

Anonymity and Privacy Behind “Golden Shield,” Communist China’s Internet Firewall

Suman Srinivasan srs2117@columbia.edu

Computer Science Department, Columbia University

Submitted for COMS6184: Anonymity and Privacy in Computer Networks

Abstract—Under the Chinese Communist Party (CCP), Mainland China today has the world’s most monitored and filtered Internet system that violates the most fundamental privacy rights of its citizens. While some other countries around the world, such as those in the Middle East, do employ Internet filtering, the depth and degree to which the Communist Party monitors and filters Internet access and punishes those who violate its strict framework makes it the regime that most violates the privacy, anonymity and human rights of its “netizens.” This paper details how the Chinese Communist Party controls the Internet and employs various methods of legal, political and technical means to violate the privacy and anonymity of its citizens in order to enforce its information control.

Index Terms—Internet, China, Golden, Shield, Monitoring, Censorship, Privacy, Filtering

I. INTRODUCTION

China today has the world’s most complex Internet monitoring system. Internet monitoring and filtering are applied through a gamut of different techniques: legal, political and technical. The Communist regime has also gotten cooperation from service and equipment providers, both local and foreign, to help monitor and censor Internet traffic.

This paper shows how privacy and anonymity of all of China’s citizens are violated simply so that the Communist regime can track cases of dissent in political and spiritual circles. While some countries filter

websites or websites with “inappropriate” information or hate speech, China is one of the few countries where the focus of Internet censorship is on political websites that criticize the Communist Party - or spiritual websites - belonging to groups that are banned by the Chinese Communist Party (CCP).

This paper shows examples of how the CCP blocks such information that it deems “dangerous” (mostly to itself), monitors and arrests those who attempt to access it and how exactly it successfully pulls off privacy violations to such a large degree.

Section II and III of the paper give legal and political background about Internet monitoring in China. A subsection of Section III discusses what exactly is filtered in China. While not directly related to privacy concerns, it hopefully provides a better understanding of why Internet monitoring has been set in place by the Chinese Communist Party.

Section IV details the technical history of Internet monitoring in China and how and when the Communist regime started patrolling the Internet and monitoring online voices of dissent. A subsection also details how the Communist regime has exported its persecution, including electronic filtering and monitoring, worldwide and possibly used Trojans to electronically monitor dissenters outside China.

Sections V to VII are more technical and relate more to filtering, but they nonetheless provide vital details on where exactly the Communist Party has implemented its technical solutions for filtering Internet traffic. All these vanguards can also be used to violate online privacy. Section V describes the infrastructure of the Chinese Internet, and how large network hardware and companies and web service providers have colluded with the Communist Party to enable it to monitor its own citizens. Section VI describes packet and e-mail filtering.

Section VII discusses DNS and possible root server hijacking in the Chinese Internet.

Section VIII, entitled “A New Hope”, looks at the use of proxy servers, which even though banned and hard-to-get, still provide Chinese users a means of getting around the Internet blockade and avoiding Big Brother. It also takes a detailed look at two of the “Three Musketeers” (as they are known in China): UltraReach [22] and Freegate [23]. Both are software that are extremely user-friendly and enable Chinese users to get around monitoring and Internet filtering, and are being widely deployed at the grassroots level across China. The section also briefly discusses Phiphon [24], anti-censorship software developed at University of Toronto’s that has been in the press recently.

II. LEGAL BACKGROUND

Contrary to the belief of many that the CCP is cracking down on Chinese citizens’ freedom of speech and belief in accordance with its “own law”, it is actually violating its own constitution by doing so. All the actions that the Chinese Communist Party is undertaking in cracking down on dissidents and free speech on the Internet are unconstitutional; they violate the current constitution that former CCP leader Deng Xiaoping signed in 1982. [1] This is, however, not dissimilar to how the Communists in the former Soviet Union and Eastern Europe also violated their own constitutions to crackdown on dissenters.

The Constitution does indeed provide Chinese citizens with basic rights as follows:

Article 36 states that “Citizens of the People’s Republic of China enjoy freedom of religious belief. No state organ, public organization, or individual may compel citizens to believe in, or not to believe in, any religion; nor may they discriminate ...”

Article 35 proclaims that “citizens of the People’s Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession, and of demonstration.”

Article 5 states that “All state organs, the armed forces, all political parties and public organizations, and all enterprises and undertakings must abide by the Constitution and the law. All acts in violation of the Constitution and the law must be looked into.”

But Article 5 is never followed: the CCP rules the country making it a police state. With control over all media and political power centered in what is called *yi yan tang* — “One Hall, One Voice” — all rights and privileges can be violated in order to support “rule of law” and “Party stability.”

CCP does give itself some legal support in Article 2: “All power in the People’s Republic of China belongs to the people. The organs through which the people exercise state power are the National People’s Congress and the local people’s congresses at different levels.” And in Article 5, “The People’s Republic of China practices ruling the country in accordance with the law and building a socialist country of law.”

In Section IV, further details are given on the history of legal legislations that made it “legal” for the CCP to monitor Internet traffic through a variety of means.

III. POLITICAL BACKGROUND: WHAT IS FILTERED IN CHINA

A. What is Censored in China?

This section details studies of what content is filtered in China. It shows that Internet censorship inside China itself is not focused on what would traditionally be considered “harmful”, unethical or hate-speech websites; instead, censorship is focused on websites that are critical of the political and human rights situation in China. This also relates to monitoring and privacy considerations, as it shows exactly which groups are most targeted by the CCP.

A 2004 study by a group at Harvard University’s Law School [2] found that filtering of pornographic content in China was minimal: it found that only 101 out of 752 (13.4%) tested pornographic sites were blocked in China. The same study found that Saudi Arabia had blocked 695 (86.2%) of those sites, while commercial web filtering applications blocked around 70% - 90% of those sites.

In a January 2006 testimony to the US House of Representatives [3], Dr. John Palfrey, director of the Berkman Center for Internet & Society of Harvard University’s Law School, detailed the most censored websites in mainland China. A small reproduction of the results follows.

- Political content (90% of The Nine Commentaries, and 82% of sites tested with a derogatory version of Jiang Zemin’s name were blocked);
- The Falun Gong spiritual movement (44 – 73% of sites tested, in both English and Chinese languages);
- The Tiananmen Square protest of June 4, 1989 (at least 48% of Chinese-language sites tested, and 90% of sites related to the search term “Tiananmen massacre”);
- Independence movements in Tibet (31% of tested Chinese-language sites), Taiwan (25% of tested Chinese-language sites) and,
- Virtually all content on the BBC’s web properties

and much of the content published online by CNN.

In March 2006, a report on the Falun Gong website ClearWisdom.net [4] reported that the word “Sujiatun” was being blocked in cell phone messages. Sujiatun refers to the first of the concentration camps that were exposed in which organs were being harvested from living Falun Gong practitioners.

In short, the main focus of Internet filtering by the CCP does not seem to be oriented at blocking pornography or other potentially “harmful” websites that other countries usually filter: instead, the focus of the filtering appears to be dissident viewpoints, news sources that do not toe the Ministry of Propaganda’s line, or publications that are critical of it.

B. Political Background for the Communist Party’s Strict Monitoring and Censorship

Why does the Chinese Communist Party monitor and censor Internet traffic, or in a broader sense, free speech?

In order to explain this, a short note about the publication “Nine Commentaries on the Communist Party” mentioned at the beginning of the censored list is in order. The “Nine Commentaries,” first published in Chinese in November 2004 by the Chinese edition of *The Epoch Times* newspaper, is a searing expose of the little-known crimes committed by the CCP before and after it seized power in China in 1949. First published as an editorial series and now as a book, the “Nine Commentaries” has generated a lot of intense discussion since its publication. One thing that it has achieved is that it has led to close to 10 million people to resign from the CCP in protest of its violent history [5].

This explains the nature of the content the CCP filters and the particular groups and content that are being monitored.

It is freedom of expression that the CCP fears; this is the reason why the “Nine Commentaries” are the most heavily censored material in China today, even above Falun Gong and democracy.

The focus of monitoring, and hence privacy violations, is on spiritual groups and political dissidents who hold different and even critical views about the CCP. This is because it wants Chinese citizens to believe its disinformation.

This is what the CCP wants to control: the mind of its citizens, and why it monitors and violates the privacy and human rights of those who believe differently.

IV. HISTORY OF INTERNET IN CHINA

A. Web of Surveillance

When the Internet first entered China in 1995, it was filtered, but barely. It was reported that occasionally one could even access the Voice of America websites.

But in October 2000, around a year after that persecution of the spiritual group Falun Gong began, the CCP ordered ISPs to hold Chinese Internet users’ data – including phone numbers and surfing history – for 60 days. [6]

In January 2001, the Internet transfer of “state secrets” was prohibited by law. In March 2001, chat rooms were required to begin self-censorship of content on their forums. These laws were the first draconian laws passed that would lead to the arrests of Internet dissidents later. It was perhaps no coincidence that the number of Falun Gong practitioners being arrested for using the Internet to access Falun Gong websites increased right after these laws became binding.

In a particularly tragic case, in January 2001, Jiang Yonghong, a 34-year old engineer at Chengdu, was arrested at an Internet kiosk for viewing a Falun Gong website [7]. He was sentenced to forced labor; but was beaten to death in a detention center before he could serve his sentence. Two months later, the first democracy activists using web were arrested.

Gutmann [6] also details how e-mail sent to Tibet would take 3 days and e-mail about Falun Gong was completely “eradicated.”

In March 2002, the CCP started requiring all Internet companies to sign a “self-pledge” document to not post information that would not “jeopardize state security or disrupt social stability.” 300 Chinese companies - and Yahoo! – were the first to sign on.

In China, the most common way to get on the Internet, especially for the great majority in the rural area, is to use Internet kiosks. A ClearWisdom.net article [8] further documents how censorship in China’s Internet kiosks, chat rooms, etc works.

For example, in 2002, all Internet cafés were also forced to install “Internet café management software,” which automatically records URLs accessed in the past 60 days. Kiosks were required to ask users to use IC cards to access the Internet. The IC cards record the name, address, ID card number and other personal information of every Internet user.

The CCP also deploys a huge Internet police force, whose only duty is to look at posts on chat rooms and BBSs and remove posts that do not conform to political or spiritual guidelines laid out. Give enough information

from the BBS or website owners, the police force may also perhaps arrest the one who made the post.

It is estimated that around 40,000 police monitor China's Internet forums and BBSs [9]. In addition to these, BBS owners and chat room hosts are also required to voluntarily spend time on filtering traffic on their sites and tip off authorities in case there are postings that are not allowed.

B. Attacking and Monitoring Computers Outside China

"You've Got Dissent!" a book published by the non-profit Rand Corporation [10], provides excellent details and insight about the history of the Internet in China, how Internet censorship works, as well as how the CCP has used the Internet to attack and monitor groups that do not conform to its ideals.

The book goes into great detail about how the CCP has tried to stop free speech over the Internet, and highlights the case of Falun Gong and the persecution of the spiritual practice [10].

You've Got Dissent also documents how Falun Gong websites outside of China were attacked by DDOS attacks and brought down.

In April 2000, attacks made to the US Falun Gong website had command files replaced with Trojan-horse rigged binaries for later penetration, but this attack was rebuffed. In May 2000, the Australian website was hacked.

Hacking attempts are still commonplace; the author was present at – and was able to save traces of – a hacking attempt at an anti-persecution project he volunteered at. The distributed denial-of-service attack was trapped by the router, but Internet access at the site was severely hit. Around 70-80% of the traffic originated from China, a fact verified by IP addresses and a quick lookup on www.ip2location.com. Luckily, the attack was redirected and no major harm was done (or at least found.)

Further, evidence points to the fact that the CCP has been successful in installing Trojans and keystroke logging programs in the websites of Falun Gong practitioners and dissidents outside of China to monitor their activities. While this cannot be proven yet, the author has heard of several cases where keystroke loggers installed on computers were sending information back to servers in China that were probably collecting data about activities.

C. Stealing of Information through Physical Attacks on Persons and Equipment outside China

The CCP has also extended its persecution to using physical attacks on persons and equipment outside China

in its attempt to monitor computer information and block websites

On March 8, 2006, Yuan P Li, Chief Technical Officer of The Epoch Times, was beaten in his own home [11]. Only his computers were stolen, indicating that the attackers had their sights on particular computer security information; information they had been unable to hack. Yuan Li was one of those who was at the forefront of helping Chinese citizens work around the Internet firewall and monitoring to access websites blocked by the Chinese Internet.

This is not a form of Internet monitoring; however it does show how far the Chinese Communist Party is willing to go: from stealthy approaches like Internet censorship or hacking to breaking into a hacktivist's house and stealing his computer in order to halt the flow of free information on its Internet.

V. PHYSICAL LAYER CENSORSHIP

A. How the Censorship Works

The June 2005 issue of IEEE Spectrum was focused on China's rapid growth. A whole article in this feature was devoted to Internet monitoring in China and how it works [12].

"China's Internet is the most efficiently censored in the world," the article says, and then it goes into great technical detail about the various means by which China's leaders monitor and control the Internet.

For one, the article details how upon detecting online activities that amount to dissent, the CCP can give an order to the telecom companies to detect the server where such activity is going on, halt server activities, confiscate the server and arrest the people involved.

What about information that is hosted outside the country? China's Internet, like that of most other countries, flows through a series of routers. It talks about a highly centralized system, with three layers of router interconnection in ring-like fashion. The innermost ring consists of core routers in 8 cities which provide the only connection to outside world. In the middle ring sits a Metropolitan Area Network. On the outermost ring are all the remaining routers.

The CCP controls core routers and hence all international traffic. These are the key points at which information hosted internationally can be blocked.

China has awarded contracts for these routers to four companies: Huawei Technologies, Alcatel, Cisco and Juniper. Two of these companies – Cisco and Juniper – are responsible for installing the core backbone routers and the edge routers respectively. There have been

claims made (with substantial proof) [6] that Cisco has taken great pains to modify its firmware to filter and detect packets, suitable to the Communist government's tastes.

Gutmann [6] in his book "Losing the New China" also provides proof: scanned brochures brought in from the China Information Infrastructure Expo in December 2002 where Cisco touted that "a Chinese policeman or PSB agent using Cisco equipment can remotely access the suspect's danwei or work unit, thereby accessing reports on the individual's political behavior and family history."

Even though Cisco vehemently denies that it built routers that can perform specialized monitoring and filtering as Gutmann details in his book, a student project at the University of Toronto [13] examined the core router that blocked traffic to a human rights organization, Human Rights Watch (Figure 1). By fingerprinting the router using the nmap program (Figure 2) to find open ports, the authors found that the router was indeed a Cisco router.

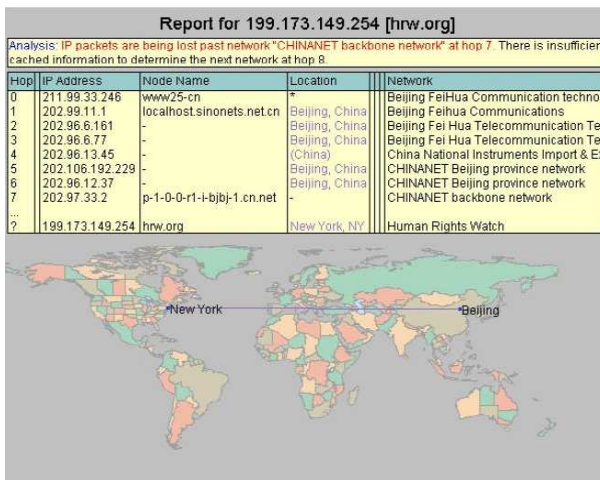


Figure 1: ProjectC attempted to connect to the Human Rights Watch website through a proxy in China. They found the address of the router that was restricting access to that website.

Port	State	Service
137/tcp	filtered	netbios-ns
138/tcp	filtered	netbios-dgm
139/tcp	filtered	netbios-ssn
2001/tcp	open	dc
4001/tcp	open	unknown
6001/tcp	open	X11:1
9001/tcp	open	unknown

Figure 2: A nmap lookup of the China core router that blocked the Human Rights Watch website. The fingerprinting revealed that the router is a Cisco router.

In the early days, censorship used to be done by simply having a list of blocked IP addresses [12]. Nowadays, experts believe that there is a proxy server

that intercepts requests to a domain name server and returns false information, thereby preventing the user from getting a correct response from the server.

However, one of the claims in IEEE Spectrum – that China does not implement packet-level filtering – does seem to be mistaken.

VI. PACKET AND E-MAIL FILTERING

In his presentation at fifth HOPE (Hackers on Planet Earth) conference in 2004 [14], Bill Xia of Dynamic Internet Technology (DIT) presented a bleak and detailed model of how China censors the Internet. He showed examples of how filtering of the Chinese Internet was done at all levels: IP, TCP, UDP and DNS.

IP blocking:

traceroute www.cctv.com.cn

From a regular machine:

```
5 sl-st20-dal-14-2-1620xT1.sprintlink.net (144.232.8.121) 7.374
ms 7.742 ms 7.197 ms
...
9 sl-bb23-ana-15-0.sprintlink.net (144.232.1.165) 39.139 ms
38.490 ms 38.527 ms
10 sl-gw23-ana-10-0.sprintlink.net (144.232.1.154) 38.303 ms
38.422 ms 38.475 ms
11 sl-chinnet-2-0.sprintlink.net (160.81.205.194) 214.290
ms 238.212 ms 244.824 ms
12 219.158.3.29 (219.158.3.29) 220.942 ms * 275.378 ms
13 202.96.12.46 (202.96.12.46) 282.376 ms 277.398 ms 218.399
ms
14 * RTR-HJL-A-S2-0.bta.net.cn (202.106.192.162) 242.801 ms
240.538 ms
15 202.108.46.26 (202.108.46.26) 241.794 ms 298.948 ms
235.100 ms
16 202.108.250.1 (202.108.250.1) 223.403 ms 228.272 ms
251.683 ms
```

From a blocked IP:

```
6 sl-st20-dal-14-2-1620xT1.sprintlink.net (144.232.8.121) 9.067
ms 7.686 ms 7.601 ms
...
9 sl-bb25-ana-8-0.sprintlink.net (144.232.9.64) 39.365 ms 38.688
ms 38.675 ms
10 sl-bb23-ana-15-0.sprintlink.net (144.232.1.165) 38.740 ms
38.589 ms 38.553 ms
11 sl-gw23-ana-10-0.sprintlink.net (144.232.1.154) 38.534 ms
38.323 ms 38.289 ms
12 * * *
13 * * *
```

Figure 3: A traceroute to the Chinese TV CCTV's website. This is from a demonstration from Bill Xia from DIT at HOPE 2004, New York. This shows the route from blocked and unblocked IP addresses; the blocked IP address did not see any replies as soon as it hit the periphery of China's national Internet.

The IP address filtering is a common way of filtering. By trying to access a site inside China (from a blocked and unblocked node,) Bill was able to show (Figure 3) how the packets from an unblocked node were able to get into China, but the packets from the blocked node

were stopped at the international gateway.

Xia further made the point that 18 Gbps of traffic was flowing through the routers, and that someone (Cisco) must have helped the regime since such intense filtering had to be done by the routers.

Xia went on to show how TCP packets are hijacked. When sending GET requests for certain keywords and URLs, he found that he was blacklisted and could not access the Internet for 20 minutes after that. He argues that such filtering is possible only by inspecting the contents of the TCP packets and must be based on keyword filters. UDP packets were also shown to have been hijacked.

Another study was undertaken by OpenNet Initiative in August 2004 [15] to study search engine filtering. The study established how packet filtering was employed in Chinese search engines. A sample session is shown in Figure 4.

```
$ telnet 202.43.217.94 80
Trying 202.43.217.94...
Connected to 202.43.217.94.
Escape character is '^]'.
GET /falun HTTP/1.0
Connection closed by foreign host.
```

Figure 4: A telnet connection to yisou.com shows how any packets sent to yisou.com with banned keywords were disconnected from the server.

As shown in the figure, the connection is simply lost. No HTTP headers are sent after the server sees the banned keyword. Furthermore, access is blocked for quite some time.

The study did packet traces to find out what was happening. They found that a RST packet was being sent back to the user. The server then advertised a ZeroWindow size. No request transmission could be made until the server advertised a non-zero window size.

Source	Destination	Protocol	Info
128.100. x.x	202.43.217.94	TCP	4572 > http [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 TSV=4309780 TSE=0 W=0
202.43.217.94	128.100. x.x	TCP	http > 4572 [SYN, RST] Seq=0 Acl=1 Win=5535 Len=0 MSS=1460 WS=1 TSV=9768541 TSE=4309780
128.100. x.x	202.43.217.94	TCP	4572 > http [RST] Seq=1 Acl=1 Win=5840 Len=0 TSV=43097914 TSE=9768541
128.100. x.x	202.43.217.94	HTTP	[TCP Retransmission] GET /falun HTTP/1.0
202.43.217.94	128.100. x.x	TCP	http > 4572 [RST] Seq=1 Acl=289354726 Win=2 Len=0
202.43.217.94	128.100. x.x	TCP	[TCP ZeroWindow] [TCP Dup ACK 641] http > 4572 [RST] Seq=1 Acl=293254726 Win=0 Len=0
202.43.217.94	128.100. x.x	TCP	[TCP Dup ACK 642] http > 4572 [RST] Seq=1 Acl=289354726 Win=2 Len=0
202.43.217.94	128.100. x.x	TCP	[TCP Dup ACK 643] http > 4572 [RST] Seq=1 Acl=289354726 Win=2 Len=0
202.43.217.94	128.100. x.x	TCP	[TCP Dup ACK 644] http > 4572 [RST] Seq=1 Acl=289354726 Win=2 Len=0
202.43.217.94	128.100. x.x	TCP	[TCP Dup ACK 645] http > 4572 [RST] Seq=1 Acl=289354726 Win=2 Len=0
202.43.217.94	128.100. x.x	TCP	[TCP Dup ACK 646] http > 4572 [RST] Seq=1 Acl=289354726 Win=2 Len=0

Figure 5: Screenshot from an OpenNetInitiative paper showing packet traces while trying to connect to yisou.com search engine with a banned keyword. The server sent a RST packet and advertised a ZeroWindow size connection to disconnect the remote user who typed that banned keyword.

VII. DOMAIN NAME AND ROOT SERVER HIJACKING

The scariest part of Bill Xia's presentation at HOPE

was probably not the fact that IP addresses were blocked, or even that TCP and UDP packets were filtered. Xia showed that DNS domain names could be hijacked.

In October 2002, DIT found that several websites' DNS addresses had been "hijacked" [16] – a process in which the domain names were made to point to blocked IP addresses. The study found that such domain name spoofing had been deployed all across China's national level backbone routers.

The records of most popular forbidden sites redirected to single IP address, blocked in China at international gateway level. The address chosen was 64.33.88.161, the website for falundafa.ca.

Why was this address chosen? It was because this address is blocked at international gateway. Previously, blocked websites would switch their IP address, enabling them to circumvent filter. Now, they would all have to resolve to one certainly blocked website.

This technique gained notoriety in September 2002, when Google users in mainland China were redirected to other Chinese search websites [17].

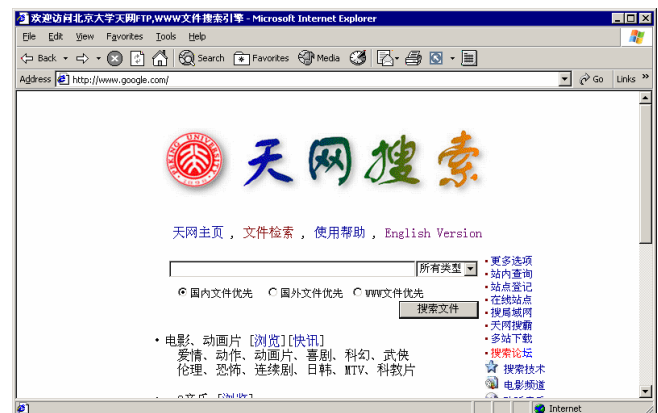


Figure 6: A screenshot taken in September 2002 shows how Chinese visitors to Google were redirected to one of China's search engines

Domain name spoofing does not only achieve censorship of the Internet, but it also leads to misinformation, since the user typically gets a response saying that the file does not exist, while in fact, he or she was being directed to a wrong IP address that had no correspondence to the domain names.

In February 2004, responding to reports [18] that Verisign was planning to deploy a DNS constellation in Beijing, DIT further warned that the consequences of deploying a root server in Beijing could be disastrous – not only would Chinese users be unable to access banned sites, but now users from around the world (especially in regions close to China) would not be able to access those banned sites since their DNS requests

would not resolve properly.

However, there are already two root name servers in Beijing, operated by ISC (2003) and Autonomica (2005). Last year at the World Summit on Internet Society in Tunisia, the US had to fight back bid (led by China) to wrest root server ownership from ICANN

A thread on the IETF mailing list [19] gives details on how China already has TLD-configured servers. One of the threads gives a summary of the situation:

“This is what the Chinese say. Users do not navigate anymore under the ICANN root. But they do not create a root. They just do not use a root anymore. This closes the dispute between authoritative and alternative roots.”

VIII. CONTENT FILTERING AND KOWTOWING

A. *Self-Censorship by Chinese and Foreign Websites*

Another big issue that has played a hand in contributing to Internet censorship in China has been the willingness of Western companies to toe the line of the CCP in censoring themselves.

Yahoo has recently been caught red-handed for its involvement in the arrests of two freelance journalists: Li Zhi in December 2003, and the more famous Shi Tao in September 2005.

Starting June 2005, MSN blocked bloggers from using the words “freedom”, “democracy” and “demonstration” in their online blogs.

Google was the most recent case of a company willing to sleep with the enemy. Google launched its Chinese site, Google.cn, in January 2006. Google.cn has been criticized for its intense blocking of results that contain banned keywords.

On February 15, 2006, representatives from Yahoo, MSN and Google were grilled in the hearing by the Committee on International Relations. [20] It is believed that Congress will follow up on this issue and put in some resources to combat the problem of Internet censorship in China, as well as Western companies kowtowing to the CCP.

On April 18th, 2006, Financial Times quote Skype's chief executive Niklas Zennstrom as saying in an interview that the company “had censored text messages containing words like “Falun Gong”.” [21]

IX. PROXYING: A NEW HOPE?

From previous sections, it is obvious that Internet monitoring and filtering is implemented at several layers of the technical framework. But is it possible to break through the firewall and escape being detected and monitored by such a powerful, global active adversary?

The most common answer for overcoming monitoring and filtering is to use proxy servers. Using proxy servers in mainland China is still possible to some extent, but the CCP has had more and more ways to try to filter them out.

Proxies were frequently in use before 2001. However, after 2001, proxies were more and more successfully blocked. The Internet police would just block advertised proxies, as well as websites advertising proxies. Triangle Boy was successfully blocked in 2001 when Voice of America sent Triangle Boy addresses in its e-mails to mainland China. [6]

If the user found a proxy and it was detected, that would be banned too. If users searched for proxy servers and found one, that would be quickly blocked. Thus, the censors were one step ahead of the surfers.

But dissidents — and Falun Gong — are working around it to give Chinese people a chance to look at news from outside the mainland by developing and deploying easy-to-install software that functions as an advanced proxy service to bypass the Chinese filtering and monitoring system.

One of the most recent advances in this area has been the software UltraReach. This is described in some detail on their website at [22]. It does not rely on open-relay proxy, and the developers claim that it has survived IP blocking, DNS hijacking and DOS attacks.

The software itself is a proxy, and it runs as a plugin for Internet Explorer. The author downloaded and tested the software. The program was just one single executable file that was 200 KB in size and required no installation. Upon running it, it presented the user an option screen from which he could choose which p

The author further performed packet traces of UltraReach by using a packet analyzer called Ethereal. From the packet traces, it appears that Ethereal connects to servers in countries around the world in the background, without user intervention. It allows one to browse the Internet using the proxies, while looking for proxies in background and changing proxies frequently.

UltraReach appears to exchange information using encrypted packets to proxy servers on different ports. Further, it seems to change proxy servers frequently and connect to websites through these.

Freemate [23] and Psiphon [24] are two other proxy servers that are used to overcome the Chinese Internet monitoring. Freemate, developed by Dynamic Internet Technology, is software that has been tried and tested and is reputed to be easy to deploy.

Psiphon is a project under development in the University of Toronto's Citizen Lab. It works similar to

Freagate and UltraReach, except that instead of employing discrete means to advertise proxies, it works through building a trusted peer network between diasporas overseas and their relatives in mainland China.

X. CONCLUSION

In this paper, I have attempted to provide some details about the vast array of means by which the Chinese Communist Party censors and clamps down on the Internet inside China. The paper shows that the censorship exists solely to protect the sovereignty of the Party and monitor those who attempt to work outside its boundaries.

ACKNOWLEDGMENT

I would like to thank Bill Xia of Dynamic Internet Technology for his advice as well as providing helpful pointers to places where I could find out more about Internet censorship in China.

REFERENCES

- [1] Constitution of the People's Republic of China, http://www.oefre.unibe.ch/law/icl/ch00000_.html
- [2] Zittrain, Edelman, *Emperical Analysis of Internet Filtering in China*, <http://cyber.law.harvard.edu/filtering/china/>
- [3] John G. Palfrey, Jr., *Testimony to the US House of Representatives Committee on International Relations*, [http://blogs.law.harvard.edu/palfrey/stories/storyReader\\$1063](http://blogs.law.harvard.edu/palfrey/stories/storyReader$1063)
- [4] ClearWisdom Net, *CCP Fears its Crimes Being Exposed - "Sujiatum" Becomes a Blocked Word*, <http://clearwisdom.net/emh/articles/2006/3/31/71380.html>
- [5] The Epoch Times, *Nine Commentaries on the Communist Party*, <http://www.ninecommentaries.com/> (English)
- [6] Ethan Gutmann, *Losing the New China*, Encounter Books, 2003
- [7] Falun Dafa Information Center, *Police Brutality Claims Four More Falun Gong Lives in China*, <http://www.faluninfo.net/displayAnArticle.asp?ID=5328>
- [8] Yuan Ye, *Exposing the Illegal Monitoring of the Internet by the Public Information Internet Monitoring Bureau*, <http://clearwisdom.net/emh/articles/2004/6/12/49130.html> ClearWisdom Net
- [9] Yale Global Online, *China's 'Big Mamas' in a Quandary*, <http://yaleglobal.yale.edu/display.article?id=3676>
- [10] The Epoch Times, *Epoch Times Chief Technical Officer Beaten in His Own Home*, <http://www.theepochtimes.com/news/6-2-9/37956.html>
- [11] Chase, Mulveron, *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies*, Rand Foundation, 2002 http://www.rand.org/pubs/monograph_reports/MR1543/index.html
- [12] S.Cherry, *The Net Effect: as China's Internet gets a much-needed makeover, will the new network promote freedom or curtail it?*, IEEE Spectrum, June 2005
- [13] Nart Villeneuve, *Project C*, <http://www.chass.utoronto.ca/~citizenl/assets/articles/ProjectC-r1.pdf>
- [14] Bill Xia, *How the Great Firewall Works*, HOPE 2004, <http://www.dit-inc.us/report/hope2004/cover.htm>
- [15] OpenNet Initiative, *Probing Chinese search engine filtering*, <http://www.opennetinitiative.net/bulletins/005/>
- [16] Dynamic Internet Technology, *Forbidden sites hijacked all over China*, October 2002, <http://www.dit-inc.us/report/hj.htm>
- [17] Berkman Center for Internet and Society, *Replacement of Google with Alternative Search Systems in China: Documentation and Screen Shots*, <http://cyber.law.harvard.edu/filtering/china/google-replacements/>
- [18] InfoWorld, *VeriSign to deploy Internet hub in China*, http://www.infoworld.com/article/04/02/19/HNverisignchina_1.html
- [19] Jefsey Morfin, *Beyond China's independent root-servers -- Expanding and Fixing Domain Notation*, <http://www.mhonarc.org/archive/html/ietf/2006-03/msg00038.html>
- [20] Fortune magazine, *Tech execs get grilled over China business*, http://money.cnn.com/2006/02/15/news/international/pluggedin_fortune/index.htm?cnn=yes
- [21] Financial Times, *Skype Says Text Messages Are Censored In China*, <http://news.ft.com/cms/s/875630d4-cef9-11da-925d-0000779e2340.html>
- [22] Ultrareach software, <http://www.ultrareach.com/>
- [23] Freegate software, <http://www.dit-inc.us/>
- [24] Psiphon software, <http://www.citizenlab.org/>

Suman Srinivasan is a 25-year old Electrical Engineering PhD student at Columbia University in the City of New York. He has a MS in Electrical Engineering from the University of Florida, Gainesville, and a BE in Electronics and Communication Engineering from the University of Madras, India. His area of research is in a wide area of topics in computer networking.

Suman has also interned with Mammatech Corporation in Florida, where he helped develop software that would teach doctors how to detect breast cancer through tactile instruments.

Suman was a member of the IEEE Society while an undergraduate student at the University of Madras, India.