Great Firewall of China

CHAPTER · JANUARY 2014

READS
90

1 AUTHOR:

Fei Shen
City University of Hong Kong
33 PUBLICATIONS **119** CITATIONS

SEE PROFILE

Shen, F. (2014). Great Firewall of China. In Harvey, K. (Ed.). (2014). Encyclopedia of Social Media and Politics. SAGE, Volume 2, 599-602.

The Great Firewall of China

"The Great Firewall of China" (GFW or GFC) is a phrase coined by Charles R. Smith in 2002 to describe Internet censorship in China, where foreign "harmful" ideas are prevented from invading the authoritarian state to safeguard its one-party rule through filtering content as well as monitoring users online. The metaphoric term draws parallels between the world's most complex Internet control system and the Great Wall, magnificent ancient fortifications built to protect China proper from intrusions by nomadic groups. A firewall is a network security system that controls the flow of information that travels through a node. A common interpretation of the GFW refers narrowly to the inspecting, filtering, and blocking technologies deployed in the international gateways of Chinese Internet service providers (ISPs). Nevertheless, some use the term loosely to imply the whole set of legal, regulatory, and technical measures China has put in place for Internet censorship and control.

The GFW is operated by the National Computer network Emergency Response technical Team Coordination Center of China (CNCERT/CC) under the Ministry of Industry and Information Technology (MIIT). The chief designer of the project, Binxing Fang, dubbed as the father of the GFW by Chinese Internet users, is the president and a professor of Beijing University of Posts and Telecommunications. The GFW is often confused with the "Golden Shield Project (GSP)," a public security information technology project aiming to establish a nation-wide computer application and communication system for the police force. Both projects started in late 1990s, but the GFW is a tool of ideology control whereas the GSP is primarily used for crime prevention and investigation by the Ministry of Public Security (MPS). However, since Internet crime investigation and monitoring constitute a part of the GSP, it is possible that the GFW and the GSP overlap to a certain degree, but the relationship of the two projects remains ambiguous.

While CNCERT/CC oversees the daily operation of the GFW, CNCERT/CC is merely a technical and research organization that has little influence over censorship decisions. Orders of censorship (e.g., which website to block, which keyword to filter) primarily come from government institutions that wield stronger political power: the Central Propaganda Department, the State Council Information Office (SCIO), and the Public Information Network Security Supervision Department of MPS, etc. The hardware of the GFW is mainly produced by domestic information technology companies such as Sugon (Shuguang) and Huawei to ensure information security and to protect state secret. But quite a few American companies including Sun Microsystems, Cisco, Nortel Networks, 3COM, Websense and Bay

networks of California have all been implicated in sales of web filtering and monitoring technologies to China. The OpenNet Initiative's 2004-05 report on Chinese Internet filtering claims that the backbone of China's Internet relies on Cisco technology.

The general philosophy of Internet control in China is to territorialize domestic computer networks into a large national intranet whose connections to the rest of the world are funneled through a few major Internet service providers. The international gateways are located in three metropolitan areas: Beijing, Shanghai, and Guangzhou. The largest two Chinese ISPs are CHINANET and CNCGROUP, owned by China Telecom and China Unicom respectively. According to findings from a series of empirical testing conducted by researchers from University of Michigan in 2011, CHINANET possesses 79.4% of the filtering interfaces and CNCGROUP possesses 17.4%. CHINANET has a mature filtering capability while CNCGROUP has been strengthening its infrastructure continuously. Most of the filtering devices are concentrated at border routers, but a small proportion of them are internal autonomous systems. This leads observers to suspect that the GFW also has the capabilities to monitor and filter domestic traffic. CNCGROUP places most of its filtering devices in the backbone but the majority of CHINANET's filtering devices belong to provincial networks.

Targeted content

A number of legislations have been introduced since mid-1990s to restrict the flow of web content that could endanger the rule of the Chinese Communist Party. The claimed purposes of Internet censorship in China are always vague and broad. Laws and regulations prohibit the production and dissemination of information containing content that endangers national security, divulges state secrets, subverts the government, undermines national unification, harm the honor and interests of the state, defames government agencies, instigates ethnic hatred, preaches cults or feudal superstitions, disturbs social order, encourages gambling, and shows pornography and violence, etc.

But in practice, the blocked websites roughly fall into eight categories: foreign social media platforms (e.g., facebook.com, youtube.com, twitter.com, blogspot.com, wordpress.com), foreign news sites (e.g.,nytimes.com, bloomberg.com, rfa.org), file sharing sites (e.g., thepiratebay.se, slideshare.net), overseas Chinese portal sites and discussion forums (e.g., 6park.com, wenxuecity.com, discuss.com.hk, uwants.com), dissident, prodemocracy, and human right sites (e.g., 64tianwang.com, beijingspring.com, www.amnesty.org), circumvention and anonymizer tools sites (e.g., anonymouse.org, torproject.org, openvpn.net), sites maintained by Falun Gong (e.g., epochtimes.com, aboluowang.com, www.ntdtv.com, etc.), and pornography and gambling sites.

The most heavily censored keywords are names of top leaders and dissidents, Falun Gong, and the 1989 Tiananmen Square crackdown. The blocked sites and filtered keywords are not fixed and tend to vary across time. For example, during the 2008 Beijing Olympics,

the government loosened Internet control by unblocking a number of sites including China Times, Mingpao, Wikipedia, and BBC, etc. In contrast, during politically sensitive periods such as the "two meetings" (the annual meetings of the National People's Congress and Chinese People's Political Consultative Conference), the government tends to tighten up the control.

Technical measures

To control the domestic network, the government has a large variety of legal and administrative measures at their disposal, including promoting self-regulation, deploying human censors and Internet police force, recruiting paid commentators, or even shutting down regional Internet connection when needed. Nonetheless, when it comes to dealing with content from international website, blocking and filtering are the only feasible choices. The Chinese authorities have never publicized any technical details of the Great Firewall, but researchers worldwide have conducted various empirical and technical studies of the GFW. The most frequently mentioned techniques are IP blocking, DNS manipulation, URL filtering, and keyword filtering.

IP blocking. IP (Internet protocol) blocking is the earliest form of filtering mechanism used in China. All international gateways of Chinese network are configured with a list of banned IP addresses – numerical labels assigned to computers connected to the Internet to indicate where the computers are. When users try to access a blacklisted address, the packets will be routed to a black hole server which then ignores the connection request. IP blocking is easy to implement, adding only a tiny work load to the gateway routers, however, it tends to "over-block" innocent websites. When a target is hosted on a server with multiple sites, all websites will be blocked as they share the same IP address. However, if a banned website move or copy its content to another server with a different IP address and keeps the domain name unchanged, the blocking can be circumvented (assuming the site is not banned through DNS manipulation) until the Chinese authority spot the new IP address and update their list.

DNS manipulation. Most people visit a website through typing its domain name into an Internet browser and a few would remember its IP address. The domain name system (DNS) is a database used to translate textual hostnames (e.g., www.facebook.com) into IP addresses (e.g., 173.252.110.27). In addition to the IP address list, the GFW maintains a list of banned domain names. When a router detects any pre-defined domain name queries passing through network traffic, the GFW will inject a forged IP address so that users will not be able reach the desired website or will be redirected to a wrong site. Almost all the DNS servers in China are polluted. When Google's search engine service was blocked in 2002, domestic requests to access Google.com were directed to Baidu.com.

URL filtering. A URL (uniform resource locator) is a string of characters representing a web address which usually consists of a protocol name, a domain name or IP address, and a

path (e.g., https://en.wikipedia.org/wiki/Falun_Gong). Requested URL string can be scanned for blacklisted keywords.

Keyword filtering. Keyword filtering (a.k.a, packet filtering), which occurs at the protocol level rather than at the network level, is more technically complex. When a connection between two computers are established through a three-way hand-shaking process, information wrapped in TCP segments will flow through a series of routers to reach their destinations. Routers use intrusion detection system (IDS) technology to inspect content contained in TCP packets for pre-defined keywords. When blacklisted keywords are spotted, multiple forged TCP reset packets (RST flag) will be sent to both ends to terminate the connection. Once activated, the blocking can last for a few minutes to an hour. Replying upon a set of keywords, packet filtering is more flexible than the aforementioned measures because it can dynamically cut out a connection without locating the originations of the information (e.g., domain name, IP address, URL, etc.) or blocking the whole website regardless of the content on individual pages. For example, both English and Chinese Wikipedia homepages are accessible in China at the time of writing. But when one tries to access the page of Wikipedia entry for Falun Gong (English: https://en.wikipedia.org/wiki/Falun_Gong; Chinese: http://zh.wikipedia.org/wiki/法轮功), it takes a long time to load a part of the page. When "refresh" or "reload" button is clicked, the connection is terminated.

Circumvention and Counter-measures

Despite its technical sophistication, the Great Firewall is not invincible. The two basic requirements to bypass the GFW are reliable proxy servers and encryption. A proxy can serve as an intermediary to relay information from the otherwise blocked sites and filtered pages to end users while encryption keeps keyword filtering from identifying "harmful" content in traffic streams. The common tools of circumvention include anti-censorship software, VPN (virtual private network), and SSH (secure shell). Most anti-censorship software (e.g., FreeGate, GoAgent, GTunnel, Ultrasurf, Psiphon, Tor, etc.) relies on open, free proxies but VPN and SSH use private hosts outside of China. Only a small fraction of tech-savvy Chinese users know how to get to the other side of the GFW. According to a non-representative online survey conducted in 2010, Internet users who use circumvention tools were predominantly young males with high levels of education, and FreeGate, Ultrasurf, and Psiphon were most popular in China because of their nontechnical features.

Circumvention tools are not invulnerable either. The GFW can detect and block proxy servers used for circumvention via analyzing Internet traffic, and recently, more sophisticated technologies have enabled the GFW to recognize encrypted protocols. Thus all circumvention tools have to seek technology innovation to stay up-to-date. The tug of war between Tor and the GFW serves as a good example. Tor started as an anonymous communication tool in 2002 and was used for circumvention by many Chinese Internet users. Tor used a centralized directory server which maintains a list of proxy nodes. However, when the IP address of the

directory server was blocked by the GFW, Tor became useless and lost its Chinese users. Tor came back to life through developing hidden "bridge" nodes that are not listed in the directory server, but the GFW learned the way to block hidden private bridge nodes subsequently in 2011. Yet in 2012, Tor launched a new product named obfsproxy, a tool that can transform the Tor traffic into innocent-looking traffic so that the GFW cannot differentiate the use of Tor from other Internet activities. It is possible that the GFW will soon find a way to defeat obfsproxy. The arms race between blocking and circumvention will never reach its end until China aborts the mission of Internet censorship.

Fei Shen
City University of Hong Kong

See Also: China (social media, unrest)

Further Readings

Anderson, D. (2012). Splinternet behind the Great Firewall of China. *Queue – Web Security*, Volume 10, issue 11, 40.
Clayton, R., Murdoch, S.J., & Watson, R.N.M. (2006). Ignoring the Great Firewall of China. *Privacy Enhancing Technologies, Lecture Notes in Computer Science Volume*, 4258, 20-35.
Xu, X., Mao, Z. M., & Halderman, J. A. (2011). Internet Censorship in China: Where does the filtering occur? *Passive and Active Measurement. Lecture Notes in Computer Science Volume*, 6579, 133-142.
Zittrain, J. & Edelman, B. (2003). Internet filtering in China. *Internet Computing IEEE*, 70-77.