The Construction of Next Great Cyber Wall?

Taylor J Canann

2020 年 9 月 1 日

Censorship and the internet go hand in hand in China dating back to widespread adoption of the internet within the country. What about in the United States? Do we have these same standards of censorship online? No, and the main point of this article is to compare America's current policies such as banning Chinese apps and other firewall like security methods to the Great Firewall of China (防火長城).

These are very broad questions to answer in a single oped and should be the focus of broad based research, so below I will briefly discuss some of China's and America's policies and provide some data and links (within the article) to both put this in a historical perspective and allow the interested reader to examine both of these country's policies further.

In simplest terms, walls have been used by governments throughout history to either keep people out of a country, i.e. protection, or keep people in a country, i.e stop mass emigration. Some historical examples of protectionist walls are the Great Wall of China, Hadrian's Wall, or city walls such as the walls of Vienna. We then have the prime example of the Berlin Wall, the wall built to prevent a mass exodus of people from East Berlin to West Berlin.

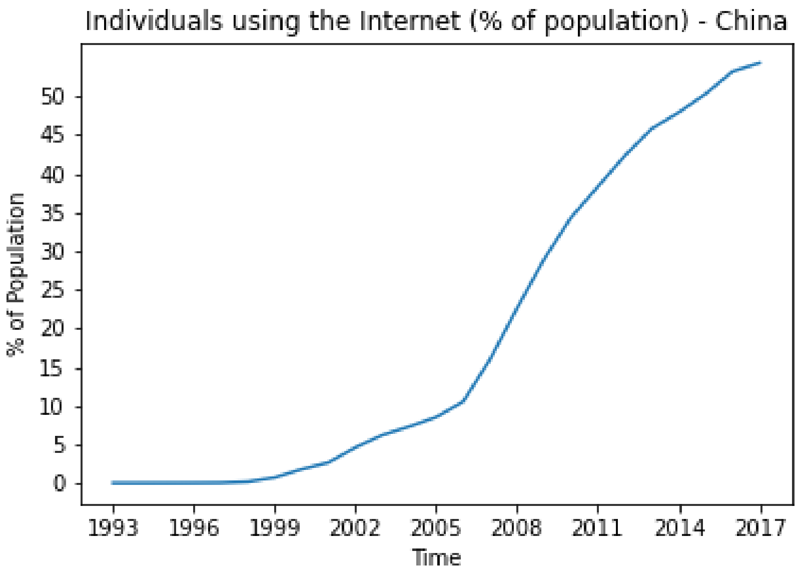
As we are moving into this "Cyberspace" realm, I will look at how these walls have been built from a historical perspective, then analyze how they differ and what analysis needs to be done. To do so, I will begin with discussing China's policies, then a brief introduction to American policies, concluding with a comparison of these "walls" and where research and analysis should lead us.

1 Great Firewall of China (GFW) (防火長城)

For those that would like to introduce themselves to the concepts of the GFW, feel free to skim the following articles:

- How-To Geek discussing how the GFW works
- maketecheasier describes what the GFW is, why it exists, and how it works
- The Citizen Lab has published a nice “little” list of search terms that are not allowed and why they are not allowed

The internet arrived in China in 1994, but internet usage did not have a significant uptick in users until the late 90’s. As depicted below, the Chinese government passed internet censorship laws starting in 1996 just prior to the pick-up in usage. In 1998, the Chinese Communist Party launched the Golden Shield project, a subsystem of which is the Great Firewall of China. These policies were developed following the commonly known Deng Xiaoping saying: 打开窗户，新鲜空气和苍蝇就会一起进来 (If you open the window, both fresh air and flies will be blown in).



Let’s address the question: Is the Great Firewall of China a defensive or restrictive wall? The LA Progressive stated:

“First, let us turn to China’ s “Great Firewall.” China instituted the firewall just prior to the turn of the 21st century. The blockage of mainly Western and American websites has indeed caused a stir inside of China and has faced criticism from “netizens” for its lack of precision and convenience. But many in China also understand why the central government would take a hard stance on the filtration of information into the country...

The Great Firewall is not ideal. Class struggle is not built on idealism. Class struggle is a byproduct of the uneven social relations that exist between classes and nations of people. In the case of China, a very conscious decision has been made to safeguard the self-determination of the country from the threat of imperial subversion through the worldwide web. Millions of people in China use VPNs to defy the firewall. However, millions more of the 800 million-plus internet users in China are satisfied with domestically produced sources of information precisely because “socialism with Chinese characteristics” has provided an ample market for online activity. While opinions on the firewall within China are diverse, it is ultimately up to the people of China to decide the best means of safeguarding their national interests.”

There are quite a few problems with this, but the key issue that I am tackling in this article is: What type of wall is this? The above quote is proposing that this is a defensive or protective wall such as the Great Wall of China (I will talk more about the history of the Great Wall of China later in this article). How are we to think about an example such as what is happening with the protests and the new security laws in Hong Kong (see my other blog post if you want to read more about Hong Kong)? Is China defending themselves against pro-democracy umbrella protests? If so the argument is then that China must protect itself from the “filtration of information” such as banning of searches related to the 六四事件 (The Tiananmen Square Massacre) or 支聯會 (Hong Kong Alliance in support of democracy in China)? This is clearly not a defensive wall, but this is instead a restrictive like the Berlin Wall.

According to Stephen Rosen, the Beton Michael Kaneb Professor of National Security and Military Affairs at Harvard College:

“If you want to know what people are worried about look at what they spend their money on. If you’ re afraid of burglars you buy a burglar alarm. What are the Chinese spending their money on? We’ re told from Chinese figures they’ re spending on the People’s Armed Police, the internal security force is about as big as they’ re spending on the regular military. This whole great firewall of Chinese, this whole massive effort to control the internet, this effort to use modern information technology not to disseminate information, empowering individuals, but to make people think what you want them to think and to monitor their behavior so that you can isolate and suppress them. That’ s because this is a regime which is fundamentally afraid of its own people. And it’ s fundamentally hostile to them.”

China’s approach to “securing” their cyber borders sounds very similar to the words used by Vyacheslav Molotov, Stalin’s foreign minister, to justify the building of the Berlin Wall such that East Germany should “introduce a system of passes for visits of West Berlin residents to the territory of East Berlin [so as to stop] free movement of Western agents.” The Berlin Wall was built to stem a massive emigration of citizens to the free world, i.e. West Berlin. China is mimicking the USSR’s strategy, but this time it is deploying it walls not only on land, but in cyberspace with the GFW.

2 Does a “Great American Firewall” Exist?

Let’s turn our attention to American cyber policy, and, specifically, is the United States currently constructing a “Great American Firewall”? Short answer, no. Long answer, yes. The United States does have defenses and protective barriers, but nothing to the extent to be deemed the “Great American Firewall”. American policy is more complicated than Chinese policy, so the interested reader should take this as an introduction and go learn more.

For example, the United States has recently threatened to ban TikTok unless the company sells its US business (the UK is considering following these restrictions) as well as adding Huawei to the Entity List. Does this constitute an oppressive firewall that is worse than that of China? I am going to introduce the idea that the US "firewall" policy can be thought of as a mixture of the following historic walls:

1. Great Wall of China

2. Hadrian's Wall

3. The Maginot Line

The Great Wall of China was built as a sequence of barriers to protect the empire from different nomadic tribes. These barriers were later connected. The US policy is a mixture of private companies securing their own or other companies systems (such as BlackBerry), citizens protecting their own devices either on their own or purchasing soft/hardware to do so, private companies such as CyberDefenses Inc. working with companies to stop cyber crime and to help cyber law enforcement officials, and finally direct government and military enforcement of defense such as US Cyber Command.

In simplest terms, there are three types of firewalls in the United States: Government, Business, and Personal. Each of these entities have slightly differentiated incentives. The government is acting to stop crimes, enforce current laws, and defend against current cyber attacks, where as a standard business firewall may also want to stop intellectual property crime and protect their business assets, but the company may also want to stop employees from accessing unwanted websites such as social media or pornography sites. Personal firewalls may be deployed by citizens to protect themselves from financial abuse, i.e. they want to stop crime, as well as maintain their privacy. Notice that there are some similarities in these incentives, but enough differences to make creating effective policies difficult. These firewalls can be thought of as guard posts, that are built, and disconnected to keep out different "evils from your empire". However, just as the Great Wall of China did not keep the nomadic hoards at bay, neither will a simple firewall keep your computer, company, or country safe, there must be some interplay and connection between government, businesses, and individual citizens.

For example, there are many defenses built in both the private and public sector, some stronger than others. Some of these “fortifications” have been connected, others are currently being connected, while others are still stand alone guard posts. For example see the following:

- Forbes describing the challenges of protecting critical infrastructure
- Georgetown Journal of International Affairs discusses the role of the state in private sector cybersecurity
- Government Technology analyzes the CISA’s importance in both state and local cyber defense

What about Hadrian’s Wall? From 122-128 AD, emperor Hadrian oversaw the building of a wall toward the northern part of the Roman Empire in Britannia. For this analogy, I am going to base the idea of building Hadrian’s Wall on Anthony Everitt’s book because it’s useful to analyze current American cyber policy. Everitt proposes that the wall was constructed to control immigration (not emigration), customs, and smuggling, while still allowing trade and movement through the walls since Roman citizens lived on both sides of the wall.

Like Hadrian’s wall, America’s firewall aims to protect the country’s borders from smuggling, enforcing customs, and otherwise enforcing the law. One prime example of this is the shutdown of the Silk Road. If you are unaware of the Silk Road, feel free to read about it on Investopedia. I find it useful to describe the Silk Road in the immortal words of Obi-Wan Kenobi: “You will never find a more wretched hive of scum and villainy.” There are still more Darknet Markets, for a small list of them, see the Dark Web Links’ list for 2020. Even though the United States is constantly monitoring, there will always be leaks, but as the defenses strengthen, more of the “scum and villainy” will be stopped.

Finally, I will argue that the American cyber policy also follows a similar defensive method to the Maginot Line. I am hoping that it will not be as effective as the Maginot Line, just arguing that the policy seems eerily similar. The Maginot Line was a defensive fortification built along the French-German border after World War I so as to avoid the catastrophic bloodshed they had just witnessed. The defensive fortifications spanned the entire border French-German border, and relied on British deployment of troops into Belgium at the first sign of German mobilization of troops, which did not happen for international political reasons (this is of course an over-simplification, so if you are interested in learning more about the Maginot Line, read Judith Hughes' book). Germany was able to bypass these formidable defenses and topple France in 46 days. This was not a failure of the gun turrets or the defensive structures, but of defensive reliance on other countries to secure their own border.

Why would I then argue this is similar to cyber policy? The USA is part of an intelligence alliance known as the Five Eyes in which Australia, New Zealand, Canada, the United Kingdom, and the United States have a joint signals intelligence cooperation agreement. These countries work together to secure their own borders and share information to help one another. This type of cooperation works so long as the incentives of each nation align, but this is not always the case. Right now, the 5G Huawei debate is a hot topic, and if Canada does not also ban Huawei, as have the other countries in the Five Eyes, then there will exist a backdoor into their private communications. I am not proposing that Canada should be kicked out of the Five Eyes right now, but I am promoting that we should use discretion.

What about privacy and free speech concerns? These are important points of debate that should not, and are not being cast aside, but they are too large to be dealt with here. For those interested, I am open to having a civilized, data driven discussion on the trade-offs between security, free speech, and privacy. As an important distinction for this article, the United States government is not banning individuals from searching for terms online, which is an important difference between American and Chinese policies.

As we have seen, American cyber policy is rather complex, and can be seen as some mix between Hadrian's Wall, the Great Wall of China, and the Maginot Line.

3 Conclusion

As laid out above, there does exists a dispersed defensive firewall in America, however, we can see that American and Chinese cyber policies are quite different in their methodology and application. Therefore, the suggestion of a “Great American Firewall” being equivalent to, if not worse than, the Great Firewall of China is clearly an inflated accusation.

For more information on hacking and policy trends, visit the Salem Center’s Cybersecurity Policy Program to follow our upcoming opeds, as well as learn about our speaker series, courses offered, and current research.