Statement of Bill Xia
China's Cyber-Wall: Can technology break through?
November 4, 2002

DynaWeb was launched on March 12, 2002. It is a proxy network that allows users to circumvent the Internet censorship in China and to have secure and full access to the Internet. Users use DynaWeb as an information web portal to all other web sites. Since the inception of DynaWeb, we have managed to stay ahead of the censorship by China most of the time. 20,000 unique users gained regular unblocked access to the Internet through us.

DynaWeb has already played several rounds of the censorship and anti-censorship game in the past eight months.

Before I start, I would like to explain a few critical technical terms for understanding DynaWeb experience. There are two ways to access a web site through an Internet browser. One is to type in the domain name, for example, www.google.com. The other way is to type in the IP address of the domain name. The IP address is the essential place the browser will fetch the web site information for the user. However, domain name is more user-friendly. After a user types in a domain name, web browser will resolve domain names to IP addresses and fetch the right information for the user.

The game started with e-mail subscription service. DynaWeb e-mailed unblocked IP address updates to subscribers. After two weeks, the censors probably subscribed to our e-mail service too because the valid time window of DynaWeb IP addresses reduced to a range from a couple of hours to a few days after release.

Then our services expanded to domain names with dynamic IP addresses. However, censors started chasing DynaWeb domain by automatically detecting the IP addresses that pointed to the domain name. This dramatically increased the needs for back-up IP addresses, hence increased the cost of DynaWeb maintenance. DynaWeb adopted new strategy so that censors had to manually verify the IP addresses before blocking it. Then automatic IP blockage stopped.

Soon in August, users started to have difficulty of accessing DynaWeb through https even the IP was not blocked. It was found out later on that the certificate DynaWeb used for secured access from the Internet browser was filtered. This can be achieved by package level analysis of Internet traffic to find out signature related to the certificate DynaWeb used. In response to this, DynaWeb started to change its certificate daily. No reports of certificate blocking have been found since then. Again, censors were frustrated with the resource required for daily updates of all related content filtering engine, and quit.

At the end of September, DynaWeb domain names were hijacked to a fixed IP 64.33.88.161 in China, along with many other web sites like www.voa.gov. DIT has published a detailed report about this hijacking (http://www.dit-inc.us/report/hj.htm), and it can be independently verified from the U.S. More study about this hijacking is still undergoing and will be released after we pass this stage.

So, what is next with the Cyber-wall?

At the first look, it is a technical question if technology can break through China's Cyber wall. In fact it is not. This process is a race of technology and time. As DynaWeb's experience has demonstrated, both parties can always implement new technologies to stay ahead and sustain the advantage. If Internet breakthrough is defined as a pure technical issue, the future is brighter for censors because China purchases the most advanced censorship technology from western companies.

China is also developing the Golden Shield project, a "database-driven remote surveillance system". When the whole Beijing city is wired with biometric sensor and camera network, no Internet based anti-censorship can get around the surveillance system.

Even now, during the eight months of technical race with DynaWeb, China has developed the largest and most sophisticated IP blocking and content filtering system in the world. The more anti-censorship technique is deployed, the more comprehensive censorship technology has become. This leaves less and less technical room for anti-censorship. It is critical to take full use of technologies to benefit as many people as possible before the door is closed.

Second, it is a matter of available resources. China has 30,000 Internet police specialized on Internet censorship, and ISPs are forced to perform self-censorship. The self-censorship is even adopted by foreign ISPs such as Yahoo. China has purchased top technology from western companies. These technologies have even been modified for China's particular censorship needs. Nortel, Sun Microsystems, Cisco and many smaller companies contributed to building China's Cyber Wall [1]

Comparing to China's investment in censorship and cyber wall, investment in breaking though this Cyber Wall is next to nothing. There are very few groups developing technologies suitable for this Wall. With more resources, DynaWeb can provide services to more people, develop better client software, have closer monitoring of censors' new technologies and respond faster.

Third, people develop technology and technology serves people. People factor is the most important factor eventually. Recent increase of public awareness about China's Internet censorship both inside and outside of China is a great sign. We hope that this will help improve the current situation soon. Currently companies contributing to China's Cyber Wall bear little public pressure, not mention any legislative limitation.

Inside China, more and more harassment and arrests of dissidents and journalists are related to the Internet. Last year, there are more than ten arrests in China for distributing forbidden information. This will create fear among the public. For the general public in China, they are now gradually realizing the existence of censorship consciously.

More importantly, government has adopted subtler mind control and propaganda to decrease Chinese's interests in uncensored information. All major events outside of China are reported, with seemingly a variety of views, although all the different views are in fact the government's view. There is a fully developed online community inside China serviced by self-censoring ISPs. This strategy is an extension of China's Cyber Wall, a wall in people's mind. Internet, combined with TV, newspaper and other information channels now offers Chinese people different types of information and different views on certain issues. It looks like that full freedom of speech has been achieved. However, the government produces all the different views and types of information. The censors try to use this to reduce people's interest in uncensored information.

In summary, technology along won't decide the future of China's Cyber Wall. But people do. If all Chinese people would like to obtain uncensored information, the cyber wall will be broken, from the inside.

---

[1] China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China, by Greg Walton, International Centre for Human Rights and Democratic Development
http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html