A Study On Various Government Internet Restrictions and How To Get Around Them

Aiman Priester
Department of Electrical and Computer Engineering
Iowa State University
Ames, Iowa 50010
Email: priester@iastate.edu

***Abstract*—Information is meant to be free. Access to information should be granted to everyone who seeks it. However there are many governments around the world which intends to block this information to control their people. This paper dives into the state of internet censorship in three countries, China, Iran and Malaysia. Discussions are made on how their censorship systems work and their driving motivation behind their choice of system. The methods of restrictions are then discussed followed by how a user would potentially get around them. Research is done in hopes that future generations will be well equip ed to get around any censorship systems they face.**

1. Introduction

> Evolution rewards the most powerful creatures, and power is determined by the ability to access, harness, and manipulate information effectively.
>
> —Mark Manson, Everything is F*cked: A Book About Hope

Since the inception of TCP/IP in 1974, the internet has grown from strictly academic research use to something that we all use on a daily basis. It has been ingrained into our lives, so much so that the United Nations condemns internet access disruption as a "human rights violation" [1]. This technology allows us to connect with each other like no other civilization before us. Allowing us to communicate and collaborate to further mankind's never-ending mission to greatness. Ideas and criticisms get channelled through from all over the world allowing for new ways to enrich our lifestyles and help the needy. However, with information being at our fingertips, there are parties that are actively trying to slow this down to control and limit human innovation. These countries present these restrictions as benevolent. However, these restrictions can be seen as a way to control the masses. Painting authoritarian governments as beacons of freedom. Internet censorship is done in many countries. It is wrong to assume that most countries provide unfiltered access to the internet. In fact, a lot of the countries do filter out parts of the internet. In this paper, we will be discussing the methods that China, Iran and Malaysia use to filter and restrict internet access. Attempts to access website during simulations of time at the country, a view on how these filters work and methods to overcome the filter. This research aims to discuss in detail issues pertaining to internet censorship. Of which is;

- Providing an overview of censorship systems and different aims of censorship
- Provide insights on how the censorship is done
- Discuss implications and other novel ideas on censorship circumvention

2. State of Internet Censorship

Different countries employ different techniques to suppress information from the internet. The techniques used conforms to the level of urgency, balanced with cost of implementation. According to Dr. Vincent Poor at Princeton, censorship criteria can be further broken down into 8 parts which are [2]:

1) **Cost**
   Both monetary and opportunity cost associated with the implementation
2) **Scope**
   How far censorship is applied
3) **Scale**
   Reach of people can can be censored at a given time
4) **Speed**
   How quickly censorship can be deployed
5) **Granularity**
   Censorship resolution at different levels of the network
6) **False Negative**
   Censorship accuracy
7) **False Positive**
   Causes a load on censor resources
8) **Ease of Circumvention**
   How easily censorship is circumvented

These factors are the main considerations that governments around the world discuss when implementing censorship.

While one could argue that censorship in of itself does not physically drain the pockets of its citizens, it does take a toll on the their respective GDP. The fundamental design of the Internet, being as abstract as it is, allows for a plethora of different ways to circumvent censorship. Any physical damage to the network would cause an internet blackout. While some countries such as China look to enhance their Great Firewall, the countries' administration also acknowledges that a blackout outcome will not be ideal in their quest to strengthen their economy. As an outside observation, the key is to strike a balance where the censorship is enough to have a show of force, but to also keep their citizens in check.

2.1. China

According to Freedom House, China has scored a 10/100 in their Freedom On The Net Index in 2019 [3]. This low score is cause by a buffet of issues stemming from obstacles to access the internet, content limitation and violations of user rights [4]. Popular social media websites such as Facebook, Twitter and Instagram have been blocked. This is not inclusive of article congregation websites such as Reddit or any news websites such as The Washington Post [4]. Popularly, this is caused by China's Great Firewall by using legislative and technological methods to deny access to blacklisted foreign websites that are deemed not beneficial to the country [5].

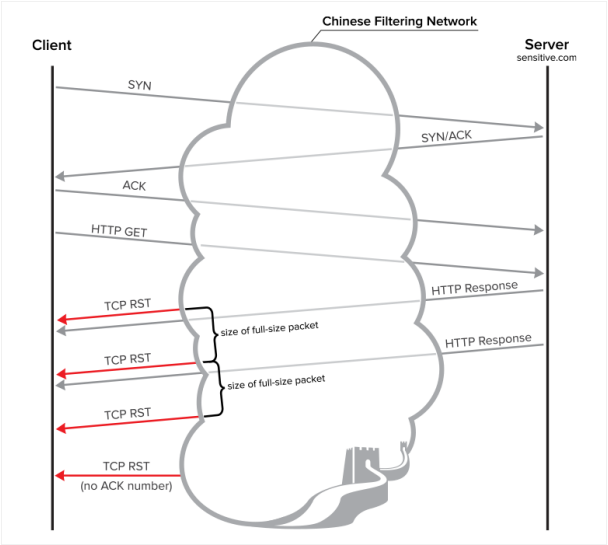

Figure 1. Simplified Overview of China's Network [6]

2.2. Iran

Iran scored relatively the same as China. The country scored 15/100 on the same index on the same year. Reports show that the internet penetration in Iran is upwards of around 70%, however the freedom to access various websites is limited [7][8]. The ability to access certain websites are dictated by the Supreme Council of Cyberspace of Iran (SCC), where 27 council members are directly selected by the current Supreme Leader of Iran. The council has the full authority to self determine and categorize websites or specific information that are considered "of evil intent" [8]. Iran's National Information Network (SHOMA), that will be completed in the near future, is poised to be the national Intranet where information is pulled and vetted by the SCC. In 2019, after widespread protests caused by a 50% to 300% increase in fuel prices, the Iranian government pulled the plug on the internet completely for a whole week in effort to quell the protests [9][10].

2.3. Malaysia

Malaysia does a much better on internet freedoms than China and Iran combined. Coming in at 57/100 it is scored as "partially free" [11]. However, a score like that is no cause for celebration. The Malaysian Communications and Multimedia Commission (MCMC) regulates internet usage. MCMC's policies are resonant of the Malaysian Government's directives. In 2015, the Malaysian Government banned access to SarawakReport, a news agency based in the United Kingdom, for exposing the then-Prime Minister of mishandling of sovereign funds [12]. Subsequent action was taken towards proposing the "Anti Fake News Bill 2018" to Parliament [13]. This proposal allows the government to effectively dictate definitions of fake news. Critics have said that this will allow the government to create their own narrative and penalise people who speak out against them. However, this bill was scrapped after the opposition party took power later that year [14]. The Pakatan Harapan (PH) government has lifted most barriers to press freedom and pledged to keep it that way [15]. But in spite of that, internet restrictions mostly remain for adult websites or certain file-sharing websites.

3. Restriction Methods

There are a plethora of different ways authorities can block or restrict access to the internet. Specific restriction implementations are in regard to criteria specified in §2. In this section, we will be exploring IP blocking, DNS hijacking, connection resets, keyword filtering and network disconnections.

3.1. IP Blocking

Blocking specific IP addresses is the simplest of all censorship techniques. A standard feature found in a router is the ability to drop all packets if it comes from a specific IP address. In China, this is done by having a global IP blacklist. Any attempts to connect to an IP on the blacklist will be denied through a technique called "Null Routing". Null routing works by having an active packet sniffer on a TCP connection and rerouting the user to a null or an error page on detection of attempted connection to a blacklisted IP

address. Upon closer inspection, null routing allows inbound traffic while restricting outbound traffic [16]. However due to the nature of a TCP handshake, the connection is broken as TCP requires a two-way interaction between user and server. With this technique, only a tiny load is added to they gateway router of ISPs and dedicated sniffing solutions are not required.

3.2. DNS Hijacking

DNS hijacking, also called DNS redirection, is where attackers or authorities attempt to incorrectly resolve DNS queries and have traffic redirected elsewhere. There are multiple types of DNS hijacking, attacking the user at different levels of the network namely, local, router, DNS server and middleman attack. All three governments discussed in this paper applies the middleman attack technique. This technique is often used alongside IP blocking. Once a sniffer detects a DNS connection, the node in the middle will serve a fake IP address that redirects user to a different website. The connection to the actual website is cut no packets are ever received by the intended server [2][17].

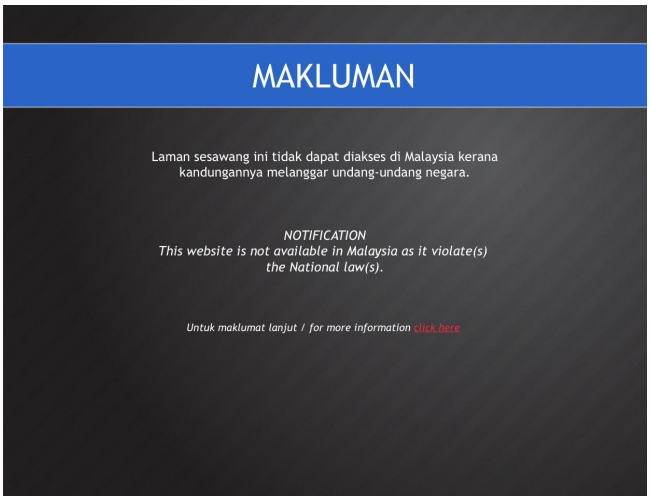

Figure 2. Redirected Page in Malaysia via DNS Hijacking

3.3. Connection Reset

Connection resets work by implementing a timer on a connection with a server that has been blocked. If a previous TCP connection is blocked by a global filter, a timer runs for a specified amount of time before a request can be processed to that server. However, this method is atomic to people using the same outbound router. This method is used alongside **Keyword Filtering**.

3.4. Keyword Filtering

While IP blocking and DNS hijacking are effective censorship techniques, they can only target websites at the domain level. However, an oppressive government is would likely aim to block information about a specific subject. Blocking all possible websites is not possible without a total disconnection from the internet. There is nothing stopping a seemingly politically apathetic website from having a blog post on how to liberate a country. Therefore, specific keyword filtering must happen. Any website enquiries with specified keywords will be blocked. Typically this is done by scanning the websites full Uniform Resource Locator (URL) [18]. As an example, a website with the domain name `priester.io` is likely to not have any useful information. However, keyword filtering will detect and perform a connection reset if the full domain is `priester.io/liberate-your-country-now/`. Governments are likely to raise an eyebrow at that link, the author would too. This method does not come without flaws. This method requires active sniffing of packets, which in turn causes a huge load on the last node of the internal network. To add to that, the word ”liberate” is not specific to getting rid of governments or even remotely causing dissatisfaction within the country. Therefore, countries are to use this technique with some caution as to not cause a false positive.

3.5. Network Disconnection

If all else fails and access to information, or lack thereof, is imperative to retaining the status quo, there is nothing stopping a government body from disconnecting the country from the internet completely. As discussed in §2.2, Iran shut off the internet to quell protesters from being able to gather. This is done by shutting off the main gateway, prohibiting any packets from entering or leaving the countries network. This method is only used in extreme cases. The Democratic People’s Republic of Korea (DPRK) or just North Korea for short, has perfected this method. Only top government officials, scholars and elites are allowed to access the internet. For the average Joe, the DPRK has setup a national intranet service called ”Kwangmyong” [19]. This intranet service is North Korea’s localized version of the internet where any information is sent around within the country. The government is in full control of information in the Kwangmyong. Like the free internet as we know it, the Kwangmyong does have its own internal search engine, email services and news portals (government owned, of course).

4. Censorship Circumvention

While governments around the world do their best to restrict information, people will always find solutions. Humans have a thirst for knowledge and nothing will stop someone from seeking that very knowledge. Hence, with every restriction, there are solutions to them. Some of them will require the active user to change connection settings and others will require the host to perform clever methods in circumventing government restrictions. This section details those very methods.

4.1. Web Proxy

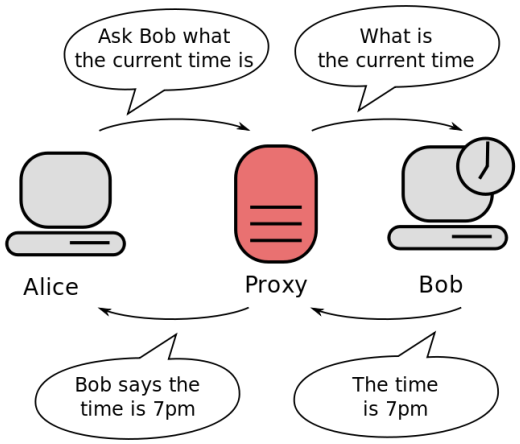

Figure 3. Simplified View of the Proxy Connection

A web proxy works as a middleman to connect to the internet.A proxy server is a special HTTP server that runs on a firewall machine [20]. The proxy waits for a request from the user for information, then requests the very same information from the server. The server then sends the requested information to the proxy server. The proxy server then relays that information to the user. This method ensures that the server never knows who and where the information is being sent. In terms of bypassing internet censorship, this method bypasses IP Blocking as it does not request information directly from the blocked IP address. This method is relatively easy to set up and maintain as IP addresses can change to avoid potential IP blocks.

4.2. SSH Tunneling

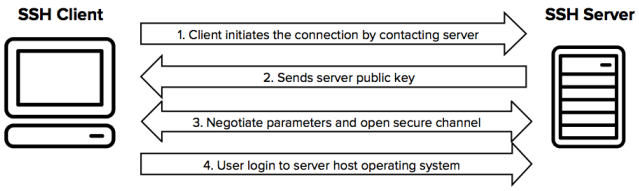

Figure 4. Simplified View of SSH Tunneling

Secure Shell (SSH) Tunneling uses cryptographic techniques to encrypt messages that are sent via the use of private and public keys. Typically SSH is used for command line and logins. However, SSH can be used to send messages from one place to another. A user aspiring to use this would first initiate a connection by contacting the server. The server then sends the servers public key. This public key is used in conjunction with a private key of the user in order to encrypt plain-text messages. The server then confirms parameters with the user and opens a secure channel. The encrypted message is then sent to the to the server. Internally, it is then decrypted. Therefore all packets in between the connection is secure. While cracking the encryption of the messages is out of reach for most people, government agencies such as the National Security Agency (NSA) have been shown to be able to intercept and decrypt the messages using their multimillion dollar supercomputers [21].

4.3. Virtual Private Network (VPN)

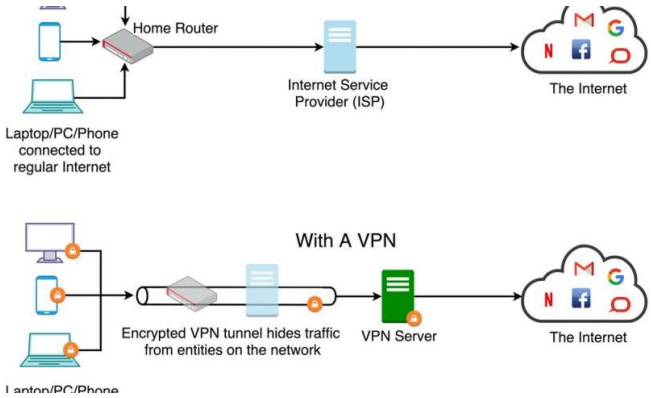

Figure 5. Top-Level View of a VPN

It seems that almost every tech video online will have a Virtual Private Network (VPN) sponsor. All with different features that aim to capture the attention of many. All of them sell the service under the guise of privacy and personal data protection. The use of a VPN is highly recommended, especially while using free public WiFi. VPNs work by hiding packet traffic within your network and routing them through a private network. In this case, instead of packet requests going straight to ISPs, the packets will be encrypted on the client side, go through the ISP and connect straight to the VPN server to handle any requests, shown in fig. 5. This can be viewed similarly to SSH described in a previous section. ISPs are not able to decipher the encrypted packets. Because the VPN server acts as a pseudo ISP, information such as location can be hidden as packets will have the source as the VPN server. This is useful in avoiding censorship as it goes around most methods of restrictions. It is still possible that governments around the world attempt to block the usage of VPNs. However, given the nature of VPNs and their dynamic IPs, it is no easy tasks. The Great Firewall of China has had great success in sniffing out VPN packets and persecuted those who attempt to use them [22]. In the guise of privacy, most VPN providers claim to keep zero logs on users activity. Unfortunately, some of them have been caught doing the contrary [23].

4.4. Anonymity Networks

Anonymity networks are a group of servers acting as bridges to one server to another. These server IPs are not publicly listed in effort to conceal where the information

originally came from. One could think of this as multiple VPNs stacked on top of each other, where information is encrypted at each node. A notable network goes by the name of The Onion Router (TOR). TOR redirects information from a client through a free, worldwide, volunteer network consisting of thousands of relays. Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested one on top of the other, like layers of an onion [24]. To request information or packets, the client would have to initially obtain a list of Tor nodes from a directory server. With this list, the computer randomly generates a path from the client to the host server, passing through TOR nodes, encrypted at every stage. When the host attempts to send information back to the client, information travels at a different, random route through the TOR network. Due to the dynamic nature of connecting to random nodes, and some nodes might be offline right after transmission, the information will be transferred anonymously. Knowing this, it might be tempting to double down. Why not add connect to a VPN and then connect to TOR? While this *should* help with privacy, using a VPN creates a permanent exit or entry node on the network. This makes TOR less secure if a client has a connection to a VPN provider that keeps logs [25].

4.5. Decentralised Hosting

Decentralised hosting, also called Peer-to-peer hosting, is another way of bypassing government censorship. This method is different than the ones discussed because it involves server hosting at multiple locations at once. There are two versions of this method. The first one involves mirroring the main website on multiple different hosts. The information contained on one host is the same as information on its mirror. This allows for multiple IP addresses to the same website. This method bypasses blanket bans on servers residing in a specific country. As an example, a quick google search on mirrors to ThePirateBay, a popular torrenting website, will display hundreds of different mirrors of the same website. Since these websites are essentially caches of each other, governments with the intention of blocking access to this website will have to query a large sum of servers. By the time censorship takes place, it is likely that the IP address is no longer used, rendering censorship efforts useless. The second version of this involves thousands of different servers around the world. The full file that is requested is broken up and transferred from thousands of different computers simultaneously. If a few servers disconnect, other computers pick up the progress and continue from there.

4.6. Notable Mentions

We have discussed typical methods of getting around government censorship. However there are a few efforts towards freedom of information that deserves a mention.

Satellite Internet: By transmitting internet connection down to Earth via satellite, this will get around total disconnection from the internet by oppressive regimes. Information will not be transferred via the countries' end points, but rather straight to the satellite. An example to this is Project Starlink by Space X.

The Uncensored Library: Even where most information is blocked, the popular game, Minecraft, is not. This lead a group of Minecraft design volunteers to team up with Reporters without Borders to create a save file that has a building with uncensored news from a few countries around the world. Users can enter rooms in game represented by countries with oppressive governments to read up on events that are covered up [26].

5. Conclusion

While there are many attempts to block information to the common man, there are always some that will fight for freedom of information. Whether it is as simple as IP Blocking, or as extreme as total disconnection, humans will collectively find solutions to create a freer world. It is important to note that this is not an exhaustive list on how information is being censored as new technologies are being developed around the clock for benevolent and malicious intent. Author hopes that future work will involve enabling access to millions around the world to open their eyes and rise up to the oppressors.

Acknowledgments

I would like to thank Dr Doug Jacobson, for teaching CPRE 530 which has allowed me to learn about numerous taxonomy within the realm of internet and internet security. I would also like to thank both of my parents for continously supporting my dreams to obtain a world class education from Iowa State. Furthermore, I would like to thank my partner, Farra Aleisya for being a personal cheerleader and companion throughout my study efforts. Last but not least, I would like to thank Ahmad Nazar for being a great person and a tremendous friend who I will cherish for years and years.

References

[1] James Vincent. *UN condemns internet access disruption as a human rights violation*. July 2016. URL: https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access.

[2] Christopher Leberknight et al. "A Taxonomy of Internet Censorship and Anti-Censorship". In: (Jan. 2012).

[3] FreedomHouse China. *China*. URL: https://freedomhouse.org/country/china/freedom-net/2019.

[4] Alexa GreatFire. *Censorship of Alexa Top 1000 Domains in China*. URL: https://en.greatfire.org/search/alexa-top-1000-domains.

[5] Paul Mozur. *Baidu and CloudFlare Boost Users Over China's Great Firewall*. Sept. 2015. URL: https://www.nytimes.com/2015/09/14/business/partnership-boosts-users-over-chinas-great-firewall.html.

[6] Yong Xu. *Deconstructing the Great Firewall of China*. Apr. 2019. URL: https://blog.thousandeyes.com/deconstructing-great-firewall-china/.

[7] ITU. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[8] UK FilterwatchIR. *Filterwatch // August 2017*. URL: https://smallmedia.org.uk/news/filterwatch-august-2017.

[9] Ivana Kottasová. *What makes Iran's internet blackout different*. Nov. 2019. URL: https://edition.cnn.com/2019/11/19/middleeast/iran-internet-shutdown-intl/index.html.

[10] Author: Farnaz Fassihi Gladstone and Rick. *Iran Abruptly Raises Fuel Prices, and Protests Erupt*. Nov. 2019. URL: https://www.iranwatch.org/news-brief/iran-abruptly-raises-fuel-prices-protests-erupt.

[11] FreedomHouse Malaysia. *Malaysia*. URL: https://freedomhouse.org/country/malaysia/freedom-net/2019.

[12] M. Kumar. *MCMC blocks access to Sarawak Report website*. Dec. 2015. URL: https://www.thestar.com.my/News/Nation/2015/07/19/MCMC-block-sarawak-report/.

[13] Nazura Ngah. *FAQs: What you need to know about the Anti-Fake News Bill 2018: New Straits Times*. Mar. 2018. URL: https://www.nst.com.my/news/nation/2018/03/349691/faqs-what-you-need-know-about-anti-fake-news-bill-2018.

[14] The Star Online. *Finally, Dewan Negara approves repeal of Anti-Fake News Act*. Dec. 2019. URL: https://www.thestar.com.my/news/nation/2019/12/19/finally-dewan-negara-approves-repeal-of-anti-fake-news-act.

[15] Bernama. *PH supports press freedom but with certain limits: New Straits Times*. May 2018. URL: https://www.nst.com.my/news/nation/2018/05/369061/ph-supports-press-freedom-certain-limits.

[16] Daniel Anderson. "Splinternet Behind the Great Firewall of China". In: *Queue* 10.11 (Nov. 2012), pp. 40–49. ISSN: 1542-7730. DOI: 10.1145/2390756.2405036. URL: https://doi.org/10.1145/2390756.2405036.

[17] Borges Esteban. *SecurityTrails: DNS Hijacking: How to Identify and Protect Against It*. June 2019. URL: https://securitytrails.com/blog/dns-hijacking.

[18] Anne Henochowicz. "The Human Side of Censorship: Keyword Filtering and Censorship Directives on the Chinese Internet". In: Washington, D.C.: USENIX Association, Aug. 2015.

[19] Andrew Jacobs. *Visit by Google Chairman May Benefit North Korea*. Jan. 2013. URL: https://www.nytimes.com/2013/01/11/world/asia/eric-schmidt-bill-richardson-north-korea.html.

[20] Ari Luotonen and Kevin Altis. "World-Wide Web proxies". In: *Computer Networks and ISDN Systems* 27.2 (1994), pp. 147–154. DOI: 10.1016/0169-7552(94)90128-7.

[21] Dan Goodin. *How the NSA can break trillions of encrypted Web and VPN connections*. Oct. 2015. URL: https://arstechnica.com/information-technology/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/.

[22] Michael Gargiulo. *Which Countries Block VPNs, and Why?* June 2020. URL: https://www.vpn.com/guide/which-countries-block-vpn/.

[23] PAUL BISCHOFF. *"Zero logs" VPN exposes millions of logs including user passwords, claims data is anonymous*. July 2020. URL: https://www.comparitech.com/blog/vpn-privacy/ufo-vpn-data-exposure/.

[24] TOR. *The Tor Project: Privacy Freedom Online*. URL: https://www.torproject.org/about/history/.

[25] TOR2. *Introduction*. 2019. URL: https://trac.torproject.org/projects/tor/wiki/doc/TorPlusVPN.

[26] Amy Woodyatt. *Minecraft hosts uncensored library full of banned texts*. Mar. 2020. URL: https://edition.cnn.com/2020/03/13/tech/minecraft-uncensored-library-scli-intl/index.html.