

1 Jun 2005 | 4:00 GMT

The Net Effect

As China's internet gets a much needed make-over, will the new network promote freedom or curtail it?

By **Steven Cherry**



Photo: Fritz Hoffmann/DocumentChina

Café Society: Young Shanghai professionals surf the Net and complete their work at the Cha Tea café, in the city's Xujiahui commercial area.

China's open-market reforms, begun a quarter-century ago, launched an unprecedented social experiment. Never in modern history has there been a truly enduring technological and economic world power that wasn't a democracy—a free economy without free speech.

For the experiment's first 15 years, the Chinese government had no trouble keeping a firm grip on the reins of the news media. Then came the Internet. Could the government open the floodgates to the waves of information washing up on every shore yet keep out the ideas it was afraid of, such as ones about sexuality, democracy, religious expression, and Taiwanese independence?

So far, the answer has been yes. China's Internet is the most efficiently censored in the world. From a computer in China, try to visit the Web site of the banned activist organization Human Rights in China, based in New York City, and your request will be blocked by filters in the network.

Instead of the group's home page, you'll get an innocuous error message such as "File not found." Hundreds, maybe thousands, of sites are similarly blacklisted. The exact number can't be determined and changes daily.

Now China's experiment in cyberspace censorship is about to take a dramatic turn. A massive upgrade to the country's Internet will soon give China a robust, state-of-the-art infrastructure easily on a par with any in the developed world. China Telecom Corp., in Beijing, is investing US \$100 million in what it calls the ChinaNet Next Carrying Network, or CN2.

The former national telephone monopoly is snapping up new network routers from four of the largest telecommunications equipment companies in the world: Cisco Systems and Juniper Networks of the United States; the French giant Alcatel; and Huawei Technologies, the only Chinese company to get a CN2 contract. During the next 12 months, the routers—the vertebrae of an Internet backbone—are to be installed in 200 cities throughout China's 31 provinces, autonomous regions, and municipalities.

Few doubt that China will emerge as a 21st-century global power. The questions now are about when it will emerge and what kind of power it will be. The issue of how China continues to censor its Internet, even as its infrastructure becomes vastly more sophisticated, has implications beyond what ideas China's populace—almost one-fifth of humanity—will be allowed to tap into. For one thing, if censorship technology flourishes in China, it will be easier and cheaper for it to also take root elsewhere. "The concern I have is that this is laying the foundation for a much more intrusive and censorship-friendly Internet infrastructure for all countries," says Roger Clarke, a consultant in Canberra, Australia, affiliated with the Australian National University. "The features that China wants installed in intermediating devices and software will gradually find their way into all of the suppliers' products, if only because it's cheaper that way."

Whether China's Internet censorship continues at the same level or—with its powerful new equipment—increases will probably play a significant role in answering the "What kind of global power?" question. Experts say that up to now, there have been technological constraints on the amount of censorship possible at the router level. In the network now taking shape in China, those constraints will be largely eliminated, making censorship more a matter of politics than of technology. Given the choice, will China move toward the openness of, say, South Korea? Or will it become something not yet seen in the postindustrial age: a closed capitalist colossus? No one now can say.

China's telecom and Internet infrastructure already is so mammoth, the authorities must wonder if they can really control it. China Telecom is the largest phone company in the world, with about 190 million users. Its ChinaNet subsidiary is the country's biggest Internet service provider. Almost 100 million Chinese are online, and analysts predict the number will triple by 2008.

All that traffic has outpaced capacity, so China's Internet is now a bottleneck to the country's massive push toward greater industrialization. Without state-of-the-art phone and Internet networks, the myriad routine exchanges that keep a technology-based economy humming start to break down. Bank fund transfers are slower and less reliable, videoconferences falter, and e-mail gets lost. Supply chains become weaker for importers such as Wal-Mart Inc., in Bentonville, Ark., which bought \$18 billion worth of goods last year from thousands of Chinese suppliers, and for exporters such as the Haier Group, in Qingdao, which sells its refrigerators and other appliances in 160 countries.

But the Internet in China, as it is everywhere, is more than a development tool. It's also the main medium for political speech, organizing, and social networking.

"It's a dilemma for the Chinese leaders," notes Xiao Qiang, who left China after the 1989 Tiananmen Square pro-democracy uprising and now directs the Berkeley China Internet Project at the University of California at Berkeley's graduate school of journalism. "On the one hand," Xiao says, "they need a competitive economic development environment, and you cannot do that without the latest communications technologies—they are indispensable for a globally competitive economy. On the other hand, there's the explosive nature of communications technologies, which cause much greater freedom of expression."

Today, a vast, sophisticated, and multifaceted program of control has evolved to monitor China's Internet. It blocks access to banned sites and uses a long and continually updated collection of keyword filters that prevent Chinese citizens from viewing sites deemed pornographic or subversive. In addition, Internet service providers and Internet cafes [see photos, "[Cafe Society \(/images/jun05/images/net.cafesociety.jpg\)](#)" and "[China Online \(/images/jun05/images/net.chinaonline.jpg\)](#)"]. are subject to numerous state regulations. Tens of thousands of dedicated "Internet Police" reportedly do nothing but enforce those regulations, a special police force that has no parallel elsewhere in the world.

Yet, in the shadowy struggle that Internet censorship has become, the censors' first line of defense will surely be the routers and other machines that filter what Chinese users can see online. As the flow of data coursing through China's Internet becomes as wide as the Yangtze River, the government will need to raise its barriers to free speech to the height of the Three Gorges Dam.

Understanding How Internet censorship works in China—and how long it can go on—requires some background on the country's networks and plans. China Telecom's current network dates back to 1994, which doesn't sound so long ago. But it has been a busy 11 years—think Netscape and Napster, eBay and Amazon, Yahoo and Google. Today, with fiber-optic cable snaking through the Chinese countryside, torrentially firing data at those routers and servers, the machines are being overloaded [see [Wiring Small-Town China \(0605ctow.html\)](#) in this issue].

In addition, China's decade-old Internet infrastructure wasn't designed to stream data for fast-growing applications such as Internet telephony (voice over IP), video on demand, and Web-based radio. Those applications are far more sensitive to network congestion than are e-mail and static Web pages. You don't really care if a Web page takes 5 seconds to paint across your monitor screen. But even 1-second gaps in a telephone conversation or video feed are annoying, especially if they happen repeatedly.

China Telecom's CN2 project is designed to solve such problems. For example, CN2 will introduce a feature known as multiprotocol label switching, which tags time-sensitive packets of data that are part of a streaming video clip or voice-over-IP call. The tags let the routers know that those packets should get a higher priority than the ones that make up e-mail or a static Web page. It is also incorporating the next-generation Internet protocol, IPv6, which adds security features helpful to e-commerce.

The groundwork for CN2 was laid in mid-2004, when China Telecom's Research Institute, in Beijing, took bids from many of the world's largest telecommunications equipment suppliers. Juniper Networks, Cisco, and other firms offered up their burliest machines: mainframe-class routers, costing around \$100 000 each and capable of moving a trillion bits of data per second.

In the vast postal system that is the Internet, routers are the post offices, directing streams of data that have been grouped into packets. The packets flow into a router and are then hurtled out to others closer to their eventual destination. It's a firemen's bucket brigade, with bytes instead of water. Generally, bigger and faster is better in the router world, not least because the tens, hundreds, or thousands of data packets that make up an e-mail message or Web page might be forwarded a dozen times or more from router to router before finally—milliseconds later—showing up half a world away.

Up to now, Cisco, which first came to China in 1994, has dominated the router market there, with as much as a 70 percent share in 2003. For CN2, though, China Telecom awarded [six contracts, splitting them up among Alcatel, Cisco, Huawei, and Juniper \(/computing/networks/the-net-effect/six-contracts-four-companies\)](#).

The roles the four companies will play in CN2 can be understood only in terms of the distinctive structure of China's Internet. It is highly centralized, with three layers, which can be thought of as concentric rings. The innermost ring consists of core routers, to be built by Juniper (a surprise choice for this key contract, given its late entry into the Chinese market). They are expected to be as sophisticated as any in the world. The core routers—being installed in eight large, strategically located cities, including Beijing, Shanghai, and Chengdu—are the principal means by which data packets will cross from one region to another or make their way to the outside world.

The outermost of the three rings consists of routers located throughout China. CN2 awarded Cisco a nationwide contract for these devices, called edge routers, which businesses and institutions will use to make their high-speed connections to one another and to the world. If the core routers are the interchanges of the autobahns of China's Internet, the edge routers are the intersections to its local streets.

The middle ring consists of metropolitan-area networks—the network's state and county roads. CN2 will upgrade routers in at least 193 of the nation's largest cities, dividing China's provinces, autonomous regions, and municipalities into four regions and giving each of the four vendors its own territory. Thus, CN2 gave Juniper and Cisco two contracts each, nationwide ones for core and edge routers, respectively, plus regional contracts. Alcatel and Huawei each got only regional contracts [see map,].

Although in most countries Internet traffic ends up flowing through a relatively small number of routers, China's network is centralized by design instead of by economic evolution. Moreover, in China, almost uniquely, most traffic—including all its international traffic—is effectively under state control. Data sent by a restaurant in a remote village that is buying pigs from a farm two towns over might not travel through the metropolitan network. But most data, whether it's a request for a Web page in Australia or an e-mail message to a colleague 500 kilometers away, would go through one or more metropolitan networks, be pushed through a core router, and go from there across the country or to the outside world.

How will censorship work with four different companies' products? According to Seth Finkelstein, a Cambridge, Mass., network programmer and an expert on Internet censorship, router-based censorship can and does take place at any point in the network. Each of the routers in the CN2 contract—in all three rings—can be expected to access a database of banned names and words, either within the router itself or in a subsidiary server connected to the router.

Those subsidiary computers—known as proxy servers—can be ordinary PCs, and they're not just in China; they're everywhere today. Corporations use them to keep employees from shopping online or playing games during working hours. Internet companies like AOL use them to create "family friendly" spaces online, free of pornography. Libraries in many countries, including the United States, are required to use similar blocking lists to keep pornography away from underage viewers.

China's mechanisms of censorship have been widely scrutinized, most notably in a 2002 study by the Berkman Center for Internet and Society at Harvard Law School, in Cambridge, Mass. "The primary and most longstanding means of blocking is at the router level," says Derek Bambauer, a resident fellow at the center, who participated in an April 2005 follow-up study as part of a project called the OpenNet Initiative.

Since 1998, at least, Cisco has been developing and selling equipment that was designed to help China Telecom comply with government censorship, claims journalist Ethan Gutmann, author of the 2004 book *Losing the New China: A Story of American Commerce, Desire, and Betrayal*. In an interview, Gutmann reiterated a charge documented in his book that China "could not have controlled this radical new means of communication without overwhelming technical assistance from North American corporations." In his book he quotes, among other sources, unnamed Cisco representatives and a non-Cisco Internet engineer, identified only as Wen, who all claim that Cisco modified its equipment and software at the censors' bidding.

A Cisco spokesman responded that the company rejects Gutmann's assertions. "He has never produced one shred of evidence to support his claims," the spokesman insisted. Elsewhere, too, Cisco has flatly denied any complicity in Chinese censorship. In response to a challenge by an activist shareholder two years ago, Cisco declared that the products it sells in China "do not contain any detection or monitoring capabilities which are different from the products the company sells to anyone anywhere else in the world." And, indeed, today most routers are designed to work with proxy servers without further modification.

In the early days of China's Internet, the mid-1990s, the routers had to shoulder the entire censorship burden. The censorship was, unsurprisingly, simpler than it is these days and more heavy-handed, with the routers doing nothing more than blocking IP addresses. An IP address is a string of numbers separated by decimal points, such as 192.168.141.24. It is the main identifier used for personal computers, routers, and all other nodes on the Internet. Domain names, such as [ieee.org](http://www.ieee.org), are translated into the appropriate IP addresses by a parallel network of servers, called domain-name servers, within the Internet.

Because routers recognize only numerical IP addresses, blocking a domain, such as [xamax.com.au](http://www.xamax.com.au), or a specific Web address (URL), such as www.xamax.com.au/CV/RC.html (www.xamax.com.au/CV/RC.html), at the router requires a separate entity—a proxy server. (Domain name and URL filtering can be done within the device that does the routing, but network designers usually assign that task to a separate process. The proxy server can reside within the device or be an external computer attached to it.) In a network's design, the proxy server resides between the Web surfer's PC and the targeted server. A typical purpose is caching: it stores frequently requested Web pages so that when, for example, millions of people want to view the latest Olympics results, the relevant Internet server isn't overwhelmed.

But because their basic function is to intercept requests, proxy servers are also routinely used to block access, an application known in this context as filtering. Here, the proxy server intercepts requests to a domain-name server, finds the domain name that's being sought, and checks it against a table of forbidden URLs or domains. If the requested address is on the list, the proxy then "tells a lie," says the Australian National University's Clarke. "It returns an IP address which is willfully incorrect." When the request is forwarded to that—incorrect—IP address, the server responds—correctly—that the requested page isn't available there.

No one outside of the involved officials themselves knows for sure if that is how Internet censorship is done in China, but outside experts have little doubt. "It's the most likely technique," Clarke says, adding, "I've had some students assess whether it is a breach of international law. It is, of course, a rather hazy issue."

Today, there's a cat-and-mouse game between the authorities and publishers of Web pages deemed offensive. After having its Web pages added to the forbidden list, a publisher has two options: put the content on a new server with a new IP address or leave it where it is and acquire a replacement IP address. Either way, surfers eventually find the new IP address. So, however, do the authorities, who then add the new address to the forbidden list.

The game took a twist in the late 1990s, when the government erected what has come to be called the Great Firewall of China. It introduced a whole new form of censorship by using proxy servers to inspect URLs themselves for words that indicate banned topics, such as "falun" in <http://www.faluninfo.net> (<http://www.faluninfo.net>). The URL request passes through the first of many routers on its way to the Web server, www.faluninfo.net. It's a simple matter for the router to also pass the URL through the proxy, which looks for the banned string of letters. Once it finds it, the proxy gets in touch with a Web server that has been set up to mimic the servers containing banned content. The masquerading Web server then sends an innocuous error message—"File not found" or "Service unavailable"—back to the surfer who requested the banned page.

That's not all. The proxy server also might note the IP address of the computer that requested the forbidden page and suspend all transactions from that machine for a while.

Zhao Ziyang's death in January was ignored by newspapers and television but not on the net

Here the game gets downright Byzantine. To shield themselves from identification, surfers sometimes take countermeasures. Their tool of choice is none other than another kind of proxy server! Suppose someone has helpfully placed one of these anonymizing proxies on the Web and left it open for anyone to use. Recall that a proxy can sit between the surfer and the Web server that has the pages the surfer wants.

The anonymizing proxy lets the user enter a desired URL, such as <http://www.hrichina.org> (<http://www.hrichina.org>), as a field in a Web form, which the censoring proxy server can't see—it only sees the user innocuously interacting with the anonymizing proxy. That is, the censoring proxy sees URLs that look like this: <https://www.proxyweb.net/> (<https://www.proxyweb.net/>). The actual page request to www.hrichina.org comes from the anonymizing proxy, proxyweb.net, which is typically located outside of China and is therefore beyond the reach of Chinese censorship. (Proxyweb.net is a service of Aaex Corp., Nassau, Bahamas.) So the user gets to see the Web page, in this case www.hrichina.org's home page, after all. It shows up as a frame on a page provided by the anonymizing proxy, in this case <https://www.proxyweb.net/antilog.php> (<https://www.proxyweb.net/antilog.php>).

The OpenNet Initiative investigators don't believe that router-based filters are looking deeply within packets of data for banned keywords. "There are no technical problems with doing that," says researcher Bambauer. "But it would place an enormous load on the routers." So the CN2 upgrade to the router infrastructure might enable the authorities to employ even more keyword filtering than is done now.

Sites that deal with banned topics but avoid banned keywords in their domain names generally don't fool China's censors for long, thanks to the Internet police. When they find such sites, they put the addresses on the blocking lists.

The Internet police force, established just five years ago, has between 30 000 and 50 000 officers, says Xiao, of the Berkeley China Internet Project. "According to government publications, it operates in 700 cities," he adds. "Every police department has a division called Internet Police, just like it has traffic or fire police. The Internet police investigate Internet crimes, such as viruses, and online matters concerning financial security, pornography, and politically sensitive materials."

Blocked political sites are generally inaccessible for months, not minutes. That was the experience of Yan Sham-Shackleton, a resident of Hong Kong who goes by the Internet nom de guerre Glutter Girl and writes a blog about China's underground democracy movement [see photo,]. (Hong Kong is located just outside the virtual gates of the Great Firewall.) On her birthday last year, she wrote, "My 30th Birthday Wish: Democracy in China." That entry got her blog, at <http://www.glutter.org> (<http://www.glutter.org>), banned in China for several months. As a protest, she altered its design, putting white text on a black background. In sympathy, a hundred or so sites around the world also reversed their layouts and "went black," an action that in turn was noticed on the discussion site Slashdot. Sham-Shackleton says Slashdot itself—one of the most popular locales on the Internet—was unviewable for a time within China.

As of mid-April, the Glutter Girl blog was filled with photographs memorializing former premier Zhao Ziyang, a hero to students and intellectuals for having opposed the violent 1989 crackdown at Tiananmen Square. His death in January was deliberately ignored by Chinese newspapers and television but generated a lot of traffic on the Net. "There were thousands and thousands of messages on Chinese bulletin boards," Sham-Shackleton says. But they had to be surreptitious, avoiding any direct mention of Zhao. "A typical one was, 'My friend died last night, I really miss him.'"

Chinese authorities don't rely just on the technological controls of the Great Firewall. They also require all Internet businesses, including Internet service providers and cybercafes, to obtain operating licenses. In the first of a number of periodic crackdowns, more than 17 000 cafes were shut down in 2001 for failing to block Web sites that were considered to be subversive or pornographic.

As recently as March, more than 2100 cafe licenses were revoked for not blocking porn. Internet service providers also have to record every message that crosses their networks. Ones that seem to violate a law must be forwarded to the Ministry of Public Security and two other state agencies and then deleted. Cybercafes aren't required to run so-called censorware—software that inspects data packets for banned keywords. But many do so of their own accord.

Berkeley's Xiao says, "Commercial entities have to follow the rules, or else they don't get a license. To survive in cyberspace, they have to censor themselves."

Despite such repressive moves and even though he himself cannot return to China, Xiao still holds out hope that the Internet will democratize China. "Overall, the authorities have to give in tremendously, in what they let people know and say, because of the Internet," he says. "It has the hope of opening up Chinese society more than any other technology I can think of. Yes, there's censorship. But if you look from the other direction, there are much greater, richer information and social spaces that exist today than would have without Internet technology."

That sentiment was echoed by Ken Farrall, a graduate student at the University of Pennsylvania's Annenberg School for Communication, in Philadelphia. He lived in China from 1996 to 2001, working on a number of consulting projects, including the now-defunct China Matrix, an English-language information site for Westerners wanting to do business there. "I pretty much looked at all the things I wanted to on the Internet when I was in China," he says. "I looked at American newspapers, listened to National Public Radio."

Farrall says China's authorities are much more effective today in keeping even technologically savvy Chinese from banned sites. Also, the censors are much more interested in Chinese-language sites than others. But the censorship is still pretty light, he says. "In some ways, it's not that different from AOL, here in the United States." AOL has blacklists to create "safe zones" free from pornography, anti-Semitism, or other things deemed offensive.

"The Internet is fairly centralized in the United States, too," notes Finkelstein, the Cambridge, Mass., programmer. "Not for political reasons but for economic ones." It turns out that the largest Internet providers push all their packets of data through large regional routers connected to proxy servers that already examine packets for evidence of quality-of-service or other problems.

"Our political system is vastly different from China's," Finkelstein says, "but if we had a national panic, if we felt we had to censor the Internet, it's scary how easily it could be done. There's a famous saying, 'The Internet considers censorship to be damage, and routes around it.' I say, what if censorship is in the router?"