“Breaching the Great Firewall:

Testimony of

James C. Mulvenon, Ph.D.
Deputy Director, Advanced Studies and Analysis
DGI Center for Intelligence Research and Analysis

Before the U.S.-China Economic and Security Review Commission

“China’s State Control Mechanisms and Methods”

April 14, 2005

Introduction

Thank you, Mr. Chairman and the other members of the U.S.-China Economic and Security Review Commission for the opportunity to take part in the hearings you are holding today on the topic of "China's State Control Mechanisms and Methods." It is an honor to and a privilege to appear here today, and I hope my presentation helps answer your questions regarding Chinese government censorship of the Internet. Before addressing that subject, however, I would like to offer some information about my background and current position. I have been studying China for more than fifteen years. For ten years, I was a researcher at the RAND Corporation, where I conducted numerous studies exploring the implications of the Chinese information revolution for U.S. national security, including analyses of Chinese domestic Internet controls, military computer network attack doctrine, and acquisition of international Internet infrastructure. With my colleague Michael Chase, I authored a 2002 RAND study entitled *You've Got Dissent! Chinese Dissident Use of the Internet and Beijings' Counter-Strategies*. My testimony today draws from our follow-on, unpublished RAND study entitled *Breaching the Great Firewall*.

I left RAND late last year to help found the Center for Intelligence Research and Analysis (CIRA), a high-quality thinktank that supports the people and organizations throughout the U.S. intelligence enterprise. CIRA's mission is two-fold: (1) improve the conduct of U.S. intelligence through unique research and analysis across the spectrum of intelligence activities, whether at home or abroad; and (2) help foster a more thoughtful and responsible debate about the future of the U.S. intelligence enterprise. I lead CIRA's Advanced Studies and Analysis unit, which currently has six advanced Chinese linguists conducting research studies for various parts of the intelligence community.

China and the Information Revolution

The importance of cyberspace as a battlefield in the struggle between the Chinese government and foreign and domestic critics of its censorship policies has been magnified as a result of the dramatic growth of Internet access in China. Increases in the number of users since personal accounts were made available in 1995 has been virtually exponential and is expected to grow at impressive, though declining rates for the foreseeable future. China's international connectivity and the number of computers with Internet access are also expanding impressively. Along with the rapid diffusion of Internet connectivity in China, many commentators, politicians, and pundits in the United States and elsewhere have speculated not only about the economic and social implications of the Internet, but also about its potential to facilitate political change and undermine the dominance of the Chinese Communist Party (CCP).

Especially in the early years of the IT revolution in China, many observers argued that the Internet would dramatically shift power to the Chinese people by allowing them to organize and by channeling uncensored information from outside, especially about democracy and human rights. To be sure, the Internet has further degraded the regime's ability to control the flow of information, both within China and across its borders.

Despite these initial expectations, however, the Chinese government has managed to stifle most attempts to use the Internet to promote political change. The regime has imprisoned dozens of web surfers for "subversive" use of the Internet and erected a technologically complex set of monitoring and control mechanisms, widely referred to as the "Great Firewall," to limit access to information it deems harmful to its interests. Online freedom of speech advocates and exiled Chinese democracy activists have mounted numerous attempts to breach the Great Firewall, achieving limited results. Meanwhile, in response to these challenges, the Chinese government has increased the sophistication of its Internet controls.

The technological enhancement of China's Great Firewall and the July 2003 approval in the U.S. House of Representatives of the Global Internet Freedom Act, which reflects the growing involvement of the U.S. government in supporting attempts to undermine Beijing's Internet controls, portend an intensification of the online struggle between the Chinese government's Internet censors and U.S.-based advocates of online freedom of information. The escalation of this struggle in cyberspace also underscores the need for thorough analysis of the strengths and vulnerabilities of the Great Firewall and of the most promising anti-censorship technologies. Drawing on Chinese primary sources, independent technical analyses, and interviews with key participants in ongoing efforts to circumvent the Chinese government's Internet controls, this report assesses the Chinese government's Internet monitoring and control mechanisms and evaluates the anti-censorship technologies that are the cornerstone of efforts to circumvent these restrictions.

Building the Great Firewall

From public statements, policies, and actions, it is clear that the Chinese regime is anxious about the consequences of the country's information technology modernization, in particular the challenge of confronting an increasingly complex and challenging global information security environment. The government fears that hostile organizations, either foreign or indigenous, will use these new information technologies to agitate the population and undermine the regime.

As a result of the rapid growth of the Internet in China, the leadership of the Chinese Communist Party faces a series of challenges that are testing its ability to balance the competing imperatives of modernization and control. On one side, the regime believes that information technology is a key engine of economic development, despite the burst of the Internet bubble and the dashed hopes of numerous Chinese "dotcom" companies, and that future economic growth in China will depend in large measure on the extent to which the country is integrated with the global information infrastructure. At the same time, however, China is still an authoritarian, single-party state, whose continued rule relies on the suppression of anti-regime activities. The installation of an advanced telecommunications infrastructure to facilitate economic reform greatly complicates the state's internal security goals. Faced with these contradictory forces of openness and control, Beijing has sought to strike a balance between the information-related needs of economic modernization and the security requirements of internal stability. In doing so,

the authorities are actively promoting the growth of the Internet even as they place significant restrictions on online content and the political use of information technology. The operationalization of this strategy includes low-tech and high-tech countermeasures. The low-tech countermeasures draw upon the state's Leninist roots and tried-and-true organizational methods, while the high-tech countermeasures embrace the new information technologies as an additional tool of state domination. The mixture of the two has proven a potent combination in deterring the majority of anti-regime behavior and neutering most of what remains.

Since the arrival of the Internet in China, low-tech countermeasures have been an important component of the regime's strategy for countering what it regards as subversive uses of the Internet and related communications technologies. The Chinese authorities have issued a series of broad regulations that forbid online activities seen as detrimental to the Communist Party's interests. These bureaucratic regulations, such as the Internet Service Provider laws that make providers responsible for the activities of their subscribers, are among the most effective lines of defense in China's Internet security strategy, shaping the market environment and the incentives of key participants in ways conducive to the state's interest. To complement the regulations, the authorities have also elicited further pledges of cooperation from key industry players.
Another important part of the low-tech counter-strategy is making examples of dissidents and other Internet users who violate the regime’s rules. In all, at least 35 Chinese Internet users have been arrested for “subversive” use of the Internet. In addition to selectively publicizing some of these arrests, the regime occasionally highlights the monitoring capabilities of its "Internet police" in the official media. In some cases, official media reports may deliberately exaggerate the ability of the authorities to monitor the activities of ordinary Chinese web surfers to deter Internet users from engaging in “subversive” online activities. The desired result is the creation of a climate in which the vast majority of Internet users are either disinterested in or deterred from undertaking any online activities that might risk punishment by running afoul of the censors.

Initially, the regime was heavily reliant on this sort of "low-tech Leninism." More recently, however, the regime has supplemented its strategy with an array of high-tech countermeasures. Over the past several years, these high-tech countermeasures have become both more sophisticated and effective, apparently reflecting a substantial investment by the Chinese authorities in enhanced blocking, filtering, and monitoring capabilities. According to an estimate by an exiled Chinese economist, Beijing’s total investment in these capabilities may amount to as much as $800 million. The centerpiece of this high-tech component of the regime's strategy for limiting what it perceives as the negative side-effects of the spread of the Internet has been the construction of a system of high-tech Internet controls, dubbed “the Great Firewall” by the regime’s critics. Although it remains far from impenetrable, in recent years, the Great Firewall has become increasingly technologically advanced and effective.

Technical analysis of the Great Firewall indicates extensive deployment of sophisticated equipment capable of blocking access to prohibited sites and proxy servers as well as filtering the content of accessed sites and email, though uncoordinated internetworking

construction in China appears to be a growing source of disruptions and failed service for China's Internet users. In particular, technical analysis reveals the widespread use of transparent proxies to perform inline content filtering, proxy server hunting, and POP3 email filtering, as well as rampant hijacking of domain name service (DNS) queries, including the capturing the requests to foreign servers on the wire and spoofing responses.

Breaching the Great Firewall

Various parties outside of China--ranging from Chinese exiles seeking to promote human rights and democratization in China specifically to international hacktivists focused on undermining online censorship worldwide--have responded by developing technologies designed to breach the Great Firewall. To date, only a few groups have managed to deploy programs that have generated substantial levels of traffic. The two groups that are currently enjoying the greatest success in that regard are Dynaweb and UltraReach. Both groups are on contract with the U.S. government to support efforts to facilitate access to the Voice of America's Chinese language news website, which has been blocked in China (the two groups are staffed largely by Chinese-American computer technology specialists and expatriate adherents of the banned Falungong spiritual sect, though the latter fact speaks more to motivation of the organizations than deliberate support for Falungong by the US Government.

Discussions with members of the DynaWeb team indicate that thousands of Chinese users access the system regularly; they estimate that the system currently transfers about 400GB of data each week, excluding media file downloads, and that the homepage is viewed about 90,000 times per day. Overall, traffic has grown considerably over the past year, as a result of several factors, including enhanced server side performance, Dynaweb's online promotion efforts, and an apparent increase in demand for uncensored information during periods when heightened political sensitivity results in particularly strict censorship of domestic media. For example, user traffic surged during the April 2003 SARS crisis and also increased dramatically around the time of the March 2004 Taiwan presidential election.

The services Ultrareach provides to VOA and RFA have generated substantial levels of traffic from Chinese web surfers. In May 2004, the latest month for which statistics were available, Ultrareach's https, UltraScape, and UltraSurf systems allowed a daily average of about 4,000 visits and nearly 30,000 page views for VOA, and about 2,600 visits and 28,000 page views each day for RFA. The usage statistics for early 2004 indicate that UltraReach traffic to the VOA and RFA websites peaked in March, probably as a result of intense interest in the controversy surrounding the contested presidential election in Taiwan.

The designers of these programs and other similar programs, however, must contend with several structural constraints that have the potential to limit the influence and effectiveness of their anti-censorship systems. Recent surveys indicate that the most significant problems related to Internet access in China are slow access speeds,

connection difficulties, and high costs. Many of the same constraints that have apparently slowed the growth of P2P technology for exchanging music files in China are also likely to pose some obstacles to the use of P2P applications for political purposes. The most frequently cited constraint, however, is that many of the P2P programs designed to breach the Great Firewall are not particularly user-friendly. Developers are aware of this problem, and many say they are making improvement of user interfaces one of their highest priorities, but much remains to be done to make the anti-censorship applications more accessible to average Chinese web surfers. This in particular reportedly has limited the popularity of some P2P applications, such as Freenet China, that were designed to help Chinese Internet users undermine official censorship. The inability on the part of many groups to produce software that is sufficiently user-friendly stems in large part from shortage of manpower and the inadequacy of financial resources. Most of the groups that are developing anti-censorship programs have only a handful of full-time programmers, and a few are effectively one-man operations. Although a few groups have received limited U.S. government support, most suffer from weak funding. With no commercial applications for their programs, many say, private foundations and governments are their only potential sources of financing. Beyond these resource constraints, there are two more fundamental problems: lack of interest and lack of trust. These final structural constraints are perhaps the most difficult challenges for the groups that seek to breach the Great Firewall.

Architectural vulnerabilities also pose serious concerns. Indeed, although the technology and tactics they have employed have evolved over time, most of the mechanisms designed to breach the Great Firewall suffer to varying degrees from architectural flaws that render them vulnerable to several blocking or exploitation measures, including IP blocking, port blocking, packet sniffing, virus attacks, and infiltration by security agents.

Implications

In its efforts to filter content and hijack DNS requests, it is no hyperbole to say that China is undermining some of the core, trusted protocols of the global Internet. The implications of these activities are profound at many levels. Internationally, China has quickly emerged as a major player in the global information technology policy arena, as measured by involvement in international organizations and creation of new IT standards, but its rampant DNS hijacking and content filtering should give pause about its dedication to international rules and protocols. Domestically, the real target of this activity, Chinese users seeking to circumvent the Great Firewall to obtain independent news and information, are clear losers, but they are not the only ones. Since the regime believes that information technology is a key engine of economic development and that future economic growth in China will depend in large measure on the extent to which the country is integrated with the global information infrastructure, overzealous application of DNS hijacking and content filtering could spill over into non-political transactions as well, perhaps threatening to undermine the Chinese government’s strategy of exploiting the Internet’s potential as a key driver of economic growth.

As for the pro-democracy activists and computer engineers who are trying to "breach the Great Firewall," even if they managed to wrest the technological advantage from China's Internet censors, they would still need to contend with a more fundamental strategic problem: devising a workable plan for using technology to promote political change in China. Harnessing the Internet and related technology to support political change has proven challenging and frustrating for those who anticipated that the diffusion of the Internet would facilitate change simply by making a variety of sources of outside information accessible to Chinese Internet users. Beyond the increasing scope and sophistication of the Great Firewall, anti-censorship and pro-democracy groups face other challenges. There are now many more internal sources of information in China, including an increasingly vibrant traditional media and a dynamic Internet news environment, and these trends reduce the demand for external sources of information, particularly given the possible risks. Inconvenience is also a factor; many of the circumvention programs are not user-friendly or require sophisticated computer skills to install and operate, and therefore appeal to only a small core group of technical experts and are not used by the much larger group of casual users. Those technologies that are explicitly designed to be as user-friendly as possible still face significant technical obstacles, especially the determined counter-measures of an increasingly sophisticated content filtering and blocking regime.

For those trying to use technology to foster change in China, it is also not simply a question of outsmarting the censors, but also one of dealing with disinterest, apathy, and mistrust of outside sources of information, all of which are obstacles to finding a workable model for using the Internet for disseminating information and facilitating change. Some advocates of online freedom of speech are beginning to recognize the centrality of the issues of trust and credibility. In a recent paper, Bobson Wong summarized the problem as follows:

> Improving the ability of people in China to access banned material online is certainly necessary and important, but there is no guarantee that Chinese users will want to take advantage of this privilege…simply 'liberating' China's Internet from government censors may not lead to a dramatic change in popular attitudes. Turning the Internet into an effective tool for social change in China involves not only solving the technological problem of reducing online censorship, but also providing a balanced forum for communication that Chinese users can trust.

This forces many anti-censorship activists to consider a problematic tradeoff: the U.S. government is likely their most attractive source of funding, yet association with a foreign government might compromise the their credibility as an unbiased source of information in the eyes of many Chinese Internet users.

Despite these many obstacles and the success of the censors in China thus far, however, there are some reasons for optimism and hope, however slim. A recent Chinese Academy of Social Sciences (CASS) report on the social impact of the Internet in China found that Chinese web surfers expect the Internet to enhance freedom of speech and increase opportunities for political participation. According to the report, "The Internet is

changing the Chinese political landscape. It provides people a platform to express their opinions and a window to the outside world as never before." As a professional Chinese middle class emerges, it will likely increasingly seek to leverage its growing economic clout in the political arena, at least to provide inputs into state economic policies. With the media under state supervision, the Internet is an attractive forum for organizing and articulating these preferences, and could thus serve as the medium for the pluralization of the Chinese political system, either within a co-opted space permitted by the Chinese Communist Party or in direct opposition. In this way, the Internet in China could facilitate political change in the same way that audio tapes of Khomenei's speeches helped overthrow the Shah in 1979 and fax machines almost brought down the Beijing government in 1989.