The Great Firewall

Wenqi He

Georgia Institute of Technology

The Great Firewall

Introduction

When I took the SAT in Hong Kong in 2014, over a million people were protesting the NPCSC (Standing Committee of the National People's Congress) decision regarding the promised universal suffrage for the 2020 Chief Executive election, meanwhile, as I later found out, the vast majority of mainland citizens held the view promoted by Beijing that the Hong Kong protesters are extremists and separatists, despite not knowing the reasons for the protest.

Historians once believed that authoritarian regimes, which are characterized by such manipulation of public information, cannot survive the Information Age, when the cost of information access becomes minimal. But sophisticated Internet censorship systems such as the Great Firewall (GFW) of China have proven the issue far more complicated, as governments, as it turns out, are able to adapt and counter the challenges posed by emerging communication technologies.

Background: Internet Protocol Suite

Some consider the Internet inherently political, in the sense that its very essence is a collection of communication protocols that “control the global flow of information and make decisions that influence access to knowledge, civil liberties online, innovation policy, national economic competitiveness, national security, and which technology companies will succeed” (DeNardis, 2009, p. 10-11). In order to explain the workings of the GFW, which exploits the design of protocols—more specifically, the Internet protocol suite, otherwise known as TCP/IP—it is necessary to first give a technical overview of these protocols. (The following is loosely based on *Computer Networking: A Top-Down Approach* by Kurose and Ross.)

The Internet is a connectionless, packet-switched network, meaning that there are no dedicated communication channels and each message from a sender to a receiver is broken down into chunks that are delivered separately through a network of computers known as routers based on the destination address marked on the packets. IP (Internet Protocol) is the layer responsible for finding a “shortest” path from one host to the other—a process called routing—as well as relaying the packets through the network of routers. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are transport-layer protocols that work on top of IP. They specify source and destination port numbers which identify the two processes communicating with each other, such as a web browser and a web server. The main difference is that TCP establishes a reliable connection between the two hosts, while UDP does not. One top of transport-layer protocols are the application-layer protocols, such as HTTP (HyperText Transfer Protocol) for web browsing and SMTP (Simple Mail Transfer Protocol) for sending emails, both of which run on TCP, and DNS (Domain Name System) protocol, which runs on UDP.

Daily web browsing involves at least three steps: First, the client’s computer queries DNS servers to translate a human-readable domain name such as “google.com” to a machine-readable IP address such as “74.125.21.101”. With the server IP address, the browser then establishes one or more TCP connections with the server. If TLS is used, the client (browser) and server would then negotiate a cipher suite to encrypt the traffic. Finally, the browser sends an HTTP request through the established channel and the server responds with files encoding the web page. Since all steps in this process cannot succeed without the cooperation of all routers between the two hosts, there are various ways to disrupt the communication.

Censorship Mechanisms

Despite often touted as a decentralizing and democratizing force, the Internet, through the oligarchy of ISPs (Internet service providers)—that is, the control of most people's access to the public networks by a handful of ISPs in each country—lends itself towards authoritarianism as governments can gain control over the entire network by just controlling the big ISPs.

It is believed that the GFW is deployed using optical splitters at the international gateways of China's major ISPs, such as China Telecom and China Unicom (Xu, Mao, & Halderman, 2011). By duplicating optical signals, the GFW is able to copy each packet and examine its metadata such as IP addresses and TCP ports and use DPI (deep packet inspection) to analyze data content from streams of packets. (Bu, 2013)

DNS and TCP Reset Injection

If DPI detects blacklisted domain name in a DNS query, a fake DNS response is injected, which would most likely reach the sender (client) ahead of the real response, causing the client to contact the wrong IP address. Moreover, due to the hierarchical structure of DNS servers and their caching mechanism, the spoofed response can pollute all downstream DNS servers.

Similarly, if blacklisted keywords are detected in TCP packet streams, the GFW injects a series of forged RST (reset) packets—RST is designed as part of the TCP protocol to signal that a connection cannot be established due to, for example, no process listening on the specified port—to both the client and the server, causing both hosts to terminate the connection. (Bu, 2013)

IP Blackholing

Routers forward packets—or simply ignore them, if the IP addresses and ports on the packet header match the special "null route"—based on its routing table in memory, which is computed from the routing information it receives from its neighbors through IGP (Interior Gateway Protocol) and BGP (Border Gateway Protocol). Compared to packet injection, which require active detection and intervention, the more cost-effective way the GFW uses to enforce censorship is to blackhole IP addresses by advertising through BGP messages null routes that capture these addresses. From the perspective of the routers that have been polluted by these null routes, the servers are unreachable as if they don't actually exist. (Bu, 2013)

Circumvention Methods

Encryption

Most web browsers and websites nowadays enforce HTTPS by default, so this usually does not require user action. In HTTPS, the HTTP traffic is protected by the underlying TLS (Transport Layer Security) protocol that encrypts the entire HTTP packet, including the headers, rendering keyword detection impossible without a man-in-the-middle attack. However, the SNI (Server Name Indication) header field in TLS packets might still reveal the identity of the server.

Bypassing Packet Injection

Before the operating system sends out requests to DNS servers, it first looks for a text file called the "hosts file" in the file system (on UNIX/Linux systems the file path is "/etc/hosts"), which contains a mapping of host names to IP addresses. If the IP addresses of censored domains can be obtained without DNS, they can be added to the file so that the DNS resolver can work properly. One can also bypass DNS spoofing by manually setting the DNS server to one that's not polluted, such as Google's "8.8.8.8". RST injection is also evadable by ignoring all RST packets, but the server has to ignore RSTs as well. (Bu, 2013)

Proxy, VPN and Tor

The above two methods are only useful when the IP address is not blackholed. Evading IP blocking is much more challenging, since any protocol-conforming router would simply refuse to forward packets directed at the blackholed addresses. The only solution in this case is to proxy the traffic—that is, to relay the communication through a reachable intermediary, such as (a) an HTTP proxy, a SOCKS proxy (such as Shadowsocks) or an SSH server that acts as a SOCKS proxy using dynamic port forwarding; (b) a VPN server, which establishes an encrypted tunnel through the public Internet to a private network located outside the firewall; (c) Tor (an acronym for "The Onion Router"), which routes packets through multiple relay nodes, encrypting the packets at each hop, thereby creating nested layers of encryption (hence the name “onion”). (Bu, 2013)

According to Lee (2018), the GFW was able to identify and blackhole VPN servers and Tor relays using active probing attacks. As a countermeasure, the Tor development team introduced pluggable transport protocols such as ofbs4, but these protocols turned out to be detectable and the GFW blocked them soon after.

Motivations and Justifications

Protection of Legitimacy

It is naive to simply describe China as Orwellian, despite apparent commonality. While Big Brother, as imagined by Orwell, arises from modernity itself rather than what precedes it, China’s politics is still largely a continuation of its *pre*-modern despotism (Wittfogel, 1955). Regardless, there is no dispute that the GFW is an attempt to protect the regime’s legitimacy.

As with most Communist Parties, the CCP (Chinese Communist Party) initially derived its legitimacy from the Leninist ideology, which asserts that liberal democracy in a capitalist society is in fact a dictatorship of the bourgeoisie, and therefore dictatorship of the proletariat, or its vanguard such as a Communist Party, is a necessary evil—no worse than democracy—to suppress the retaliation of the bourgeoisie during the transition towards a free and classless society. However, since the “reform and opening-up” in 1978, the CCP has officially abandoned Leninism, and without its ideological backing, the Party’s legitimacy becomes fragile, especially when the economic reforms resulted in a libertarian atmosphere during the 1980s. The military crackdown on the Tiananmen Square protest in 1989 amidst the collapse of Eastern Bloc regimes marked the end of the liberal era but also trapped the regime in a moral low ground.

Prevention of Collective Action

The rise and fall of Communism regimes illustrates how collective actions can be potentially subversive, regardless of the nature of the government. Information and communication technologies such as the Internet, Andrelczyk (2016) argues, are especially destabilizing in societies without formal channels of political participation such as elections because they enable horizontal communication and can therefore facilitate group mobilization and collectivization, as demonstrated in the Arab Spring and the 2014 Hong Kong protests.

Ultimately, what the GFW and many other censorship regimes seek to prevent is not necessarily anti-government speech, but information that might lead to collectivization of individuals who share interests and goals that don’t align with those of the authority (Olsen, 2017). In fact, after monitoring various topics on Chinese social media, King, Pan, and Roberts (2013) discovered that criticisms of the government might actually pass censorship as long as there is no obvious “collective action potential” (p. 2).

Legality of the GFW

Collective action potential is inherent to religions/cults, pro-democracy/independence movements, and a wide range of social activities. Specifically, the GFW censors foreign websites that contain contents that advocate (a) Falun Gong, a cult that started as a qigong group in the 1990s; (b) the Tiananmen Square protests of 1989; (c) independence of Taiwan, Hong Kong, Tibet and Xinjiang—all of which involve organizations and activities that have been explicitly outlawed in China (Lee, 2018). However, no legislation has ever mentioned the GFW itself and the government has never acknowledged its existence, which raises suspicion of ulterior motives.

On the other hand, the Chinese government could potentially use the vague notion of "cyberspace sovereignty" mentioned in its 2016 Cyber Security Law as a justification for censorship at the national border. However, it is debatable whether the Internet should be subject to a country's sovereignty, as such a notion directly contradicts the intrinsic values of a technology that enables communication across national borders.

Political Implications

Politicization of Cyberspace

Ironically, censorship could easily turn into publicization—known as the Streisand effect (Chen & Yang, 2019; Tilley, 2018). In the study by Chen and Yang (2019), when a group of the participants recognized that The Economist website was blocked by the GFW in April 2016, they spent significantly more time on The Economist. As Li (2016) describes, the "gaps and disconnections … make what is invisible visible" (p. 118).

Censorship of social media such as YouTube and Twitter has also made the use of these otherwise neutral platforms an act of political resistance. Roberts (2018) found in her study that mainland Chinese users are conspicuously more political on Twitter than their Chinese counterparts in Taiwan or Singapore. What’s more, Shen and Zhang (2018) discovered that after using censorship circumvention tools, people are more likely to distrust news media—even more so than people in countries without censorship.

Information Friction

One of the dangers of likening the CCP to Big Brother is assuming by analogy that it maintains control through terror and coercion, which is not at all true, as such a naive approach is likely to backfire as a result of reactance, as manifested in the Streisand effect. In fact, the GFW shapes the Chinese cyberspace in much more subtle ways.

It is often assumed that if given access people are equally likely to access all websites available across the Internet. However, Taneja and Wu (2014) discovered that, global cultural diversity actually results in “the Balkanization of the Internet” (p. 306)—rather than one completely connected community, the Internet is fragmented into relatively isolated, culturally defined markets (CDM) based on language, culture and geographic proximity. They also discovered that, surprisingly, in spite of censorship, the Chinese CDM, based on their metrics, has a score similar to that of the Japanese CDM and it actually “resembles other such geolinguistic clusters in terms of both its composition and its degree of isolation” (p. 297).

In light of this reality, it seems less surprising that, despite the visibility of the GFW and the relatively low cost of evasion, only about 11% of Chinese Internet users have ever used circumvention tools (Shen & Zhang, 2018). In the study by Chen and Yang (2019), only 55 percent of participants who received free circumvention tools activated the tools, while 86 percent of those who received a free Youku (Chinese equivalent of YouTube) VIP account at the same time activated the account within a week—the low demand for uncensored information seems to be a stronger barrier than the firewall itself.

Structural Friction The study by Yang and Liu (2014) confirmed the hypothesis that people use the Internet primarily for entertainment, social interactions or information seeking, and they also discovered that only information seeking is the main motivation behind GFW crossing. As a result, the user base of circumvention tools consists mainly of scholars and cosmopolitan elites who are well-educated, technology-savvy and "concerned about what happened beyond their home country" (Yang & Liu, 2014, p.255; Shen & Zhang, 2018). Roberts (2018), in his study, also discovered that Chinese Twitter users—even those who signed up using Chinese—are much more likely to use English words compared to Weibo (Chinese equivalent of Twitter) users, and "those who regularly jump the firewall are exceptional in that they typically have more resources, more technical capabilities, and an unusual interest in politics" (p. 163).

By separating those who are more likely to seek information from foreign sources and oftentimes more politically active from the general public who are the main targets of control but generally apathetic toward politics, as Wang (2019) describes it, the information gap resulted from the GFW has created two parallel realities and thus makes it unlikely for those exposed to uncensored information to influence the rest of the population.

Consumerist Friction The success of the top Chinese Internet companies, such as Baidu, Alibaba, and Tencent—the Google, Amazon and Facebook of China, commonly referred to as "BAT"—is partly attributable to the protection of the GFW (Chu, 2017). With foreign competitors blocked outside the country, these companies dominated the massive and lucrative Chinese market with relatively little effort. Thus, some suggest that the GFW, apart from being a tool of political control, is also as a form of protectionism (Taneja & Wu, 2014; Chu, 2017; Liu, 2010).

In addition to its contribution to the awe-inspiring economic growth that re-established Party’s legitimacy post 1989, a more far-reaching effect of this trade barrier imposed by the GFW is how it shaped the Chinese CDM. Roberts (2018) found in his study that 45% percent of Chinese internet users choose not to evade the GFW despite knowing the feasibility of evasion: After all, why would one spend the time, money and effort to set up proxy servers and VPNs when domestic platforms already have superior quality? Perhaps more tellingly, many overseas Chinese, despite having more options, would rather bypass geo-restrictions and obtain a Chinese IP address in order to consume entertainment content on domestic Chinese websites (Yang & Liu, 2014). In light of their findings, Taneja and Wu (2014) argue that even if the firewall were lifted today, the browsing behavior of Chinese users would likely not be affected.

Conclusions

Rather than the iron fist of the GFW itself, it is really the filter bubble created by Chinese technology giants—a most likely unintended byproduct of the firewall—that is the most dangerous. Instead of 1984, China seems to be heading towards a Brave New World.

But could history have taken a different path? Perhaps if the firewall had not been put in place in the earlier days of the World Wide Web, Chinese Internet companies wouldn’t have a chance to withstand the competition from Silicon Valley tech giants. Had Chinese users become reliant on services provided by American companies, whose content the Chinese government has no control over, enforcing censorship would have been nearly impossible because shutting off access to websites that have become part of people’s everyday life could cause massive grievances and is therefore extremely destabilizing.

Perhaps for a regime that has always taken censorship as one of its top priorities, the timely establishment of a highly effective censorship mechanism like the GFW is inevitable. Or perhaps eventually an invincible anti-censorship technology will be developed, which would almost certainly put an end to the authoritarian rule. Whatever the future might be, if the history has ever taught us a lesson, it is that the future might never arrive as expected.

References

Andrelczyk, C. (2016). *In The Shadow Of The Great Firewall: Censorship And Surveillance During Hong Kong's Umbrella Movement.* (Master's thesis)

Bu, R. (2013). The Great Firewall of China. *Murray State University*.

Chen, Y., & Yang, D. Y. (2019). The Impact of Media Censorship: 1984 or Brave New World?. *American Economic Review*, 109(6), 2294-2332.

Chu, C. W. (2017). Censorship or Protectionism? Reassessing China's Regulation of Internet Industry. *International Journal of Social Science and Humanity*, 7(1), 28.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Mit Press.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review, 107*(2), 326-343.

Kurose, J. F., & Ross, K. W. (2013). Computer networking: a top-down approach.

Lee, J. A. (2018). Great Firewall.

Li, J. (2016). China: The techno-politics of the wall. *EDITED BY RAMON LOBATO*, 110.

Liu, C. (2010). Internet censorship as a trade barrier: a look at the WTO consistency of the great firewall in the wake of the China-Google dispute. *Geo. J. Int'l L.*, 42, 1199.

MacKinnon, R. (2012). Consent of the networked: The worldwide struggle for Internet freedom. *Politique étrangère, 50*(2), 432-463.

Olson, M. (2007). The Logic of Collective Action [1965]. *Contemporary Sociological Theory, 2,* 111.

Roberts, M. E. (2018). *Censored: distraction and diversion inside China's Great Firewall*. Princeton University Press.

Shen, F., & Zhang, Z. A. (2018). Do circumvention tools promote democratic values? Exploring the correlates of anticensorship technology adoption in China. *Journal of Information Technology & Politics*, 15(2), 106-121.

Taneja, H., & Wu, A. X. (2014). Does the Great Firewall really isolate the Chinese? Integrating access blockage with cultural factors to explain Web user behavior. *The Information Society*, 30(5), 297-309.

Tilley, M. (2018). *The Great Firewall of China: Implications of Internet Control for China Post-Tiananmen Square Massacre to Present Day* (Doctoral dissertation).

Wang, X. (2019). The Great Firewall of China and its Implications for Political Information Systems. *Available at SSRN 3425612*.

Wittfogel, K. A. (1955). Oriental Society in Transition with Special Reference to Pre-Communist and Communist China. *The Journal of Asian Studies, 14*(4), 469-478.

Xu, X., Mao, Z. M., & Halderman, J. A. (2011, March). Internet censorship in China: Where does the filtering occur?. In International Conference on Passive and Active Network Measurement (pp. 133-142). Springer, Berlin, Heidelberg.

Yang, Q., & Liu, Y. (2014). What’s on the other side of the great firewall? Chinese Web users’ motivations for bypassing the Internet censorship. *Computers in human behavior,* 37, 249-257.