The Golden Shield Project of China: A Decade Later
An in-depth study of the Great Firewall

Sonali Chandel, Zang Jingji, Yu Yunnan, Sun Jingyao, Zhang Zhipeng
College of Engineering and Computing Sciences, New York Institute of Technology, Nanjing, China
{schandel, jzang, yyu18, jsun19, zzhang36}@nyit.edu

***Abstract* - The Golden Shield Project aka the Great Firewall of China is one of the most popular and vital information security and censorship technology project that is being used very strictly and extensively in the country since 2008. The Great Firewall has been preventing Internet users in China from visiting many foreign websites for one reason or the other and blocking them completely. This particular firewall implements information access control through some stringent security policies and takes the responsibility of controlling and censoring the flow of data. The Great Firewall makes China one of the strictest countries in the world when it comes to the internet freedom of the netizens residing in the mainland. In this paper, we will focus on the development of the Great Firewall that includes the timeline of its development, the censorship policy used for its implementation, its effects and the principles behind the technology used for its application. We will discuss where it stands after a decade of its implementation. We will also present a study of techniques like using a VPN to circumvent the heavily monitored firewall. These circumvention techniques have become very popular in the mainland because of severe information censorship. With this research, we aim to offer a clear understanding of the Great Firewall to the people from across the world.**

Keywords - Great Firewall, Firewall, VPN, Access control, Censorship, Circumvention

I. INTRODUCTION

The 'Golden Shield Project' of China started in 1996, but its actual implementation happened in 2008. [1] The foreign media calls it 'The Great Firewall' to indicate the seriousness and extent of the information block it poses on the entire country. According to the definition of the Chinese government, the intention behind the Golden Shield Project is only to filter and censor wrong information originating from outside of China to protect the society from its influence. From the time of its inception two decades ago, the project has evolved and turned into a highly secure, heavily monitored system which is very well described by the term, 'the Great Firewall' as it mesmerizes the rest of the world. The most significant side effects of the Great Firewall implementation can be seen from the fact that some of the most popular social networking apps and websites in the world like Facebook, YouTube, Twitter, WhatsApp, and Instagram are all blocked in the mainland.

A decade has gone by since the Golden Shield Project has been officially implemented in the country, and there is no sign whatsoever of it being removed shortly. The government and the local citizens believe that the Great Firewall contributes to stabilizing Chinese society, both online and offline.

The Great Firewall is not only a powerful political tool but also an exquisitely designed network security program. However, at the same time, it also brings endless worries to some people, especially those who live in China and have to communicate with people from other countries for personal, business, or academic purposes. To scale the wall, they turn towards using VPN applications, which are not necessarily cheap, safe, and stable. From time to time, there is always a government crackdown on VPN sellers and users, causing many issues for everyone involved.

To help people in getting a full understanding of the Great Firewall, this paper researches its development process and the technology behind it. The paper is structured as follows: Section I introduces the topic. Section II presents the related work. In section III, the development of the Great Firewall and the network censorship situation in other countries of the world are discussed. In section IV, the paper talks about the technology behind the Great Firewall. This includes the discussion of the kind of technical methods adopted and the methods implemented during the last two decades. The technology behind VPN is introduced in section V while various conditions concerning the privacy and security issues in using VPN for circumventing the censorship is listed in section VI. In section VII, the paper presents a survey result on local people's view on the Great Firewall and VPN to show how well they know about the network censorship in China and whether they can protect themselves from all kinds of online attacks and information theft that happens while they are trying to scale the wall. Finally, we present our conclusion in section VIII and discuss the future works that can be carried on by someone interested.

II. RELATED WORK

During the research for this paper, we found that the already published articles on this topic mostly focus on various aspects of the Great Firewall individually. Some of them focus only on the technology, some only on cultural and social impact and some only on the issues related to the local laws and policy.

Hounsel, Mittal, and Feamster [10] use natural language processing and search engines to automatically discover a much more extensive range of websites that are censored in China. They focus only on keyword blocking technology, which is just one aspect of the techniques used behind running the Great Firewall.

Stevenson [12] examines the methods of internet censorship employed by China and other nations and proposes a novel combination of existing legislative proposals, recommendations from the Electronic Frontier Foundation, and international cooperation as the best way to address the problem of internet censorship. It provides background information about legal and economic trade for our paper.

978-1-7281-2542-8/19/$31.00 ©2019 IEEE
DOI 10.1109/CyberC.2019.00027

Farnan, Darer and Wright [17] considers the legitimate responses from the DNS servers themselves and present the argument that this type of attack may not be primarily targeted directly at users but at the underlying DNS infrastructure within China. However, the evidence they present needs more experimental data for the verification of their argument.

Zhang et al. [22] talk about secured VPN technology, but we have extended the idea of using VPN technology specifically as a countermeasure to the Great Firewall.

In this paper, we discuss the development of the Great Firewall for over ten years from the technology to the government policy behind it. We have also analyzed some of the significant loopholes of the Great Firewall that other published papers on this topic have not mentioned. We have also connected the Great Firewall and its effects to its countermeasure, known as VPN.

III. The Development of The Great Firewall

3.1 The Timeline of the Great Firewall

The Great Firewall is the nickname, which the western media gave to a sub-system of the Golden Shield Project in 1997. The Golden Shield Project also called as 'National Public Security Work Informational Project,' is a project that includes security management information system, criminal information system, exit and entry administration information system, supervisor information system and traffic management information system. This nationwide network-security fundamental constructional project was started by the Central Cyberspace Affairs Commission of the People's Republic of China. [33]

The Internet first arrived in China in 1994. As the availability of the Internet gradually increased with time, it became the most common communication platform and tool for trading information like everywhere else in the world. [15] With the Internet, also came the western ideologies, which the government was reluctant to embrace. Hence, the birth of the Golden Shield Project.

The entire project was implemented in different phases. The main tasks of the first phase (1998-2006) of the project were the construction of the first level, second-level, and the third-level information communication network, application database, shared platform. The second phase was initiated in 2006, which took only two years to complete. It was mainly focused on enhancing the terminal construction while trying to formalize public security work. [13]

To increase the final construction, along with the public security business application system, the Chinese government started the phase II project in 2006. Compared to phase I, phase II emphasized more on information application types of the public security business and public security information. The primary goals of phase II included the application system construction, system integration, the expansion of information center, and information construction in central and western provinces of the country. With the completion of phase II in 2008, internet censorship in China became more powerful than ever [13]. Table 1 shows a brief timeline for this project.

TABLE 1. The Timeline of The Great Firewall in China

Year	Major Events
1996	The Great Firewall was first set up
2004	The services of keyword screening and sensitive words masking were introduced by Cisco.
2004	Wikipedia got blocked for the first time (It is accessible now) [4]
2007	YouTube launched Hong Kong substation, and somehow its use in Chinese mainland started being blocked.
2008	Facebook got blocked
2009	Twitter got blocked
2010	Google claimed that it was attacked by Chinese hackers because it refused to allow the Chinese government to control its server in Beijing. A few days later, Google was blocked.
2014	Instagram was blocked.
2015	All foreign websites with a domain name co.jp are blocked

Table 2 shows some most common types of information that are censored online. [9]

TABLE 2 Characters of filtered information

Classification	Example
Politically Sensitive Information	Facebook\Twitter\New York Times
Pornographic Information	Baidu.jp
Online scams and other crimes	Some online gambling websites

3.2 The Technology Development of the Great Firewall

This section talks about the four stages of technology developments of the Great Firewall from 1998 to 2018.

1). First stage: The Golden Shield blocks domain names and IP addresses

The first generation of the Golden Shield project proposed an internal filter that blocked specific domain names and server's IP addresses. A multi-level system was implemented to track Internet users who violated the rules. As a result, all Internet cafes in the country are required to install surveillance software either provided or approved by the local police. This system monitors traffic on all computers in the café, including the screens of each user. The system also has direct access to the policy network system. Users at Internet cafes are required to present their ID cards before they can access the Internet. If a violation occurs, the Internet cafe owners will submit their personal information to the local police immediately via the Internet [11]. Many Internet service providers (ISP) for residential users are also required to verify every user's ID information. Many of the web-based forums prohibit anonymous posting. Real names are required to register an ID to submit articles [21]. Many popular smartphone apps also need their users to register using their original ID to be able to keep track of every user's online activities.

2). Second stage: The Golden Shield implements keyword censorship

In the second stage, the keyword-filtering system of Golden Shield was upgraded to detect the content of the websites that netizens visit, even if the internet connection is going through a proxy. If there is some “sensitive content” communicated along with the network connection, the Transmission Control Protocol (TCP) is reset automatically. For example, some phrases that refer to any political dissents, such as “Officials called on," “Persecution activities,” “Illegal detention,” and “Declared anti-communist” will be censored. [10]

3). Third stage: Great Firewall begins detecting VPNs and other circumvention tools

With support from the government, the developers of the Great Firewall finally managed to identify weaknesses in VPNs [44]. They found that there are some distinct features of the commonly used VPN protocols, such as IPSec, L2TP/IPSec, and PPTP, which often use specific ports. When processing the encrypted connection, it leaves a distinctive trace. Again, the Great Firewall was upgraded to detect such connection traces. As a result, there is a very long list of VPNs that cannot be used functionally because the Great Firewall stopped the connection traces, such as Free VPN, Green VPN, Jiguang VPN, Tianxing VPN and many more. [21]

4). Fourth stage: Cybersecurity laws target anonymity and VPNs

In addition to continually upgrading the technology behind the Great Firewall, Beijing has also introduced new laws to criminalize VPN service providers. The first primary law to regulate Internet content was released in 1996. This law was about the “Interim Provisions Governing Management of Computer Information Networks in the People’s Republic of China connecting to the International Network.” These provisions were amended and enhanced in 1998 and 2000 by the “Provisions for the Implementation of the Interim Provisions Governing Management of Computer Information Networks in the People’s Republic of China.” [12] The law stated that all Internet information services must be licensed (if commercial) or registered with the authorities (if private). ISPs must record and retain data about the number of time users spend online, their account numbers, their IP addresses, and their dial-up numbers. The latest addition to this string of regulations came in 2005, which deals specifically with providers of “Internet news information services.” [18]

On January 22, 2017, the Chinese Ministry of Industry and Information Technology (MIIT) announced a “Notice on Clearing Up and Regulating the Internet Access Service Market,” which forbids the unapproved creation of dedicated lines or other information channels to conduct cross-border business activities. It means providing VPNs to the users without official permission is illegal in China now. Table 3 shows the development of cyber laws for VPNs in China. [6]

In December 2017, a man called Xiangyang Wu was sentenced to 5.6 years in prison and fined 500,000 Yuan (73K USD approx.) for illegal business operations of VPNs. [39] According to announcements made by Shanghai Baoshan District People’s Court in October 2018, Dai Mou was also sentenced to three years in jail and was fined RMB 10,000 (US $1,446) for selling and using VPN services in China illegally. [38]

TABLE 3 THE DEVELOPMENT OF CYBER LAWS FOR VPNS IN CHINA

Time	Development
January 22, 2017	the Chinese Ministry of Industry and Information Technology (MIIT) announced a “Notice on Clearing Up and Regulating the Internet Access Service Market” [6]
January 2017 - March 2018	A large amount of Taobao shops were shut & the VPN applications were removed from iPhone market [40]
December 2017	Xiangyang, the VPN service provider, was sentenced to jail for being guilty [39]
October 2018	Dai Mou has been sentenced to three years in jail and a fine for selling and using VPN services.[38]

3.3 Internet Censorship in China vs. the Rest of the World

China is not the only country in the world to implement censorship on its cyberspace. Besides China, there are more than 20 countries around the world that seriously monitors and censors the online activities of their netizens. Apart from these countries, some other countries keep implementing censorship temporarily during some protests or demonstration against its government or when some social disturbance happens in their territory. They do this mostly to control the news from spreading, both real and fake and causing more disruption in society. Given the different cultural background and values, each country's Internet censorship presents a very different picture. [20]

In Table 4, we briefly list the primary methods used by some countries for the censorship of their network. Most of the countries do not directly block access to any legal, foreign websites. Also, there is no official verification system adopted in any other countries as China does. [1]

TABLE 4 CENSORSHIP IN CHINA VS. THE REST OF THE WORLD

Country	Censorship
China	Great Firewall
North Korea	Closed LAN
Cuba	Limit the number of Internet users
Myanmar	Closed Internet
Turkmenistan	High Internet access costs
Vietnam	Limit speed and comments
Iran	Internal Intranet.

IV. THE GREAT FIREWALL – AN EXTENSION OF A GENERAL FIREWALL

4.1 The Firewall Technology

The core technologies behind any general firewall include the concept of Packet filtering, Application Proxy, Stateful Inspection, and Complete Content Inspection.

4.2 Methods used behind the Great Firewall

The Great Firewall technologies combine multiple firewalls technologies, as mentioned in section 4.1. For example, the IP address checking and filtering technology in the Packet Filtering Firewall and the connection blocking technology in the data detecting technology in the Application Proxy Firewall. The Chinese government employs multiple approaches for censorship that includes both technical and non-technical means. [24, 17]

The following section talks about the leading methods that are used behind the Great Firewall:

1) DNS poisoning technology: One of the essential technical methods used by the Great Firewall is DNS poisoning. When the Great Firewall observes DNS queries to specific domains, it responds by sending a poisoned DNS response to the requesting DNS resolver. Due to its position in the network, this typically reaches the requesting DNS resolver before the response from the DNS server. This results in the requesting DNS resolver caching the poisoned DNS response and ignoring the response from the DNS server itself. [17]

2) Self-Censorship: According to laws and regulations mentioned in section 3.2, Chinese companies are responsible for their content, and any violations can lead to severe penalties ranging from hefty fines to closures. Therefore, many large companies have set up their law enforcement teams to monitor and ensure that their platforms do not contain banned topics. [44]

3) Manual enforcement: To enforce censorship and filter harmful content considered detrimental to the progress of China, a large number of Internet watchdogs are employed. These people are contracted by the authorities to monitor online content and inform about any potential violations to the assigned government officials to make an on-site investigation. Some sites offer back-end access, allowing these watchdogs to edit content directly. Recently, advancement in AI technology has allowed the monitoring processes to be automated on a large scale. [44]

4.3 The Working principle of the Great Firewall

The Great Firewall blocks a specific site for many different reasons. However, these reasons entirely depend on the choice of the government. The Great Firewall aims to eliminate criticism and prevent people from being infiltrated by the information that the government decides to be harmful to the peace and harmony of the people in the country [24]. It can include a ban on sensitive words, which can insinuate national leaders, violation of the constitution or reactions that can influence the peace of society. There is much censorship regarding social issues becoming widespread and known to the public or outside world as well. Similar news coming from the outside world that the government feels might spoil the mind of the local citizens is censored as well. Fig.1 shows the working principle of the Great Firewall [5]. Between the times a user submits their request, and the server sends back the response, four things can go wrong [27]. The following points explain how it works in steps.

1) DNS Blocking: When a netizen enters a URL, the DNS finds the corresponding IP address. If DNS is set as not to return that particular IP address, then the user cannot access the site. As shown in Fig.1, the message displayed on the screen is "Cannot find the webpage." Around 2002, China began to use 'Domain Name Hijacking.' They use IDS (Intrusion Detection Systems) monitoring systems provided by routers to hijack domain names, preventing people from accessing filtered websites. At the same time, to prevent advanced users from directly using different domain name servers with normal functions, China has also begun to block overseas DNS servers and has blocked hundreds of North American DNS servers. [17]

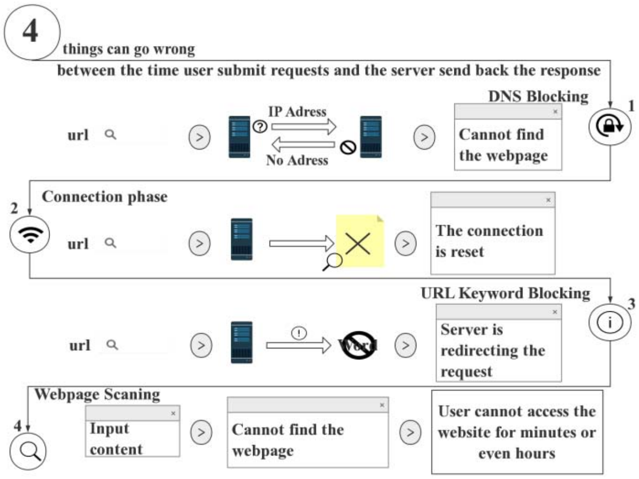


Fig.1 The working principle of the Great Firewall

2) Connection Phase: The monitor will compare the user's request to the list of banned IP addresses [5]. If it belongs to a banned address, the server aborts the request. As shown in Fig.1, the error message displayed is, "The connection is reset."

3) URL Keyword Blocking: Although the URL is not on the blacklist, the connection is reset if the requested URL contains forbidden words [19]. Advanced routing equipment from companies such as Cisco, which supplies 80 percent of China's routers, has helped China achieve keyword filtering. As shown in Fig.1, the error message displayed is, "The server is redirecting the request." [10]

4) Webpage Scanning: Once a user enters their requested site, the monitoring system scans the entire page to see if it can pass. Users may not be able to access the site for a few minutes or even an hour. As shown in Fig.1, the error message displayed is "Unable to display the web page."

4.4 The Aftereffects of the Great Firewall

4.4.1 Effects on Society

The firewall is not meant to separate the Chinese internet from the overseas internet, but it is mainly used to implement targeted blocking of individual foreign websites, mobile applications, and specific web pages. It is important to note that these interception points add up to a tiny fraction of the vast ocean of overseas internet. Some people take the blocking very seriously because some blocked websites used to be very popular among Chinese netizens. For example, Google, Facebook, Twitter, and other mainstream websites in the United States. There are two dominating views about censorship. One is that the western world has taken this as a prominent example of China's "lack of Internet freedom." Moreover, the other half includes the local people who are not at all interested in the blocked sites in any way and do not get affected by its absence. For them, the problem is almost nonexistent. The reality is that both sides are deepening or expanding in their respective directions. [2]

4.4.2 Effects on Businesses – Private and government-related

A. In China

In the past few years, the Golden Shield project has brought a significant impact on the nation when it comes to the e-business. The first thing to notice is the rapid growth of local internet companies, typically the "BAT" (Baidu, Alibaba, and Tencent). Without any powerful competitor from the outside world, these companies have gained almost unlimited and unopposed resources in the Chinese market, including the government's support. [16]

In 2018, the use of Baidu as the only search engine reached 60% of the overall purpose of the local search engine market [42]. The success of Baidu has grown tenfold after Google quit the Chinese market in 2010. Though a survey conducted by 'China Internet Watch' in, August 2018 suggests that over 70% of Chinese will choose Google over Baidu if it ever returns. [43]

The Internet industry in China, without powerful foreign competitors, is prospective yet still in chaos. Big companies like the "BAT" keep ignoring the internet's ethics principles from time to time. For example, Weibo (Twitter's equivalent), a social website where users can post pictures, short videos, and text contents, was denounced by its users for a series of violations of government policies including stealing users' account to post and re-post commercial advertisements and randomly blocking posts from accounts which are not VIP accounts in order to push people to buy its VIP services. However, Weibo is still one of the most popular social websites in the country. In addition, after learning lessons from mistakes made by Facebook and Twitter, Weibo cooperates with the Chinese government very closely.

The Great Firewall not only encourages the growth of local internet enterprise but it also brings profits to VPN service providers even when most of the free VPN applications have been defined as illegal in the last two years. Apart from the restrictions set by the government, there are some side effects, which increases the operating costs of all the foreign and local companies who have a business in other countries. Also, they have to adopt a VPN to ensure their regular communication between their overseas branches and clients. Even though such communications will not be targeted directly, but the ban on non-state sanctioned VPNs and the cost for building VPN servers are still expected to grow extensively. [41]

B. International influence

In China, the cybersecurity law was officially implemented from June 1, 2017. Many enterprises in Europe and the United States, industry associations with a government background, government departments, and mainstream media expressed varying degrees of concern, disappointment, and even anxiety about the Chinese cybersecurity laws. Foreign critics said that the law could shut out foreign technology companies from "important" departments and lead to controversial rules, such as requiring companies to store data on servers in China. Such actions were already taken before the new cyber laws were implemented. For example, Google decided to quit the Chinese market only because it refused to store data in servers under government surveillance, located in Beijing. [1]

4.5 Technology Tricks and Loopholes

Although the Great Firewall is growing to be stronger, there still exists some loopholes that users find very hard to understand. For example, some users can access a few blocked websites such as YouTube, when they use an external LAN port for connecting to the LAN. Some of these problems are still not settled, but some can be explained. For example, some users find that they can still receive notifications from blocked social media apps such as Facebook and Twitter. Take Apple's APNS (Apple Push Notification Service) as an example. The operation behind it can be seen in Fig.2.

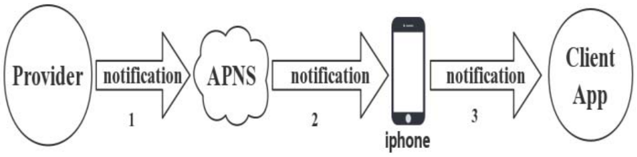
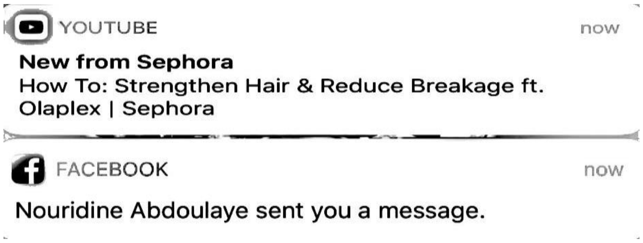


Fig.2 Apple's official APSN mechanism

The Provider is the background server of users' program. The Provider server is blocked, but the APNS server is not as it is in foreign countries (mostly more than one). It can communicate freely with the provider. Therefore, there is no communication problem between APNS and iPhones. As a result, Facebook and other blocked apps can send messages to APNS, and then APNS can push those messages to the iPhone, bypassing the wall as seen in Fig. 3. This also applies to Android phones where users can get a push notification from the blocked app, but they cannot open it.



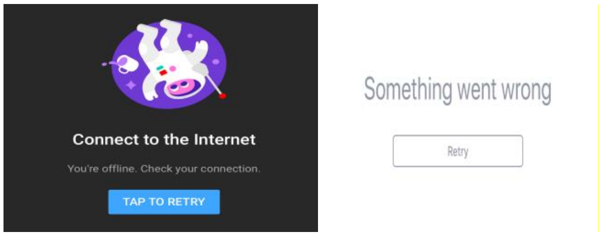
YOUTUBE now

New from Sephora
How To: Strengthen Hair & Reduce Breakage ft. Olaplex | Sephora

FACEBOOK now

Nouridine Abdoulaye sent you a message.

Fig.3 Example of YouTube and Facebook users receiving message notifications



Connect to the Internet

You're offline. Check your connection.

Something went wrong

Fig.4 The messages above shows some error messages received while trying to open and access some blocked sites

Except for a few loopholes, the Great Firewall technology is robust enough to censor everything else without fail. Some local versions of some universal apps like QQ music can even detect that the users are using a VPN to connect and hence decline the users' access to their server.

V. The Technology to Circumvent Great Firewall - VPN

VPN (Virtual Private Network) refers to a private communication environment built on public communication facilities, which is characterized by private and virtual communication. The goal of a VPN is to establish a logical network independent of the physical topology of the system, which allows a geographically distributed set of hosts to interact with each other and can be managed as a separate network [31]. It is commonly used in enterprise-level office systems, but because of the Internet censorship on such a massive scale in China, many people use VPN to scale the wall. VPN provides an end-to-end transmission system, and it is very convenient for users to log in to the company gateway from a remote location with an untraceable IP address. Because of this approach, it can easily avoid institutional scrutiny.

5.1 The Technologies used by a VPN

The mainstream applications that claim to provide VPN services are using one of the following three techniques: Proxy, IPSec, and SSH.

1) Proxy Server: A proxy server is like a courier service which is responsible for nothing but transcending the message. The work of proxy servers is conducted in the HTTP layer and Socket layer in the Open System Interconnection (OSI) model under most circumstances. [21]

2) IPSec: IP security is the most common method used by VPN applications. It works in the third layer of the Open System Interconnection (OSI) model, which is the Network layer. [21]

3) SSH: It is an encrypted channel that needs to be combined with the proxy server to overcome the blocked network. Hence the tool that is used to scale the blocked network which is usually called SSH is, in fact, an SSH agent. It can be considered as an encrypted agent, where the package is kept in a safe case while being sent to the courier. In the TCP/IP five-tier model, SSH is the security protocol that applies to the application layer and transport layer. SSH is a remote shell, an application based on SSL. Although many people use SSH to transmit data, they merely use the SSL proxy function of SSHD software to get this job done. [21]

A. The awareness of Chinese citizens about GFW and VPN

Table 5 shows the results from an online survey that shows the data from the citizens who visited the blocked websites [24]. This survey aimed to find out the awareness of the local netizens regarding GFW and how many still choose to visit the blocked websites. Figure 5 shows the motivation of people who tried to visit those websites. [24]

TABLE 5 The Survey results of The Netizens who Visited The Blocked Websites

Relevant factors	**The result of the Survey**
Gender	92% male
Education background	73% of the participants were university students
Age group	22-25 yrs.
Occupation	Students from an IT background
Methods used to visit the blocked websites	Mostly free VPN
The frequency to scale the wall	66% visited every day
Money spent on scaling the wall	88% paid less than 10 yuan per month

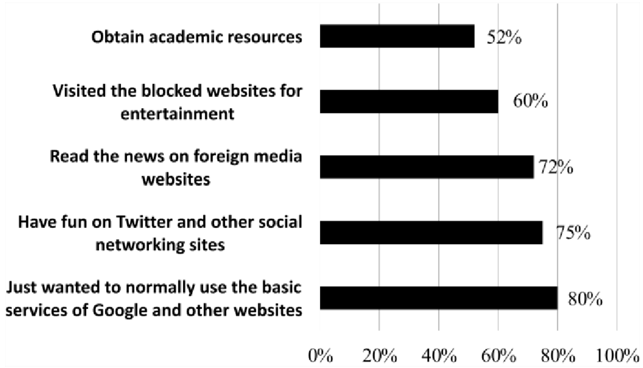


Fig.5 The motivation of people who tried to use VPNs

5.2 Privacy and Security Issues in using a VPN

When it comes to dealing with the Great Firewall, VPN is an inevitable technology. In the past few years, more and more netizens around the world have chosen to use VPN to cover up their online traces. However, the various pros and cons cannot be neglected when it is about paid and free VPNs. Table 6 summarizes the advantages and disadvantages of using various paid and free VPNs. [29] [30] [28]

Also, here are the research results that the researchers found after analyzing the original coding and network behavior of 283 VPN apps in Android's Play store. [7]

1) 18% of VPNs do not encrypt any data, leaving users vulnerable to man-in-the-middle attacks when using open networks like public Wi-Fi.
2) 16% of VPNs embed code in users' network data, such as image transcoding. The purpose of image transcoding is to make the image load faster. Two apps embed Java scripts that push ads and tracks user behavior in their data. JavaScript can be easily modified into malware.
3) 18% of VPNs do not encrypt any data, leaving users vulnerable to man-in-the-middle attacks when using open networks like public Wi-Fi.
4) 16% of VPNs embed code in users' network data, such as image transcoding. The purpose of image transcoding is to make the image load faster. Two apps embed Java scripts that push ads and tracks user behaviour in their data. JavaScript can be easily modified into malware.

TABLE 6 THE ADVANTAGES AND DISADVANTAGES OF USING A VPN

Advantages	Examples	Disadvantages	Examples
The IP address can change	Betternet, VyprVPN, PureVPN	Unstable	Betternet, CrossVPN, WhatsVPN, Astrill
Anonymous use, No Tracking	Betternet, Psyphon, UltraVPN, ExpressVPN, VyprVPN, PureVPN		
Registration and login not needed to use	Betternet	Too many ads	Betternet
Easy to install and use	CrossVPN, Psyphon, NordVPN		
Multiple devices allowed per connection	WhatsVPN, CrossVPN, ExpressVPN, PureVPN, VyprVPN	Security is not guaranteed	CrossVPN
Support several VPN protocols	ExpressVPN, PureVPN, Astrill		

5) 84% of VPNs leak traffic when using IPv6. 66% of VPNs even leak DNS information making users more vulnerable to surveillance or modification attacks.
6) 67% of apps claim to enhance privacy, but 75 percent use third-party tracking codes to monitor users' online behavior. 82% require users to provide sensitive information, such as access to user accounts and text messages.
7) 38% of VPNs contain code classified as malicious by VirusTotal. VirusTotal, provided by Google, is a collection of more than 100 antivirus software antivirus services.

VI. RELEVANT GOVERNMENT POLICIES AND CURRENT SITUATION OF THE GREAT FIREWALL

6.1 Chinese Government's policies towards the Great Firewall

Under normal circumstances, there is no privilege given to anyone at any point of time to access the blocked sites in the country. However, during some very significant international sporting, political or business events like G-20 Summit, World Expo, Youth Olympic Games, etc. the government does allow the visitors from foreign countries to have the privilege of accessing the Internet without any censorship. This exceptional privilege service is provided by the telecom operators and is only allowed within an exclusive scope of a limited zone. These free internet access zones are just set for a limited period for the guests and media reporters until the event ends. Table 7 shows some examples of such events when a censorship-free zone was created for people visiting China from overseas for the same. [32]

TABLE 7 EXAMPLES OF THE GREAT FIREWALL FREE ZONE

Free Zone	Place	Time
World Expo	Shanghai	May 1, 2010- October 31, 2010
G-20	Hangzhou	September 4, 2016- September 5,2016
Asian Games	Guangzhou	November 12, 2010- November 27, 2010
Youth Olympics	Nanjing	August 16, 2014- August 28, 2014

6.2 Chinese Government's policies towards VPN

Although there are many VPN applications available in the market that can help in getting access to the blocked content but selling and using a VPN without an official license is illegal in many cases in China [37]. In January 2017, the Ministry of Industry and Information Technology (MIIT) issued the notice on clearing and regulating the Internet network access service market, which stated: "It is not allowed to establish or rent special channels (including VPN) to carry out cross-border business activities, without the approval of the telecommunications authorities." Through this announcement, we can see that unapproved VPN cross-border business activities are explicitly prohibited [6]. During the time between January 2017 to March 2019, a large number of Taobao shops got shut for selling illegal VPN software. At the same time, a lot of illegal VPN applications have been removed from the iPhone market as it is monitored by the local government now after its local data center moved to Guizhou, a province in southwest China, in March 2018 [36]. Although fears of a blanket block on services have not materialized, VPN connections often face outages during the time of major political events in China. [30]

6.3 Current Situation and Future Plans

The government regulation allows foreigners to invest in China's virtual private network but caps foreign ownership at 50% [3]. The government intends to turn Hainan province into a free trade zone to let Hainan become the foundation of an international tourist center and encourage overseas companies to establish regional headquarters there. Google has been away from China for eight years, but now the company has been quietly testing the waters by investing in different products in China. Google has launched its Drive and Docs products in Shenzhen in China, adding to a growing list of services it wants to offer in the world's biggest Internet market [26]. On January 19, 2018, Tencent and Google announced that they had signed a cross-licensing agreement for patents covering a wide range of products and technologies, and they said they would be open to further collaboration on future innovations. [35]

VII. CONCLUSION & FUTURE WORK

As a result of this research, we have concluded that there are four stages in the technology development of the Great Firewall. We talked about the leading technologies used behind the Great Firewall, including DNS poisoning, Proxy server technology, and Network address translation technology. We can also conclude that the Great Firewall is being developed and updated continuously. Therefore, the power of the Great Firewall cannot be ignored. The increasing importance of the Internet attracts people's attention on network and data security. The Great Firewall plays a vital role in protecting national information security. It has been preventing Internet users in China from visiting certain foreign websites, which the rest of the world considers as a prominent example of China's "lack of Internet freedom." Blocking some external sites is proving out to be extremely beneficial for the rapid growth of local internet companies. Organizations and netizens are rampantly using VPNs to circumvent and scale the wall. However, nowadays, there have been some new local laws that prohibit users and sellers from using and selling VPNs, respectively. Overall, we hope that our work can be used as a complete reference to learning more about the principles and policies of the Great Firewall.

Further study needs to be done on how to improve the firewall technology to better prevent illegal users from entering the Intranets. We hope that our work on the Great Firewall can help others to learn and know more about the Great Firewall. This paper offers a reference for studying the technologies and development of the firewall.

References

[1] People's Daily Online: The cybersecurity act and the national security review system. http://theory.people.com.cn/n1/2016/0622/c40531-28469973.html

[2] Global times: what impact does the firewall have on China's Internet http://tech.163.com/15/0128/14/AH26MQKQ000915BF.html

[3] Expats Allowed to Invest in China's VPN Services in Hainan https://mp.weixin.qq.com/s/KGt3b5iMbhyScEzxc3in6A

[4] "China Now Blocked from Accessing Wikipedia." The Epoch Times. 8 June 2015. Archived from the original on 10 June 2017. Retrieved 4 May 2017.

[5] One picture shows you the data behind the Great Firewall of China. Web. https://www.svlik.com/704

[6] The evolution of China's Great Firewall: 21 years of censorship. Web. https://www.hongkongfp.com/2017/09/03/evolution-chinas-great-firewall-21-years-censorship/

[7] VPN is illegal. Use it carefully, even if it is not illegal. Web. https://www.sohu.com/a/125475123_354973

[8] US takes China VPN ban to the WTO. JobTubeDaily. 25 Feb.2018. Web. http://mp.weixin.qq.com/s/68hyFB156fj3fp36UV4JgA

[9] "GreatFire.org - Bringing Transparency to the Great Firewall of China." Archived from the original on 18 May 2018. Retrieved 19 May 2018.

[10] Austin Hounsel, Prateek Mittal, Nick Feamster, "Automatically Generating a Large, Culture-Specific Blocklist for China." presented at the Advanced Computing Systems Association, 2018

[11] Introduction on the Golden Shield. Web. http://www.china.org.cn/chinese/zhuanti/283732.htm.

[12] Christopher Stevenson, "Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World," 30 B.C. Int'l & Comp. L. Rev. 531, 2007.

[13] Golden Shield Project. Web. https://en.wikipedia.org/wiki/Golden_Shield_Project#cite_note-ccw-22

[14] VPN Seller Sentenced to 3 Years in Jail. Web. https://mp.weixin.qq.com/s/j10ai_Sr1Xx09cnpk0yAjg

[15] Internet Access to China. Web. http://www.chinanews.com/special/guoqing/60/2009/06-25/122.shtml chinanews.com. Retrieved28 August 2013.

[16] S. Chandel, T. Ni and G. Yang, "Enterprise Cloud: Its Growth & Security Challenges in China," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, 2018, pp. 144-152.

[17] Oliver Farnan, Alexander Darer, Joss Wright, "Poisoning the Well – Exploring the Great Firewall's Poisoned DNS Responses," Workshop on Privacy in the Electronic Society, ACM, 2016.

[18] Jyh-An Lee & Ching-Yi Liu, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China, 13 Minn. J.L. Sci. & Tech. 125, 2012.

[19] Ignoring the Great Firewall of China. Web. https://www.lightbluetouchpaper.org/2006/06/27/ignoring-the-great-firewall-of-china/

[20] C. Mulvenon, James & S. Chase, Michael. Breaching the Great Firewall. Journal of E-Government, vol.2, pp.73-84. 2005.

[21] Z. Zhipeng et.al. "VPN: a Boon or a Trap? A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2018, pp. 510-515.

[22] JobTubeDaily (2018). How to use a VPN in China without Breaking the Law. http://mp.weixin.qq.com/s/BWSac-wv-f-xT0RRqJEMzw.

[23] Santoro, Michael A. "China 2.0: Illusion and Promise behind the 'Great Firewall.'" pp. 106–123, China, 2020

[24] Shao Zhuqing. "The survey about the status of Chinese citizens who visited the blocked websites." The checkout(blog) http://shaozhuqing.com/?p=2295

[25] Google Drive and Docs in China? Web. https://www.abacusnews.com/big-guns/google-drive-and-docs-china/article/2158441

[26] How Goldkorn, Jeremy, et al., editors. "The Chinese Internet: Unshared Destiny." Shared Destiny, Anu Press, 2015.

[27] January 2018 different VPN ranking list. Web. https://www.pingceji.com/guowai-vpn-ranking-2018-1

[28] Five of the most useful foreign VPNs in 2018 - based on a comprehensive comparison of multi-party performance. Web. https://www.pingceji.com/best-vpn-services-in-2018/

[29] PureVPN depth evaluation. Web. https://www.pingceji.com/purevpn-review-the-good-vpn-for-chinese/

[30] China Steps up VPN Blocks Ahead of Major Trade Expo. Web. https://mp.weixin.qq.com/s/xGv1X2GotYbyi8NK3irBjA

[31] Liu, Yakun and Yang, Dingcai. "Security Analysis of VPN." Journal of Beijing University of Posts and Telecommunications. 2003 (140-143), Vol. 26.

[32] Baijiahao (2018). An analysis of the supervision of VPN in China and how to use VPN services in compliance. https://baijiahao.baidu.com/s?id=1596346285526322054&wfr=spider&for=pc

[33] "What is internet censorship?" Amnesty International Australia. 28 March 2008. Archived from the original on 27 April 2015. Retrieved 21 February 2011.

[34] "Golden Shield Project phase II will focus on information integration and application." CCW Research (in Chinese). Archived from the original on 2009-05-31.

[35] Google and Tencent reached a patent cross-licensing agreement. Web. https://baijiahao.baidu.com/s?id=1589990616004104862&wfr=spider&for=pc

[36] Alert: VPN user fined for accessing international websites. Web. https://mp.weixin.qq.com/s/YabPj0nVaRESdqmIPZa8ZA

[37] China Begins Issuing Fines for Using VPNs - Yes, They are Illegal. Web. https://mp.weixin.qq.com/s/NrdAsCbgJGb-hVx49sLxAQ

[38] VPN Seller Sentenced to 3 Years in Jail. Web. https://mp.weixin.qq.com/s/j10ai_Sr1Xx09cnpk0yAjg

[39] Build a private VPN profit sentence about VPN; you do not know 10 things! Web. http://news.wehefei.com/system/2017/12/21/011170115.shtml

[40] VPN was banned, and only a few hundred over the wall software remained in the App Store in China. Web. https://www.aiyingli.com/48563.html

[41] "How to use VPNs in China without breaking the law," https://www.techworld.com.au/article/632635/how-use-vpns-china-without-breaking-law/

[42] "Search Engine Market Share China." http://gs.statcounter.com/search-engine-market-share/all/china

[43] "Over 70% Chinese will choose Google over Baidu if it returns". https://www.chinainternetwatch.com/26275/google-uncensored-search/

[44] How China Built the Great Firewall and How it Works. Web. https://mp.weixin.qq.com/s/J-NJm9we3q0zhLL0IzyMAA