Testimony before the U.S.-China Economic and Security Review Commission

China's State Control Mechanisms and Methods

Kenneth Berman

Director of Information Technology
International Broadcasting Bureau
Broadcasting Board of Governors
Washington, DC

April 14, 2005

Mr. Chairman and Members of the Commission:

I am very pleased to have the opportunity to address the Commission today on the issue of Internet information control and censorship by China. I have been involved with developing solutions to this vexing problem for the past several years and hope to share with you some of our findings and conclusions. I would like to discuss some of our technical efforts to allow users in China to get unfiltered, uncensored access to news and about other key issues of the day.

The Office of Engineering and Technical Services is responsible for delivering program content for the various worldwide services under the Broadcasting Board of Governors (BBG). These services include the Voice of America, Radio Free Asia, Radio Free Europe/Radio Liberty, Radio and TV Marti (to Cuba) and the Middle East Television Network. The traditional way for distributing these programs has been via radio: shortwave, AM, FM and satellite. Our Office works closely with fellow international broadcasters and the International Telecommunications Union to coordinate the appropriate broadcast frequencies to ensure that there is no intentional interference between broadcasters.

Before I tell you about my work with Internet "jamming", I did want to inform you that the Chinese regularly jam all of the Voice of America and Radio Free Asia programs, in clear violation of accepted international rules and regulations followed by almost all other nations. This jamming consists of playing endless loops of Chinese opera music at the same time and on the same frequency as the VOA and RFA broadcasts. Despite numerous official protests by BBG via the FCC and the State Department, the radio jamming continues unabated. The technical capability of the FCC in observing the Chinese jamming is absolutely unambiguous. There is no doubt that the origin of the jamming is in China. The nature of the transmissions emanating from the identified locations in China have no useful telecommunications purposes, and it can only be concluded their purpose is for jamming.

The Internet is becoming a critical component in distributing program materials to those countries that are – or are becoming – "wired". And China is the most "wired" of all the large countries to which VOA and RFA send their programs. I attended a conference on China and the Internet at the University of Southern California, and it was interesting to hear the various U.S. and China scholars debate how many Internet users there were: estimates ranged from 39 to 63 million several years ago. Now the number is approaching 90 million and rising at a faster rate than for any large country in the world. What the numbers do tell us – unequivocally – is that China has the most Internet users in the world after the United States, and considering their huge growth rate of new users and the small fraction of their population that currently has an Internet connection, it is clear that they will be the largest Internet audience in the world in the not too distant future.

As has been discussed by many experts more knowledgeable than me on the subject of China and the Internet, the Chinese are attempting to have it both ways: use the Internet as a driver for knowledge transfer and business development, while ruthlessly suppressing any attempt to question the policies of the Chinese Communist Party, to discuss the rulers in any but glowing terms, or use the Internet for issues as diverse as Tibetan Freedom, Taiwan independence, pro-democracy movements, or religious groups such as Falun Gong. VOA and RFA came under the cross hairs of this censorship effort when they tried to send email summaries of the news specifically requested by Internet users in China. These same users, when they could get a message through, informed us that the VOA and RFA web sites could not be accessed from inside China, whether it be from home, office, or an Internet café.

As a result of this censorship, and considering the critical importance of China to U.S. policy interests, the BBG established a special unit to devote technical resources to this problem. We have consulted with industry and government consultant experts on what works and what doesn't work in terms of getting information inside China. What we have essentially instituted is a two prong "push-pull" program that consists of separate but related efforts. The "push" component consists of pushing email news to those users in China who would find the news interesting, useful, or a necessary complement to the official, approved news stories. The "pull" component consists of allowing users the ability to access the VOA and RFA web sites and pull Internet content into the browsers of their computers. I would like to give you a few comments on these two efforts, and then inform you of some of the other activities we are working on.

The email component of the program allows the VOA and RFA journalists to assemble summaries of critical Chinese, U.S., and international news stories each day into an easy-to-read Chinese language email. The email is distributed by our Office using techniques that will do the most to ensure the message will get through the filtering mechanisms of the Chinese Government. Originally, the VOA emails were sent from one of VOA's openly labeled voa.gov email servers. It was discovered that very few of the messages were getting through. The Chinese were in the early stages of developing their censorship technology, using computer technologies primarily purchased from U.S. companies. Over the past few years, they have continued to buy this equipment, and have also started indigenous manufacturing of these computer network routers. At this time, before I continue with the discussion on the email program, let me say a few words about the actual techniques of their censorship.

While many companies, libraries, and organizations exert some form of restriction on their users' ability to access any and all sites, the Chinese use every possible technique and are continuing to refine their methods. Internet locations are defined by a numerical address, known as the IP (or Internet Protocol) address. Since people, unlike machines, find numbers difficult to remember, a naming system has been developed whereby people use names, and computer systems translate those names into numbers. This way the machines can connect to each other while human users simply use normal names. This is known as the Domain Name System (DNS) and, like the airwaves, is governed by rules and regulations, but also a certain amount of trust; more about that later.

The Chinese Government can easily find the IP addresses of VOA and RFA and enter them in their computer router tables, with the instruction to block any traffic from the servers or any requests for information to those servers. These computer routers serve as electronic "gatekeepers" at the country's border, and are known as border routers. They are a brute force solution to the problem of censoring unacceptable sites. They do work in keeping the Chinese user separated from computer sites that have been "black listed," so to speak. But, since several, sometimes many, organizations share an address or group of addresses, this kind of blocking may keep out traffic for which there is no fear by the Chinese. This is the reason some sites that are completely harmless to the Chinese may not be accessible: they share an address or group of addresses with a censored site.

To improve their ability to focus their blocking efforts, they will also filter the actual word name of the site, as in www.voanews.com or www.rfa.org. This way, anyone coming or going to the name VOA or RFA will be denied access. This is generally accomplished by finding what Domain Name Server does the translation from name to IP address and blocking that. Thus, the user will be denied the ability to find out how to convert www.uscc.gov into an actual address computers can use, and will not be connected. In an even bolder move, if that is the right word, the Chinese have started using DNS redirection, or "hijacking". It is a severe violation of the "trust" various computer systems use to communicate with each other, and consists of going into the DNS system and inserting one's own lookup listing; this is similar to rewriting selective pages of a phone book, inserting them under cover of darkness, and letting unsuspecting users be directed to the wrong address or phone number.

Universal Resource Locator (URL) filtering and content filtering are essential tools in Chinese censorship. URLs are the addresses that we read. But, a full URL, especially when doing a search, consists not only of the URL, but text following the URL. For instance, if you were doing a search on www.google.com for "US Congress", you would generate a URL that might be www.google.com/word:US+word:Congress. This way, with URL filtering, the filter could allow traffic to Google to pass, except when some of the key words that the user was searching for were included. Initially the Chinese Internet censors blocked access to all of Google, using the more brute force methods described above. After an outpouring of protests from students, business leaders, and anyone else using the English or Chinese versions, the Chinese introduced their refined techniques. Essentially, this consists of looking not just at the site, but at the page or search one would like to do at that site. If it passes the test, the request is allowed to go through. If not, the user is not only denied the request, but is put in what I call the "penalty box" for twenty minutes to days at time. Reports differ, but our experience is about one hour for the first violation, two hours for the second, and a day for the third. Thus if one did a Google search on apples, the search goes through. If the search is on "pro-democracy", the request is denied and the user is disconnected, i.e. prevented from making any more requests to or from any part of the Internet.

One of the more interesting studies done on filtering is by the OpenNet Initiative. This is a group of scholars from the Berkman Center for Internet and Society at Harvard Law School, the University of Toronto's Munk Centre for International Studies, and the University of Cambridge in the United Kingdom. Their mission is "to investigate and challenge state filtration and surveillance practices", and they can be found at http://www.opennetinitiative.net/index.php. They have published reports on the technical details of Chinese government censorship, and we regularly confer with their technical staff in attempting to ensure we are using the latest techniques.

For our email program, you can now see that all emails from VOA's or RFA's IP address, its URL name, and any controversial content were being blocked. This was not acceptable, and working with some state-of-the-art experts from think tanks and industry, as noted above, we developed techniques to get the emails through to their intended audience. We have sponsored two symposiums with leaders in this area and have tried to do our part in sponsoring research related to technical means of defeating Internet censorship. We have looked at how to use the cellular phone system in passing information into China, as well as utilizing various instant messaging systems. Some of these areas offer promise, but require increased funding.

Other areas such as peer-to-peer computing seem less promising. One of the key drivers in the United States to peer-to-peer systems such as the old Napster and the current systems of Kazaa and Limewire are illegal file transfers for music and other files. Due to what appears to be less official concern in China over complying with international copyright laws, there is less need for these peer-to-peer systems as individuals can just go to local web sites and download music and other content.

We send millions of emails a day, and the response has been overwhelmingly positive to the VOA and RFA language services' news summaries and information on local Chinese and international news. It should be noted that we take extraordinary care to make sure that these VOA and RFA emails only go to users inside China. After all, there is no need to devote the elaborate resources to Chinese readers in Singapore, Taiwan, or any other areas with Chinese readers and no technical censorship issues. Despite having sent billions of emails over the past several years, we have received only a handful (less than five) from individuals outside the target audience.

Related to this "push" component is the "pull" component. On each of the emails we include from 2 to 6 different "proxy" sites. Just as in "proxy" voting, a proxy computer or server is simply one that is standing in for another computer. Proxy computers have many purposes, such as making communications more efficient and helping organizations keep out bad/malicious users. In our case, we are using the proxy sites we have developed to stand in for forbidden sites. By that I mean that, even though RFA and VOA are blocked, chances are that www.kenberman.com is not blocked (at least not yet!). So, if we distribute the name www.kenberman.com to our Internet users via our emails, the users will be able to click on this presumably unblocked site. Once they hit the site, a Secure Socket Layer connection is established. This is the same type of secure connection that is made when you make a credit card sale - virtually unbreakable. So, upon connecting to the proxy site, the user is given a secure connection (the same kind used in e-business, and not by itself incriminating) and landed on either a VOA or RFA Chinese language home page. From there, the user can explore the VOA or RFA news and feature stories in detail and can stream audio programs. Moreover, in line with our desire to promulgate global information freedom, we have a "jump" bar in all of our proxies. These allow the user to explore any other site in the world he or she can connect to, including controversial political sites, religious sites, business or school/educational sites. We do filter pornography, however, and also have geographic tracking to make sure that only IP addresses that originate in China are able to use these services, and not individuals elsewhere who may want to use these tools to avoid paying for these services.

We have received thousands of unique visitors each day on each of the proxy sites, and most of the traffic has been to VOA and RFA, with other Chinese language news and social sites running second.   As I described above, eventually the Chinese Internet police learn the name and address of the proxy and then we change it, distributing the new proxy name via the daily emails. The Chinese Internet police have introduced “proxy hunting” software, which has shortened the life of the proxies and resulted in more frequent changes to the names. Thus, the email push and the proxy pull are intimately connected, that is the email and web proxy techniques work hand in hand to break through the Great Firewall of China.

The systems we use are very scalable and we would like to expand the emails lists to tens of millions of emails a day, with proxies rotating automatically every day. As noted above, we have been looking at Short Message Text (SMS) cellular telephone networks. One of the problems with SMS, unlike the Internet, is that the cellular phone companies are single points of control over their networks – unlike the Internet, which is literally an interworking of networks. This prevents the freedom to maneuver that the Internet offers. Nevertheless, with as many cell phone users in China as we have citizens (nearly 300 million), our future research must concentrate on utilizing the cell phone system – either for text messages or for mobile web content such as audio and video clips – to make further inroads past the gates of censorship. We also hope to improve our proxy web sites so that they, too, can pass audio and video clips. Please remember that unlike some research programs that are underway, our techniques must reach millions and perform to the standards that all of us expect of our Internet systems. After all, if our techniques succeed in bypassing Chinese Internet censorship but perform slowly or poorly, we will lose our audience, no matter how good our information is. We must ensure that we provide a tool that the Chinese citizens seeking uncensored information actually want to use.

We feel we are making progress in this attempt to break through the Great Firewall and allow Chinese citizens free/unfettered access to a wide range of previously censored information. However, it is truly a cat and mouse game, and only by continuing to explore, test, and implement new techniques will we be sure we can stay successful. Our program has generated a wide range of support from academia, business, NGOs and think-tanks, and we look forward to leading the effort to allow people in censored regimes to have free access to news and information.