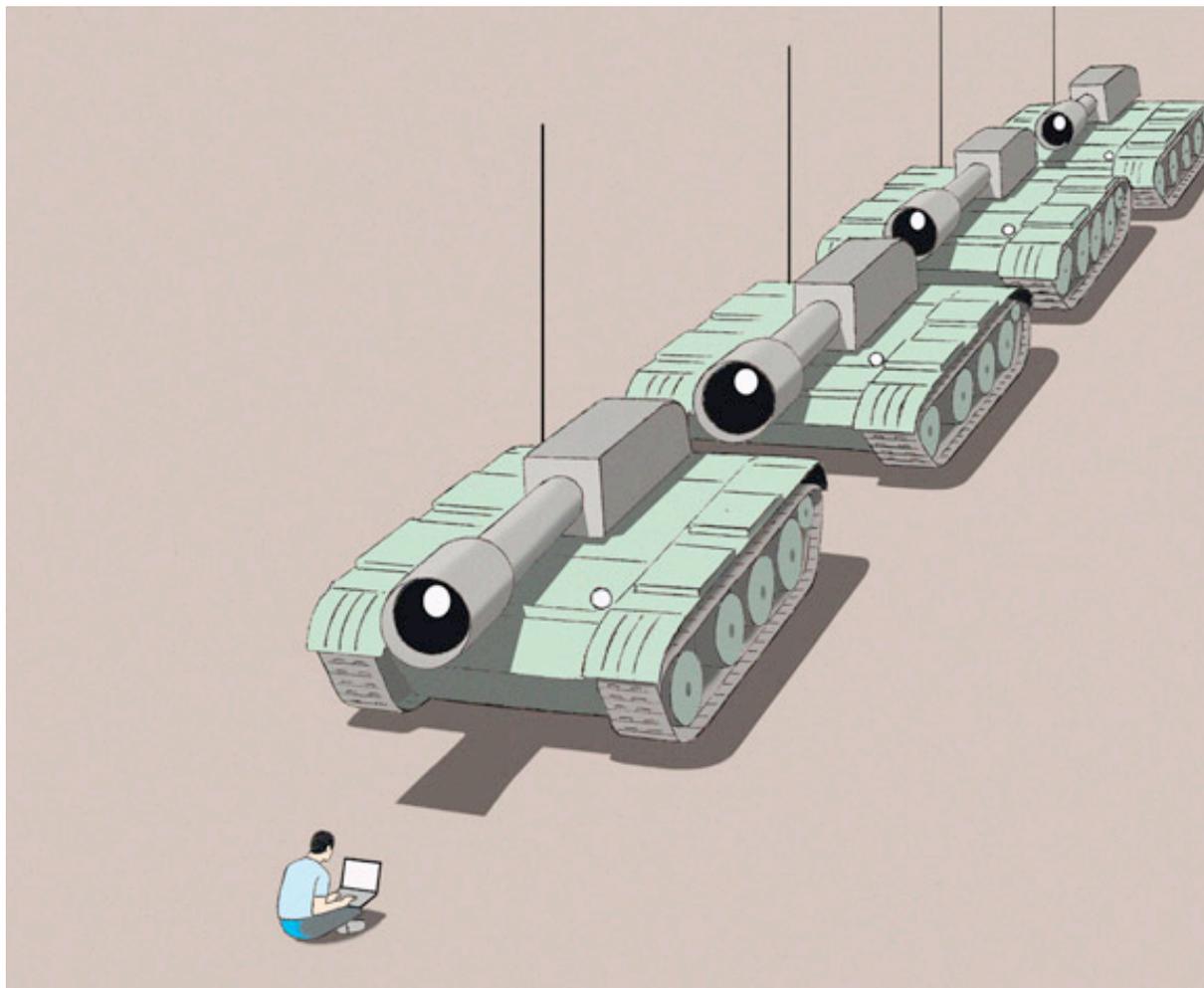By Oliver August   10.23.07 | 12:00 AM

Illustration: Guy Billout

I didn't know I was a surveillance target until the day I walked into a hotel in China's Fujian province. I was pushing past half a dozen workmen changing lightbulbs in the glum but busy lobby when a uniformed man stepped in front of me. Blue jacket, creased trousers, braided epaulets, peaked cap: government security officer. Politely, he asked

whether I would mind answering a few questions. He stood erect, with the manicured swagger of a corporate CEO. Next to him, a gangly plainclothes colleague gave me a so-you-thought-we-wouldn't-catch-you look.

How had they known I would be here? The only people who had my itinerary were my editors in London. A few days earlier, I had sent them an email outlining my trip, and I'd been updating them daily by phone. I could only assume that the authorities had been monitoring my email and calls. I had been chasing down leads on the whereabouts of Lai Changxing, China's most-wanted man. Lai had cheated the government out of $3.6 billion by smuggling oil, cars, and cigarettes. Embarrassed, Beijing wanted to hinder any reporting of his case.

How to Breach the Great Firewall of China

Go in disguise
Use proxy servers and other software that can mask your location and identity. Among the most popular apps are Psiphon, Freegate, TOR, and UltraSurf.

Scramble messages
Use encryption for email. Top software tools include Hushmail and Cryptomail, which take advantage of so-called pretty good privacy — PGP — encryption.

Post on the down low
Avoid online discussion groups for obviously controversial subjects. Post sensitive messages in lifestyle or sports Web sites, which are rarely monitored.

Search overseas
Try the international version of a Web site rather than the China-based one. Google's US-based search engine (in Chinese) isn't blocked, for example.

Watch your language
Avoid controversial terms (e.g., "democracy," "Dalai Lama"), or at least don't put them in the title of your blog post. Body text is much less likely to be monitored.

Log On to Skype
The P2P freeware uses 256-bit encryption for phone calls, staying below government radar. Use the international version (not the Chinese one) to avoid spyware.

The two officers in the hotel demanded to see my passport and asked what I knew about Lai. Then they withdrew to a corner of the lobby to confer. Eventually, they took me to a police car, drove me to the airport, and put me on a plane to Beijing.

It was, in short, impressive evidence of the government's ability to monitor and control electronic communication. And my experience only hinted at the Chinese government's

appetite for control. Beijing has recently added a new weapon to its arsenal of surveillance technologies, a system it believes to be a modern marvel: the Golden Shield. It took eight years and $700 million to build, and its mission is to "purify" the Internet — an apparently urgent task. "Whether we can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state," President Hu Jintao said in January.

The Golden Shield — the latest addition to what is widely referred to as the Great Firewall of China — was supposed to monitor, filter, and block sensitive online content. But only a year after completion, it already looks doomed to fail. True, surveillance remains widespread, and outspoken dissidents are punished harshly. But my experience as a correspondent in China for seven years suggests that the country's stranglehold on the communications of its citizens is slipping: Bloggers and other Web sources are rapidly supplanting Communist-controlled news outlets. Cyberprotests have managed to bring about an important constitutional change. And ordinary Chinese citizens can circumvent the Great Firewall and evade other forms of police observation with surprising ease. If they know how.

Like its namesake, the Great Firewall consists of hundreds of individual fortifications spread out along a vulnerable frontier. At its core is a giant bank of computers and servers. Traffic generated by China's 162 million Internet users is routed through the shield, which checks all requested URLs against a blacklist of tens of thousands of Internet addresses. The list includes pages offering political information deemed dangerous by the government, like BBC News and Voice of America. Access to these sites is blocked (at least in theory), and when users attempt to view one of them, they are punished with an involuntary time-out lasting anywhere from 30 seconds to 30 minutes. Search engines are similarly restricted. If you enter the characters for "democracy" or "Tiananmen Square massacre" into Google.cn you will generally get zero results. This is a technological breakthrough for the Chinese government. Until recently, it could not interfere with the inner workings of search engines and instead blocked entire sites, not just individual pages of a site.

The Golden Shield hardware — supplied by Cisco and other US companies — is supplemented by human censors who are paid about $170 a month. They sit at screens in warehouse-like buildings run by the Public Security Bureau. These foot soldiers in China's information war monitor domestic news sites, erasing and editing politically sensitive stories. Some sites provide the censors with access so the authorities can alter content directly. Others get an email or a call when changes are required. Similar methods are applied to blogs. Sensitive entries are erased, and in the most egregious cases blogs are shut down altogether.

The censors also monitor email traffic, looking for politically sensitive content like calls for protest marches and anti-government tracts. Because it would be impossible to screen millions of Internet users, they home in on watchlists of potentially suspicious emailers — known dissidents, suspicious foreigners — and notify investigators of possible violations.

Information spied online is collected in counties and major cities and matched up with other surveillance data. In my case, the effectiveness of this technique was obvious. Police minders always seemed to know where I was traveling and when I was back in Beijing. Sometimes they'd call as soon as I landed at the airport, telling me I had yet again broken the rules by traveling without permission or conducting interviews without authorization.

Evading them, however, was surprisingly easy. I bought additional phone numbers, a tactic I picked up from Lai. I also learned dozens of tricks to avoid arousing suspicion online. But the cat-and-mouse game was unrelenting. A year before my book on Lai was published, I told an official about it. Maybe I mixed up my tenses, mistakenly suggesting I had already finished it. "Yes," the official said. "I enjoyed the book." I was too stunned to ask how he might have got his hands on the still-incomplete manuscript. But then, I didn't really have to: When I had arrived at my office in Beijing one morning some eight weeks earlier, I had found the cables on my computer changed around. The modem wire was rolled up in a coil, the power cable unplugged, and the printer attached to the wrong port. It appeared someone had been poking around my hard drive. When I lifted up the computer to fix the mess, I found a piece of paper. On it was my office address, written in an unfamiliar scrawl.
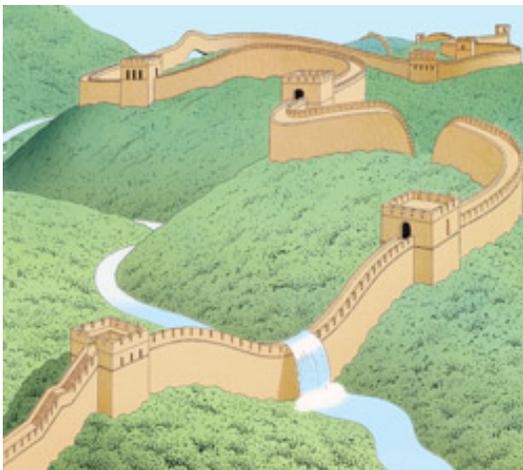

Illustration: Guy Billout

For all its ambition, the gears of the giant surveillance machine keep getting fouled with sand. On one side of the Great Firewall, a small industry is sprouting up, dedicated to evading blocks and monitors. Libertarian software engineers, enterprising students, banned religious groups, and regular for-profit companies compete with one another to

launch new downloadable tools that outfox the censors. They exploit proxy servers, deploy encryption technology, and ferret out holes in the wall. I have spent many afternoons in the Internet cafés of Beijing's Haidian University district, learning from the students who live in this world. For a dollar an hour, they will help anyone hack the system: set up secure SSH and VPN connections, use a circumvention tool called UltraSurf developed by the banned Falun Gong group, access unregulated Chinese peer-to-peer networks. Their techniques confirm John Gilmore's adage: "The Net interprets censorship as damage and routes around it."

From these students I learned that censorship is not only easy to subvert, but sometimes it subverts itself. Each week, for example, Beijing's propaganda department updates a list of banned stories. Available to senior journalists at government-controlled news outlets, the list includes scandals, protests, and sackings across the country. Newspapers are not allowed to report on them, but some journalists post the lists online, telling you all you need to know.

The system is self-defeating in other ways as well: Twelve national government bodies share responsibility for the Internet, and all of them have separate political and commercial interests. In some cases, departmental budgets are financed through revenue from online businesses, so it's often in their interests to loosen restrictions. Furthermore, the Great Firewall is besieged by bureaucratic infighting and incompetence that results in exceptions and loopholes.

One day, I received an official summons from the Public Security Bureau, asking me to present myself at the national headquarters. When I turned up, I saw hundreds of bikes covered in dust, as if their riders had gone into the building and never come out.

I was met by two uniformed officers who led me to a windowless room. They came straight to the point: Had I been in touch with Wang Dan, an exiled dissident living in Boston? Yes, I said. I had exchanged emails with him — but had not yet published a story (so how did they know?). Was I aware, they continued, of the rule requiring foreign journalists to ask for official permission to interview Chinese citizens? "Yes," I said. Then the conversation took an unexpected turn. "There is a problem," I told the officers. "Wang Dan has become an American citizen." The officers were silent. "In the future," I said, "which government department should I ask for permission to email and interview him?" Confused and sheepish, they let me leave, and I found myself back by the dusty bikes. So these were the bureaucrats guarding the mighty Great Firewall? Even police departments working in the same building were not talking to each other. Otherwise they would have known that Wang Dan was in fact still carrying a Chinese passport, as I later found out.

Government attempts to suppress coverage of another persona non grata, Lai

Changxing, were equally futile. Although excised from the official state media, Lai was well-covered by dozens of Web sites. Hunted by the government, he was cheered on anonymously online. Bloggers compared him to the characters in *All Men Are Brothers*, a 12th-century book of tales about outlaws who outwit greedy, abusive officials. "Lai is like an ancient bandit," I read on a discussion board. "He only takes from the rich."

After almost two years underground, Lai eventually sought asylum in Canada. Again, independent Web sites carried the news. "Lai has a million-dollar home in Vancouver," was the headline on one site. At this point, newspapers gave up their silence and began to report on the Lai case, too. New media was drawing away millions of readers, so newspaper owners lobbied censors and officials to give them more leeway to defend their commercial interests.

As Chinese citizens become aware that their most potent advantage over censorship is their sheer numbers, more and more grievances are aired online — sometimes with significant consequences. The first cyber-rebellion to have a major political impact took place in 2003. Sun Zhigang, a young migrant worker in Guangzhou, died in police detention after failing to produce identity documents during a street check. Sun's friends protested his death on discussion boards, and soon other sites picked up a campaign demanding police accountability and reform of the laws affecting migrant workers. Before the unprepared system monitors could react, an avalanche was in motion. Tens of thousands of Chinese became involved in a national conversation, despite the risk of punishment. Emboldened, the mainstream media jumped in and reported the Sun case. The government opted not to crack down on these violations, rightly sensing that doing so would have been more politically costly then letting the debate run its course. A few months later, Prime Minister Wen Jiabao abolished the law requiring China's 120 million migrants to have special identity papers. (Singapore, with just 2.4 million regular Internet users and very deep pockets, might have a chance at quelling Internet-fueled popular revolts. But China comprises a fifth of humanity. Any attempt to impose iron-fisted control over a network this big seems certain to trigger economic paralysis.)

Since the Sun case, dissent has regularly roiled the Internet in China. Last year, 13 retired senior officials, including Chairman Mao's former secretary, protested a decision to close down a liberal weekly. In a joint letter published online, they wrote that the government suffered from the "delusion that it can keep the public locked in ignorance." The weekly was reopened.

This year, the pace of protests has increased. In March, the government provoked an outcry online by banning eight controversial books. Their authors published petitions — widely emailed and blogged — criticizing Long Xinmin, the chief censor. Within a few

weeks their books were returned to shop shelves, an unprecedented move. Long defended the necessity of censorship, saying, "Advanced network technologies such as blogging and webcasting have been mounting new challenges to the government's ability to supervise the Internet." A month later, Long was fired. Hu Fayun, one of the eight temporarily banned authors, told *The Times of London*: "The traditional no-talk' style of control by the government has been broken by the Internet. Different voices can be found there."

Why can't the government block coverage of Lai and other sensitive subjects? Besides the seemingly insurmountable technical challenges, one important answer is this: online business. Rigorously policing encryption technology would undermine ecommerce, which is vitally important to the government's crusade to lift the economy. If all encrypted credit card details and other sensitive corporate information had to pass through surveillance bottlenecks, whole sections of the economy would be harmed. When forced to choose, the government seems to trust that raising incomes is a better way of securing power than spying on dissidents.

Of course, China is hardly a Jeffersonian paradise. Thousands languish in prison because of harmless online activities. A recent example is Zhang Jianhong — blogging as Li Hong — who was sentenced to six years for posting political essays. Cases like his justify strong criticism of China. But they don't prove that its monitoring system is successful on a national scale. Furthermore, the government is increasingly relying on physical rather than electronic surveillance. Internet cafs are now required to write down the ID numbers of all users so police can track them down no matter how clever their online disguises. But again, there are physical limits. Police cannot chase after millions of Internet caf&233; visitors.

Today, anyone in China can send a sensitive message if they are minimally savvy, and that fact is transforming the political discourse. True, technology has not led to the overthrow of the Communist Party, as some had predicted — the party has even harnessed the Internet for its own purposes. But this does not mean that Beijing has insulated itself against political change driven by technology. Its critics have unfettered access to mass communications, and the Internet — not the Communist Party — is the main influence on public opinion. No shield, golden or otherwise, can protect them from the public. China's leaders should know this. Their predecessors built the Great Wall of China to keep out Mongol invaders. It proved as useful as every other fixed fortification in history, and the Mongols still invaded Beijing and overthrew the political elite.

Oliver August (www.oliveraugust.com) *is the author of* Inside the Red Mansion: On the Trail of China's Most Wanted Man.