

The Great Firewall of China: Cyber-Censorship

Elmo M Recio

SOC 330 - Problems and Policies of Developing Nations
Psychology, Sociology, and Anthropology Department
College of Arts and Sciences - Drexel University

June 13, 2000

Abstract

The Chinese government has long been able to suppress the varying external influences to their country by banning the physical availability of opposing press. As the rest of the world's economic and political views become increasingly available on the Internet the Chinese government faces another medium by which opposing propaganda may enter their country. Outlined will be the current threats to Chinese government through the Internet and the policies they have taken to counteract these threats.

1 Introduction

There are really only two routes that the Chinese government can take towards the deflection of outside propaganda, and exposition of "state secrets." They can either, ban the Internet entirely from the country's computer networks, or become selective gatekeepers for the traffic flowing into and out of the Chinese network. The simple solution of isolating the Chinese cyberspace from the rest of the Internet may seem rather simple enough.

However, what complicates the isolation scenario is the fact that in order for China to remain aloft in the technological scene, it must keep its cyberdoors open to innovation and the world technological advances. By China isolating itself from the rest of the Internet, it limits innovation and fosters technological stagnation. This, in the end, exacerbates the difficulty of the cyber-border patrol maintenance.

2 Status Quo

There are several strategies that the Chinese government is undertaking to attempt to censor its web-sites. These strategies stretch from suspending a site, to blocking out entire subnets of the Internet. Here we will overview several case studies where the government has successfully quieted the Internet sources, and analyse the resources involved.

2.1 Rumour Mongering

Chinese financial-information web site called China Finance Information Network (WWW.cfi.net.cn) suffered a government imposed suspension for 15

days and a fine of \$1800 USD. The crime is rumour mongering; the web site published an article which accused some local official of corruption.[5]

This article got through the filtering of politically sensitive areas like Taiwan, Tibet, or the Falun Gong, the religious group that has recently roused the anger of President Jiang Zemin for using e-mail as a way to organise protests against the government.

For two weeks CFI Net could not post anything on their web-site. They cannot post financial related materials, or any other articles. Most importantly, they could not post any advertisements, which CFI desperately relied on for their revenue.

If web surfers would go to the company's web-site, all that they would have seen was a blank page with boldened letters in the middle stating their "Suspension of Service Announcement". Beneath it a small paragraph which stated that the site had been suspended for two weeks during which time the employees of CFI are undergoing "political re-education."

2.1.1 Impact

The obvious impact that this suspension had on CFI is immediately apparent: pecuniary. CFI, each day, had about a million page views, from 100,000 daily users. As a result of the suspension, an estimated \$120,000 in advertiser spending had been lost in just the first 4 days.

An Internet user only known as "mcc"[7] posted the following on a web-site forum for news:

Quick but painful slap on the wrist, and the whole thing is more or less over 15 days later ... the damage to the psychological state of the employees lasts.

Another Internet user known as "krog"[6] posted the following regarding the emerging new force (the Internet):

The Internet is by far the most effective irritant ever to the differences in countries' laws; in this case, it's China's (over)reaction to information physically located within its bounds but visible to and destined for the entire world.

2.2 Information Security Issue

Recently, China imposed a new law[3] on cryptography on 31 January 2000. Encryption technology, which is supposed to protect data from interception, was supposed to have been registered with the government by the 31st of January. However, many of companies paid little regard to this law due to its convoluted conditions.

The government expected every company that uses encryption technology to register their technology. Additionally, the company was to submit the names, phone numbers, email addresses, and locations where the encryption technology is used. End users of encryption technology were also required to submit a registration form.

To finish it all off, the registration for all nine million Internet users in China, was to be hand delivered to a small office in an alley in Beijing, to the newly created administration: State Encryption Management Commission.

2.2.1 Impact

The immediate impacts seem to be non-existent. In fact, when the deadline approached, only a dozen individuals were present to submit the forms. However, the long term effects are to benefit the government as they selectively enforce it.

The law is clearly unworkable; there aren't enough people and the commission just isn't large enough to handle the paperwork necessary for filing all of the registrations. The government isn't doing much to enforce these new laws either. So why then would such a law be passed? Selective enforcement that may be used by the government as needed later.

3 Net Nanny

Two men sentenced to death for hacking into a Chinese bank's computer system.

Businessman sentenced to life imprisonment for releasing 30,000 email addresses to external dissident organisations

China's Internet population has quadrupled in a span of only a year. Totalling 8.1 Million as of December 1999. And an estimated 20 Million by the end of 2000. With an increase of 1,500 to 15,000 web-sites, and 35 Million

email addresses[10] Beijing will have to struggle to maintain control of the Internet.

3.1 Internet Dissidents

The Internet is increasingly being viewed by China as a medium through which National security issues may leak out. More importantly it is being seen as a way through which its citizens may organise and rally, to the point which will be hard to manage.

3.1.1 Technically...

Wherever there is an interruption in service due to censorship, the Internet traffic will just route around the unaccessible site. This was the original intention of the Internet when created by DARPA (Defence Advanced Research Projects Administration.) The purpose was that if the Soviet Union would attack the United States they could blow holes in the network, but the traffic would route itself around the broken bits of Internet.

In China, there are central servers (Internet Service Providers) that through which all of the Internet access for the country flows. These specialised servers are called firewalls. This is the simplest way to block access to website that Beijing feels are subversive; however, users are still able to access the Internet by making long distance calls to Internet service providers in neighbouring countries.

3.1.2 Hacktivism

Dissidents of current Chinese policies (from outside the country) have hacked into Chinese servers and place dissenting political statements. These people have been termed “Hacktivists”; hacktivists are emerging as the new wave of political activists in the digital age. They are finding out that such actions are quite effective and powerful in countermanding the oppressive Chinese government.

Political hacking appears to be the most potent threat to the authorities’ attempts to censor the Internet. Many official government sites are using outdated and insecure software, giving hackers leverage and opportunity to make their point on sites to which every Internet user in China would have access.

3.1.3 The Beijing Crackdown

Beijing has launched (with increasing aggression) various actions against individuals that have been identified as having contributed to subversive behaviour. The recent case of the Chinese businessman, Lin Hai, owner of a Shanghai-based software company, was sentenced to two years in prison for disseminating 30,000 e-mail addresses to a US-based dissident publication. And another case of the government ordering the closure of an on-line discussion board.

The e-mail list in the Hai case was reportedly used to distribute banned news materials to the owner of the email addresses. Although Hai admitted to disseminating the list, he stated that he did it for commercial purposes. He had no idea of the e-mail list's final use.

3.2 Reality Check

There are two facets to China's control of the Internet. On the one hand it is attempting to "keep national secrets from being stolen." On the other, it is seeking to curb political criticism, both from within, and without.

The bureau of government to administer the Internet encryption is the State Information Security Appraisal and Identification Management Committee. It seems that China has become aware of the political implications of the Internet. The government already controls access to the Net through officially approved Internet service providers. This new committee only increases the power of the State by facilitating the identification of Internet users.

4 Action and Reaction

What are some of the tactics used by the government in the past years to attempt to quiet the Chinese people? How effective will these actions be on the Chinese Internet populous?

4.1 Web-sites

As mentioned above, China funnels most of its Internet's web service through several central locations. In doing so, it is able to block out key web-sites that the government believes is not appropriate for its citizens.

The normal Internet user (with very little know-how) may utilise a tool called a proxy server. While others may just make a long distance call to a neighbouring country and use an alternate service provider.

4.2 E-mail

Action taken by the government may extend only as far as a deterrent to individuals. They may make examples of people like Hai, and companies like CFI to spread fear, uncertainty and doubt (*fud*).

Luckily e-mail is very secure and virtually anonymous. Additionally, hacker organisations like Cult of the Dead Cow, 2600, and Hackers Defence Fund are funding, or creating software that may *plug-in* to easily encrypt, obfuscate, and deliver “sensitive” materials blocked by the government.

4.3 Newsgroups

China has completely blocked all newsgroups. This seems to make sense, after all, China doesn't allow freedom of speech (as we see it), and newsgroups are all about free discussions of everything. The best a user in China can do, is dial out to another service provider in another country.

4.4 Propaganda

Beijing has used the Internet, however, to foster its own image. To spread propaganda to the outside world about itself. It has initiated such sites as: a human rights site, educational centre site. Hacktivism may be used in this case, to combat these sites.

5 Conclusion

It's readily apparent that the Chinese government has some major hurdles to overcome if they are going to be a part of the global market. The advances in technology are making it more and more difficult for China to keep their people isolated from the rest of the Internet. Within the next five to ten years, China will have to learn to adapt to the global market, or wither from neglect, as other countries run circles around them, both technologically and socially.

References

- [1] “China plays Net nanny” *BBC World News*.
{http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_278000/278452.stm}
(31 May 2000).
- [2] “China ‘Standardises’ Web News” *Wired News*.
{<http://www.wired.com/news/politics/0,1283,35825,00.html>}
(31 May 2000).
- [3] “Chinese Crypto Regs? Whatever!” *Wired News*.
{<http://www.wired.com/news/politics/0,1283,33992,00.html>}
(31 May 2000).
- [4] “Dissent on the Internet” *BBC World News*.
{http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_227000/227994.stm}
(31 May 2000).
- [5] Einhorn, Bruce. “A Web Site Feels the Wrath of Beijing.”
Online Asia.
{<http://www.businessweek.com/bwdaily/dnflash/may2000/nf00522b.htm>}
(31 May 2000).
- [6] Krog. “Another Straw on the Camel’s Back.” *Censorship In China*.
{<http://slashdot.org/comments.pl?sid=00/05/24/1338225&cid=12>}
(31 May 2000).
- [7] Mcc. “Re: Difference.” *Censorship In China*.
{<http://slashdot.org/comments.pl?sid=00/05/24/1338225&cid=98>}
(31 May 2000).
- [8] Muldrake. “Infowar on China inevitable.” *Censorship In China*.
{<http://slashdot.org/comments.pl?sid=00/05/24/1338225&cid=15>}
(31 May 2000).
- [9] “Net Dissident Appeals.” *BBC World News*.
{http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_275000/275296.stm} (31 May 2000).

- [10] “Online boom for China” *BBC World News*.
{http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_609000/609971.stm} (31 May 2000).
- [11] “Routing round Chinese Walls” *BBC World News*.
{http://news.bbc.co.uk/hi/english/sci/tech/newsid_228000/228030.stm}
(31 May 2000).