



Digital Walls, Digital Holes

By Hampton Stephens : [BIO](#) | 19 Apr 2006

Details of the conversation between Bill Gates and Chinese Premier Hu Jintao when they met recently at the Microsoft campus near Seattle, and afterward at a \$20,000-per-plate dinner at Gates' Lake Washington compound, [are somewhat scarce](#). A new deal between Microsoft and Chinese computer-maker Lenovo to pre-load Windows on the company's Chinese-made machines probably was eagerly discussed. It is less likely that Hu and Gates were eager to talk about the Chinese government's Internet censorship and control policies. In recent debates about that issue -- in international human rights circles, in the national media and even in [the halls of Congress](#) -- both men have been portrayed as villains.

Indeed, the Chinese Internet censorship story owes much of its national prominence to the growing realization that American Internet companies like Google, Yahoo, Microsoft and Cisco are enabling China's censorship regime. The moral and practical dilemma about whether technological engagement or a principled embargo is the better way for U.S. companies to affect change in China has rightly been the subject of much debate, though the correct solution to that dilemma is not immediately obvious. More readily apparent is the logic of the Chinese government's censorship efforts. In a delicate balancing act between economic liberalization and the maintenance of political authority, China's leaders want to harness the Internet's potential as a propaganda tool and as a contributor to economic growth -- the bedrock of their tenuous legitimacy -- while suppressing the Web's use as a tool of political activism and truth-telling.

In the midst of this recent attention, however, the most important question about China's censorship of the Internet has not received its due consideration: Will the Chinese regime achieve its goals? Can it cleanse the Internet of undesirable information and thus shield its people from the influence of subversive truths?

So far, the Chinese regime has had remarkable success in controlling the Internet. The absence of any organizations in China that are using the Internet to challenge China's single-party rule is proof of this fact, James Mulvenon of the Center for Intelligence Research and Analysis [told the U.S.-China Economic and Security Review Commission](#) in April 2005. [The most comprehensive study](#) yet of the so-called "Great Firewall" similarly found that "China's filtering regime is pervasive, sophisticated, and effective."

However, unfortunately for Hu and his Chinese Communist Party, and to the benefit of Gates and the rest of the American computer industry, which no doubt would love to do business in China without an authoritarian regime looking over its shoulder, the success of Chinese Internet censorship is bound to be short-lived. In the long run, the Chinese government's efforts are likely to fail because of the sheer magnitude of its task. China's censorship regime cannot possibly keep up with the dramatic growth in the number of Chinese Internet users and the resulting rise in the ranks of those actively working to subvert government control. Thus, the existence of the Internet will be a persistent and growing thorn in the side of the Chinese Communist Party.

It is still very early in the life of the Internet's development in China. Less than 10 percent of the Chinese population regularly uses the Internet, but that number is growing fast. From January 2005 to January 2006, the number of Internet users in China grew by about 18 percent, from 94 million to 111 million, according to [the Chinese government's own surveys](#). Even if the rate of Internet adoption does not accelerate, almost 600 million Chinese will be connected to the Internet by 2015. This reality poses a huge problem for Chinese authorities if they wish to maintain their censorship regime.

As the number of Internet users grows, the magnitude of the government's policing effort

also must expand. Information about the exact methods of China's Internet policing system is scarce, but its characteristics can be deduced from available information.

Much of the system is probably automated, employing computer programs to block sites identified by keywords and other clues to their content. However, as anyone who has managed a computer system of any size -- whether it is a network, a server farm, or a Web site -- can attest, regular human intervention is necessary to manage the inevitable bugs, maintenance and upgrades that even automated systems require. In addition, there is much evidence that China's Internet control regime also involves widespread ground-level policing and enforcement at precincts throughout the country. As the number of Internet users in China increases, both aspects of the system will require growing expenditures of manpower and money if they are even to begin to keep up.

One analogy available for examining the level of effort involved in monitoring such a huge computer network is the work of one component of the U.S. Department of Defense. DOD's computer "enterprise" -- the approximate 2 million computers and myriad civilian and military networks that DOD administers -- is the largest in the United States, and probably the world. The [Joint Task Force for Global Network Operations](#) (JTF-GNO), part of U.S. Strategic Command, is responsible for defending DOD computers from outside attack, an undertaking that requires closely monitoring department networks for unusual activity that could indicate a breach of security.

JTF-GNO's mission is vastly less complicated than the mission of China's Internet police because DOD's network is a known quantity -- the department has awareness and control of every computer connected to it and every Web site that needs to be defended. In addition, the JTF-GNO must only keep unauthorized users out, not monitor the activity of those authorized to use DOD networks. Still, the JTF-GNO employs 255 people to protect a network of approximately 2 million computers. With an equivalent manpower-to-network-size ratio, a Chinese bureaucracy charged with monitoring and filtering the Internet activity of 600 million users -- less than half the Chinese population -- would need to have 76,500 members.

But the Chinese Communist Party's Internet control regime is not limited to automated methods. Old-fashioned policing is apparently a significant component of the government's censorship regime. Some experts estimate the number of ground-level Chinese "[Internet police](#)" at more than 30,000. Extrapolating for a 600 million-user network from the estimated 30,000 Internet police now used to monitor about 100 million users yields a number of 180,000 Internet police the country will require by 2015. What's more, recent reports indicate the Chinese government sometimes temporarily increases manpower dedicated to policing Internet activity. During a meeting of the National People's Congress in March 2005, government "security guards" monitored chat rooms and other sites, according to a March 2005 report in Xinhua, China's state-controlled media organ. "Any messages submitted by Internet users will go through rigid censoring and filtering before appearing on the Internet," the report stated.

Independent researchers have reported similar findings about chat room monitoring, suggesting the Xinhua report cannot be dismissed as mere government disinformation designed to discourage mischief-makers. In most chat rooms, in addition to sensors, "undercover agents are working . . . to guide the discussions, to cut away certain topics, to make sure the majority of the public opinions online are under their control," Xiao Qiang, head of the Berkeley China Internet Project, told the U.S.-China Economic and Security Review Commission in April 2005. [Other recent reports](#) suggest the regime aims to significantly increase the level of "real-time" Internet monitoring in 2006. These reports suggest the existence of a level of security that will be increasingly difficult, and probably impossible, to maintain.

And then there is the cost. Lacking Chinese budget numbers, the JTF-GNO's expenditures provide some basis for considering how much China will need to spend on its censorship system. According to DOD budget documents, the department plans to spend more than \$60 million this year funding the JTF-GNO's Global NetOps Center, where technicians monitor the DOD network for intrusions. An equivalent Chinese monitoring operation for 600 million users could cost \$18 billion. And this doesn't even include the cost of operating the wider policing system. This analogy is no doubt far from perfect, for one reason because labor costs are lower in China, but it does provide a framework for thinking about the

magnitude of the task the Chinese government has set for itself.

Just as the growing number of Internet users in China means a growing job for Internet monitors, it also means more users that are actively attempting to circumvent the government's control regime. This is already being done with the help of foreign software, much of it developed in the United States. Two of the most successful software products are DynaWeb, developed by [Dynamic Internet Technology](#) and UltraReach, developed by [UltraReach Internet](#). As of November 2005, about 200,000 copies of the latest DynaWeb software had been downloaded by Internet surfers in China, DynaWeb founder Bill Xia told me in an interview last year. After copies of such software are downloaded, they are routinely copied and passed on to other users via e-mail or floppy disk. The software is based on an "intelligent proxy network" that is able to "dynamically adjust itself" to get around China's Internet blocking system, which can quickly root out less sophisticated proxy server systems, Xia said. UltraReach's software works in a similar way. Voice of America and Radio Free Asia both use DynaWeb to deliver their Internet content to China.

These technologies demonstrate that the struggle over control of the Internet in China is not a one-sided battle, in which the Chinese government has all the resources on its side. The situation more closely resembles an arms race between the Chinese government and activists and freedom-loving computer programmers the world over. As the number of Chinese Internet users grows, so will their access to tools like DynaWeb and UltraReach. The U.S. Congress is also poised to give Internet freedom activists' efforts a significant boost. In May 2005, former Rep. Christopher Cox (R-CA), with bipartisan sponsorship, introduced the [Global Internet Freedom Act](#) in the House of Representatives. The bill would significantly increase money spent by the State Department's International Broadcasting Bureau to counter Internet jamming by foreign governments. The bill so far has not made it out of committee, but that could change now that the issue has gained more attention. A hearing held in February by the global human rights subcommittee of the House International Relations Committee seems to have given Chinese censorship more visibility in Congress. Meanwhile, the [U.S-China Economic and Security Review Commission](#) has recommended that Congress prohibit American companies like Yahoo from disclosing private information about its users to the Chinese government absent "formal legal action."

Despite the early success of the Chinese government in controlling and censoring the Internet, it is clear that the difficulty of its task will only grow. Whether future holes in the filtering regime are due to Chinese government failures or new filter-proof technologies, more and more Chinese citizens will inevitably gain access to an unfiltered Internet. Xia, recounting his journey from Chinese citizen to expatriate working to undermine the censorship of the Chinese Communist party, neatly characterized the political effects that free access to information can have. After studying in the United States for a period, "I realized that many things I learned in school were basically propaganda from the CCP, and that key facts were actually lies," Xia said. That revelation was enough to turn him actively against his government. China's leaders have sought to censor the Internet because they know the truth has such power, but theirs is a fool's errand.

Hampton Stephens is a writer in Washington.