Internet Censorship: An Integrative Review of Technologies Employed to Limit Access to the Internet, Monitor User Actions, and their Effects on Culture

Joseph Hyland

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2020

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____

David Holder, Ph.D.
Thesis Chair

_____

Philip Schall, Ph.D.
Committee Member

_____

Cindy Goodrich, EdD
Assistant Honors Director

_____

Date

Abstract

The following conducts an integrative review of the current state of Internet Censorship in China, Iran, and Russia, highlights common circumvention technologies (CTs), and analyzes the effects Internet Censorship has on cultures. The author spends a large majority of the paper delineating China's Internet infrastructure and prevalent Internet Censorship Technologies/Techniques (ICTs), paying particular attention to how the ICTs function at a technical level. The author further analyzes the state of Internet Censorship in both Iran and Russia from a broader perspective to give a better understanding of Internet Censorship around the globe. The author also highlights specific CTs, explaining how they function at a technical level. Findings indicate that among all three nation-states, state control of Internet Service Providers is the backbone of Internet Censorship. Specifically, within China, it is discovered that the infrastructure functions as an Intranet, thereby creating a closed system. Further, BGP Hijacking, DNS Poisoning, and TCP RST attacks are analyzed to understand their use-case within China. It is found that Iran functions much like a weaker version of China in regards to ICTs, with the state seemingly using the ICT of Bandwidth Throttling rather consistently. Russia's approach to Internet censorship, in stark contrast to Iran and China, is found to rely mostly on the legislative system and fear to implement censorship, though their technical level of ICT implementation grows daily. TOR, VPNs, and Proxy Servers are all analyzed and found to be robust CTs. Drawing primarily from the examples given throughout the paper, the author highlights the various effects of Internet Censorship on culture – noting that at its core, Internet Censorship destroys democracy.

Keywords: Internet Censorship, Circumvention Technologies, China, Russia, Iran, BGP Hijacking, DNS Poisoning, TCP RST Attacks

Internet Censorship: A Meta-Analysis of Technologies Employed to Limit Access to the Internet and their Ensuing Effects on Culture

Introduction

Throughout history there have been a plethora of disruptive technologies which have completely reshaped the way the world functions. Take for example the revelation made by Michael Faraday in 1831 about how electricity is generated, or the invention of the telephone by Alexander Graham Bell in 1876, or even the "invention" of the personal computer in the mid-1970s. Each revelation or breakthrough listed above fundamentally changed the world. Much in the same way as the previous breakthroughs, the creation of the Internet in the early-1970s, and the proceeding widespread adoption in the mid-1990s, also completely changed the way the world functioned. The Internet is the primary mode of communication for the majority of the world, the primary mode of information dissemination, and is fast becoming (if not already) the primary mode of education. As such, uninhibited access to the Internet by any individual is of the utmost importance – because access to the Internet is access to modern society. For totalitarian states, the use of the Internet poses a threat because of what it provides – namely, information and access to people, which are two fundamental building blocks of individual freedom. Paired with the ever-increasing influence of Social Media, which has a well-documented history as a tool of social protest (Hu & Zheng, 2019), the threat uninhibited access to the Internet poses to tyrannical governments grows daily. Totalitarian states such as China, Russia, and Iran all employ a plethora of Internet Censorship Technologies & Techniques (ICTs) whose primary purpose is to limit or completely cut off individuals' access to the Internet. In spite of their efforts, circumvention technologies have become widely available, and the adoption of said technologies continues to grow. In light of the current state of countries such as China, Russia,

Iran, and others, an analysis of Internet Censorship is timely. This includes the ICTs used, an overview of the Internet infrastructure of China, specifically, an overview of the circumvention technologies used, and the effects Internet Censorship has on the populace.

The other Great Wall: The Great Firewall (GFW)

Background

Out of all the countries that employ ICTs liberally, China is the most notorious, and by far the most sophisticated (Bradbury, 2011), which is not surprising, particularly in light of other actions taken by the state. Take, for example, the recent 2018 decision by the Communist Party of China (CPC) to abolish term limits, or the creation of a "social score" to rate the trustworthiness of citizens (Ramadan, 2018). Each of the proceeding examples points to a blatantly obvious conclusion: the Chinese state values control over all else, and what better way to control a populace than by limiting their access to the most prevalent communication medium. Commonly given the moniker of "The Great Firewall", China's Internet Censorship attempts are far-reaching and invasive. One might say that censorship is at the core of who China as a country is, and an analysis of the ICTs employed would give credit to such an assertion. China's relationship with the Internet is particularly interesting because of their economic system. In the mid-1970s, on the back of economic stagnation, China opened itself to foreign markets, which precipitated massive economic growth which has continued to last into present-day (Hall & Zhou, 2017). Because of the pseudo-western economic system, China's relationship with the Internet is akin to a double-edged sword: it is both a money-making machine, a powerful propaganda apparatus, and a source of political views contrary to the regimes own (Feng & Guo, 2013). The threat is only compounded by the vast amount of Internet users in China, which totaled 854.5 million, or roughly 61.2% of the population, by June of 2019 (CNNIC, 2019). As a

comparison point, the total amount of Internet users in China is greater than the total users of Japan, Russia, Mexico, and the United States combined. The growth rate is particularly striking given that only about 10.5% of China's population used the Internet in 2006 (CNNIC, 2017). The driving factor behind the astronomical growth is due primarily to 3 things: the widespread use of mobile devices, the widespread use of instant-messaging/communication apps, and the widespread use of video services (CNNIC, 2019). Respectively, 99.1% (847 million), 96.5% (825 million), and 88.8% (759 million) of China's netizens use mobile devices, instant messaging/communication apps (social media), and online video services, respectively (CNNIC, 2019). While it is true that Chinese netizens have access to Social media/communication apps, they must comply with Chinese laws on content control and user monitoring (Lotus, Knockel, Ng, & Crete-Nishihata, 2016), thereby severely limiting their use. While the Chinese government has many ICTs built into various platforms, the backbone of their internet censorship attempts begins with the overall structure of the Internet in China, which is tailored specifically for government control.

Internet Infrastructure Overview

Many individuals believe that the Internet is a unitary structure, meaning that it would be one massive network (Naughton, 2016). But, contrary to such a belief, the Internet is actually a network of networks which communicates via a predefined ruleset known as Transmission Control Protocol/Internet Protocol, or TCP/IP, as it is commonly known (Naughton, 2016). Different entities and organizations (usually private sector) around the world own and operate different backbone networks, and through a series of gateway routers, enable connections between different devices (Naughton, 2016). The keyword in the preceding sentence is private. In the United States, for example, a number of private-sector Internet Service Providers (ISPs),

such as AT&T, Verizon, Comcast, etc. have massive internet backbones that their customers run off of. The infrastructure of China's internet is much the same. It is built with a top-down hierarchical approach, uses ISP backbones as the starting points for connection, and employs gateway routers for broader connection between networks (Feng & Guo, 2013). The major difference between China's Internet Infrastructure and that of the rest of the world is ownership – A large majority of the world's ISPs are private companies. China's ISPs, on the other hand, are state-owned and state-run entities, making them not much more than an extension of the government itself (Feng & Guo, 2013).

The International bandwidth (speed of transmission) and gateways are strictly controlled by 6 state-owned and operated Internet companies, but there are only three that are widely used by the public (Feng & Guo, 2013). Two of the major corporations, China Unicom and China Telecom have the majority of the bandwidth for regular Internet access, whereas China Mobile, which is the largest mobile internet provider, has the majority of the mobile bandwidth (Feng & Guo, 2013). The other 3 providers, China Science and Technology Network, China Education and Research Network, and China International Economy and Trade Net, are smaller networks with significantly less bandwidth allocated and are mostly used for research purposes (Feng & Guo, 2013). From the six state-run ISPs, the structure can be thought of as a series of 3 concentric circles, with each circle representing a level of access. Within the innermost circle there is domestic and school traffic which is routed to local ISPs that are also state-owned (Feng & Guo, 2013). Within the second circle, there are three national Network Access Points (NAPs) that are extensions of the six primary ISPs in China (Feng & Guo, 2013). The NAPs are a strategic part of China's Internet Censorship attempts in that they allow the ISPs to either increase the bandwidth transmission rate within the country, or decrease it (Feng & Guo, 2013).

Within specific major cities in China, there are 8 major backbone nodes whereby all other network nodes in the smaller cities are forced to access from (Feng & Guo, 2013). Within the last circle are the international Internet Gateways, and they are the last gateway for outgoing requests for access to foreign websites, and the first gateway of foreign requests for websites hosted within China (Feng & Guo, 2013). Because they are the last gateways before the internet traffic is routed to gateways outside of the state's control, they are the most important part of China's Internet infrastructure (Feng & Guo, 2013). All 6 of the major ISPs have their own international Internet gateways, but for the most part, China Telecom and China Unicom are responsible for the majority of traffic. Interestingly, research indicates that China operates much like an Intranet (Feng & Guo, 2013), meaning that the entire system is a closed-loop, which enables the government to keep tight control of what happens across the entirety of the Internet.

Internet Censorship Technologies & Techniques Used in China

Border Gateway Protocol Hijacking

The ICTs employed by China are numerous and quite sophisticated. Some censorship technologies are baked into platforms such as Baidu, China's most popular search engine, which blocks access to certain websites (Jiang, 2014). Other ICTs are much more general, such as DNS hijacking and keyword blocking, which also have a pervasive history of use within China and other totalitarian states (Aceto & Pescape, 2015). One censorship/monitoring technique that is used within China and other countries, although somewhat sparingly, is the use Border Gateway Protocol Hijacking, known as BGP Hijacking (Aceto & Pescape, 2015). To transfer data across a packet-switched network, packet-forwarding is used, whereby a routing algorithm determines the destination of the packets (Aceto & Pescape, 2015). The routing algorithm used in the case of data being set across administrative boundaries is the Border Gateway Protocol, and if changes

are made such that the path to the next destination is invalid or subverted, it can affect sub-networks, and even an entire countries network (Aceto & Pescape, 2015).

On a technical level, the Border Gateway Protocol governs the exchange of routing information between Internet Entities, known as Autonomous Systems (AS) (Wan, Oorschot, & Kranakis, 2005). Simplistically, ASs are large groups of networks with many routers governed and owned by individual entities (Chiesa, Battista, Erlebach, & Patrignani, 2015). For example, AS 7018 belongs to AT&T, whereas AS 701 and AS 702 are owned and operated by UUNET (Wan et al., 2005). Using the BGP, ASs can propagate and exchange routing information by constantly updating their routing tables with the latest routes and sharing them between neighboring ASs (Kent, Lynn & Seo, 2000). This is important because as previously stated, the Internet is a network of networks, which means requests made by users are propagated across many intermediate systems (ASs) before they reach the intended destination. The BGP enables a request to not only take the correct path, but also the most efficient. As a more concrete example, one can imagine the BGP as a postal system, and ASs as post offices, whereby routing information is exchanged and the request is propagated to the next AS, which has further routing information for the request until it reaches its final destination. There are many different routing protocols and algorithms in use, but BGP is arguably the most important because “it is the only inter-domain routing protocol used on the Internet for exchanging reachability information between ASs” (Wan et al., 2005). The goal of the BGP hijacking is to redirect traffic from the destination AS to a malicious AS, thereby routing users’ data to the incorrect location (Chiesa et al., 2015). Basically, the message is sent to the wrong destination. The ramifications of BGP Hijacking, if performed correctly, are massive. Take, for example, the accidental 2008 hijacking of YouTube by Pakistan Telecom. Pakistan Telecom desired to block access to YouTube within

the country by redirecting traffic to a null route (Balakrishnan, 2009). They accomplished this by advertising a /24 prefix for the range of addresses which YouTube resolved to, but instead of being applied locally, the announcement was passed upstream to one of Pakistan Telecom's ISPs and because of the way BGP functions on a technical level, the announcement was broadcasted globally, thereby redirecting all traffic to YouTube to Pakistan Telecom (Balakrishnan, 2009). In regards to China specifically, they have a checkered history when it comes to BGP Hijacking, with some of the most notable cases being attacks against foreign governments (Demchak & Shavitt, 2018). For example, as early as 2010 China has had noted incidents of possible BGP Hijacking (Hiran, Carlsson, & Gill, 2013), but in 2016 and early 2017, China engaged in covert BGP attacks on foreign entities. For 6 months in 2016, China Telecom hijacked the routes from Canada to South-Korean government sites, routing all traffic through systems in China before it was routed to South-Korea (Demchak & Shavitt, 2018). Another example is the 2016 case of the United States and Italy, in which China Telecom redirected traffic going from the U.S. to Milan to themselves (Demchak & Shavitt, 2018). In this particular case, they were unable to redirect the traffic from China to Milan, so the information was dropped completely (Demchak & Shavitt, 2018), making it more obvious that there had been foul play. Yet another example is the 2017 case of Scandinavia and Japan. For a period of 6 weeks, traffic from Sweden and Norway to the Japan outlet of a large American News organization was hijacked (Demchak & Shavitt, 2018). As one can see, China's actions around the world mirror the actions they take within their own state, with the exception of being more covert. Within their own country, China does not need to employ BGP Hijacking secretly, given the structure of their Internet. it is quite literally designed around the principle of user monitoring and spying. For example, IP Address Blocking, a common form of censorship within China, uses BGP Hijacking to insert a list of blocked

addresses into the routing table of gateway routers within China, thereby completely cutting off access to specific sites (Anderson, 2012).

Domain Name System (DNS) Poisoning

In conjunction with previous censorship techniques, DNS poisoning is a common ICT used in China to deny individuals access to internet resources (Farnan, Darer, & Wright, 2016). Whenever a user types in the domain name of an internet address they want to go to, a query is made to a DNS resolver, which resolves the name the user inputted into an Internet Protocol (IP) address, which is the computer-readable address to the requested website. Structurally, there are generally 3 phases or levels a request goes through before the response is sent back to the user: the root level, the top-level domain, and the authoritative name server. When a user requests a webpage, the DNS resolver, which is generally the name server operated by a user's ISP, checks its cache to determine whether it has the IP address in memory. If it does not, the request is sent to the root server, which has the IP addresses of all the top-level domain servers, (i.e., .com, .gov, .edu, etc.), and sends it to the appropriate top-level domain server associated with the name. The top-level domain server then determines what domain type the request is and sends the request to an authoritative name server that has the information about the specific domain. For example, to reach Google.com, the root server is queried, which then sends the request to the top-level domain server associated with the .com domain, which then sends the request to the authoritative name server that has the necessary IP information about the Google domain, which then sends the request back to the ISP's resolver. The resolver then sends the IP address back to the user and displays the contents of Google.com. It should be noted that often, certain IP addresses are stored locally on the user's computer, particularly when they are consistently accessing a specific site. By storing locally, the time between query and response is cut down, thereby providing the

necessary information much faster.

In the case of DNS Poisoning, when certain censorship technologies detect a query for a banned domain, they respond by hijacking the DNS response, sending a poisoned response to the DNS resolver (Farnan et al., 2015). Due to network structures and the fact that the poisoned response is sent to the resolver before the legitimate response, the DNS resolver generally responds before the correct DNS address is sent, which in effect, cancels the legitimate response from ever reaching the user (Anonymous, 2012). Not only is the wrong address sent back, but the resolver actually caches (stores/saves) the response for future use, thereby 'poisoning' the DNS server (Farnan et al., 2015). The ease with which DNS poisoning can be accomplished is rather astonishing. If a malicious actor has access to any of the links along a DNS query route, packet injection can take place, responding with a forged result, but with the appropriate query question and protocol identifiers (Anonymous, 2012). The attacker can then map the response to a dead end, or a domain controlled by them (Anonymous, 2012). Research indicates that the majority of China's DNS servers themselves, not just the resolvers, are poisoned (Farnan et al., 2015), which in effect, would nullify their ability to provide accurate results. Indeed, a study was conducted inquiring about DNS responses of resolvers in China, and out of more than 800 separate resolvers, 99.88% were adversely affected by China's GFW (Lowe, Winters, & Marcus, 2007). Because of the way DNS servers share information, poisoned results which have been cached can spread to other DNS servers (Lowe et al., 2007), thereby effecting systems outside the intended target group. Keeping in mind that the Internet is not a unitary structure, but a network of networks, studies have shown that China's pervasive DNS injection and poisoning has affected resolvers outside of the country, particularly in areas such as Korea (Anonymous, 2012). Oddly, the .de Top-level domain, which is associated with entities in and around Germany

seems to be very much affected by DNS poisoning from China because of the amount of traffic passing through China before it reaches Germany (Anonymous, 2012).

TCP Reset (RST) Attacks via Keyword Filtering

Whenever data is being transferred over a network, it follows a specific pattern and interaction hierarchy. From an abstracted standpoint, the interactions can be broken down into distinct layers, each performing a specific function. The most prevalent model of interactions is known as the OSI model, and it consists of the following 7 layers: Application layer, Presentation layer, Session layer, Transport Layer, Network layer, Data link layer, and the Physical layer (Bora, Bora, Sing, & Arsalan, 2014). While a full analysis of each layer would prove useful, of interest is the transport layer. Within the transport layer, there is the Transmission Control Protocol (TCP), which deals primarily with establishing a connection between devices, packaging and sending data between computer nodes, and retransmitting the data if necessary. Of primary importance is the fact that TCP is responsible for establishing (and maintaining) a connection between nodes. For example, if a server wants to send a file, it will request that a connection be made via TCP, and TCP will then package the data and send it. Due to TCP functionalities, it is exploitable via what is commonly known as TCP reset attacks.

The infrastructure of China's Internet is set up as an Intrusion protection system, which (theoretically) enables every piece of data sent across the network to be inspected (Anderson, 2012). As such, the transmission of data containing elements that are considered 'bad' or banned can be completely terminated via TCP RST attacks. Taking note of how data is transferred from a local system to a neighboring system, normally when a packet arrives at a router it is placed in a queue to be transferred to the next location (Clayton, Murdoch, & Watson, 2006). In the case of data being transferred inside China, when a packet arrives at a router, it very well may be

placed into a queue to await further transmission, but it is also sent to an out-of-band Intrusion Detection System (IDS) (Clayton et al., 2007). It should be noted that when a device is out-of-band it simply means that it is connected to the devices on the main network, but it resides on its own network, isolated from the main network. Generally, access to an out-of-band device is limited to administrators, and there is not 2-way access, meaning the out-of-band device can manipulate and see the devices on the main network, but not the other way around. The out-of-band IDS analyzes the packets being sent using keyword filtering to determine if it contains any 'bad' content (Clayton et al., 2007) In the case that the IDS does flag contents in the packets, three TCP reset packets with three different sequence numbers are generated and passed to the router to be sent to the destination of the user request so as to terminate communication between the devices (Clayton et al., 2007). If the IDS can also determine the transport level port numbers, they can censor not only by IP address and keyword filtering, but also by the application being used, such as Hypertext Transfer Protocol, Secure Shell, and others (Aceto & Pescape, 2015). While TCP reset attacks are prevalent, there are ways around them, such as deliberately ignoring the TCP reset packets. Bearing in mind that the Internet runs off certain protocols (i.e. rulesets), computer nodes have the ability to filter content that passes through a firewall based on certain criteria (Shinder & Cross, 2008). In the case of TCP reset attacks, the receiving node can specify that the firewall being used completely ignore any TCP RST packets, (Clayton et al., 2007), thereby nullifying their ability to sever the connection. While TCP reset attacks are still in use, because of the latter example and others, their effectiveness has been drastically decreased over time.

Internet Censorship Around the World

Iran: China 1.0

Far from a haven for individual freedom, the totalitarianism of Iran very much extends into the use of the Internet, with watchdog groups consistently labeling the country as one of the worst offenders of Internet freedoms (Aryan, Aryan, & Halderman, 2013). As in the case of China, the ICTs used by Iran are pervasive, deriving from the same starting point: state control of ISPs (Warf, 2011). Iran's state-owned telecommunications monopoly, Telecommunication Company of Iran (TCI), is the backbone network to which all ISPs are forced to connect to (Anderson, 2013). Additionally, every ISP in the country must agree to censor content according to a growing list of content deemed 'criminal' by the Iranian government and can be held accountable for the actions their users take while using their services (Anderson, 2013). As of 2001, the government of Iran assumed complete control over all international traffic entering or leaving the country (Warf, 2011). Iran also has a wide array of Internet content that is outright banned, such as content that insults Islam, promotes national discord, promotes immoral behavior, etc. (Warf, 2011). Freedom of expression is even further limited by the fact that individuals must obtain licenses from the Ministry of Islamic Culture and Guidance for running both websites and blogs, or risk being declared illegal by the Iranian government. The speed of data transmission is incredibly inconsistent, with speeds faster than 128kbps being declared illegal, at one point in time (Warf, 2011). As for specific ICTs, Iran employs a plethora of them: Deep Packet Inspection, keyword filtering, DNS hijacking/poisoning, protocol-based throttling, etc. (Warf, 2011; Aryan et al., 2013). While the above forms of censorship are all used rather frequently, one of the most prevalent forms of censorship is bandwidth throttling (Anderson, 2013).

Bandwidth throttling is exactly what it sounds like: the intentional slowing of an internet

connection by an ISP or some entity with access to network configurations. While the government in Iran does occasionally engage in bandwidth throttling for legitimate reasons, such as network congestion, but studies indicate that they also significantly throttle the bandwidth during times of planned protests, political unrest, holidays, important dates, such as the Arab Spring, and other such occurrences (Anderson, 2013). In addition, bandwidth throttling is almost engaged in parallel with more overt forms of censorship, such as filtering of secure Google services, or the jamming of international broadcasts (Anderson, 2013). For example, during the 2012 Anniversary of the detention of prominent Iranian election protest leaders Mehdi Karroubi and Mir-Hossein Mousavi, there was a significant decline in bandwidth that precipitated the event (Anderson, 2013). Now, the case can be made that the throttling could be due to the poor Internet infrastructure of Iran, which is valid, but the timing of the outages, as well as the duration and the amount of network degradation, cannot be explained, even taking into account the former contention, when compared against normal fluctuations (Anderson, 2013). Or take for example the 2009 elections in Iran, where mass protests began because of perceived election fraud. During the events, there were a series of network shutdowns, as well as the wholesale blocking of mobile texting networks (Rahimi, 2015). Not only are the basic connections to the Internet throttled, but specific applications, such as HTTPS, SSH, and VPN tunnels have been known to be throttled regardless of what is happening in the country (Aryan et al., 2013). A study conducted in 2013 showed that when researchers engaged in a file transfer using HTTP and HTTPS, 85%-89% of possible bandwidth was used, but when researchers engaged in file transfer using SSH, only 15% of total bandwidth was used (Aryan et al., 2013). From the research, it seems that the Iranian government uses a whitelist for desirable protocols, blocking or severely limiting any protocols outside of the list (Aryan et al., 2013). In conjunction with the

consistency of bandwidth decreases around events or dates/times the Iranian government is wary of, a strong case is laid forth for a pattern of behavior which indicates that the Iranian government engages in manipulation of user bandwidth and manipulation of network access.

In addition to bandwidth throttling, one of the more concerning developments is the fact that the Iranian government is trying to create a closed system, (Intranet), much like China (Rahimi, 2015). The primary motivation for the system seems to be twofold: monitoring users and creating in-house services (Rahimi, 2015). The creation of a closed system would enable wholesale monitoring of all users on the network without the need for a complex and costly censorship apparatus, while the creation of in-house services would further enable the Iranian government to tighten their grasp around Iranian citizens, primarily by creating a monopoly on online services and media platforms, forcing citizens to only use the prescribed platforms (Rahimi, 2015).

Russia: Censorship Through Fear

The dynamic of internet censorship within Russia is interesting because of the pace at which Russia has censored the Internet – slowly. Instead of a mad grab for power, Russia's authoritarian leader, Vladimir Putin, slowly acted, both covertly and openly, to extend the government's control of the Internet within Russia (Warf, 2011; Soldatov, 2017). Not only is the pace of censorship of interest, but also the fact that the Russian government had done very little to censor the Internet before 2012 (Nisbet, Kamenchuk, & Dal, 2017). Indeed, Internet Freedom watchdog groups had seen very little movement in their attempts at Internet Censorship, with Russia generally hovering around the middle of the pack when compared to other countries, in stark contrast to their media censorship rankings, which were near the top (Nisebet et al., 2017). But between 2012 and 2015, there was a sharp increase in their attempts to censor access to the

Internet, with their “Internet-Freedom” score moving +10 points (higher is worse) in 3 years (Nisbet et al., 2017). Interestingly, the means employed to increase the Russian government's control of the Internet have been primarily through the legal system, with the government passing a series of laws that drastically increased their power over internet use. This highlights a key distinction between Russia’s Internet Censorship apparatus and approach relative to other countries: In the Russian system, ICTs themselves are not the primary means of Internet censorship – fear, mass media brainwashing, and the legal system is (Soldatov, 2017).

During its first 20 years of existence, the Russian Internet developed as a free and open platform, mostly free of invasive censorship (Soldatov, 2017). Indeed, one reason ICTs have taken a backseat to more traditional means of censorship is because the Russian Internet was not built to be censored (Soldatov, 2017). The infrastructure behind it, unlike China, did not have the censorship technologies in place to effectively monitor it (Soldatov, 2017). Even today, the ICTs, while increasing, still primarily act as deterrents aimed at ensuring continual loyalty of ISPs and general Internet users (Soldatov, 2017). By no means is this to say that the Russian government does not want complete control over the Internet via ICTs – it is plainly obvious that they do (Duffy, 2015), as is evidenced by their aggressive restrictions of Internet freedoms. The catalyst for the swift stance-shift seems to have been the 2011 elections (Duffy, 2015). Proceeding the elections, there were mass protests, both on social media services and in real life, with protests gathering as many as 100,000 people at times (Duffy, 2015). Following the protests, the Russian government enacted a series of laws that laid the groundwork for their censorship apparatus (Soldatov, 2017; Duffy, 2015). Beginning with Federal Law No. 89417-6, formally titled as “On the Protection of Children from Information Harmful to Their Health and Development”, the Russian government began their censorship (Soldatov, 2017; Duffy, 2015). The proceeding law

created what are known as blacklists, which, much like the Chinese government has, are lists of websites and content that are blocked via IP address and domain name (Duffy 2015). The law was incredibly vague, and it gave the Federal Division Roskomnadzor, the Russian equivalent to the FCC, unprecedented power to censor practically any content the Russian government deemed inappropriate (Duffy, 2015). The blacklist was immediately put to use, with 4000 websites being blocked after only 4 months, with the use continually rising as time went on (Duffy, 2015). The law has been used to target a vast array of different groups, especially independent news sites (Duffy, 2015).

The blacklist law was only the beginning of the Russian government's censorship attempts, which drastically increased during 2014, with the Russian government passing a series of laws severely limiting Internet freedoms and drastically increasing surveillance capabilities (Duffy, 2015). In April 2014, two incredibly broad 'antiterrorism' laws were passed stating that owners and operators of websites and various services were required to store practically all data that goes to and from their systems, and that anonymous online money transfers were now illegal (Duffy, 2015). In May of 2014, a law effectively known as the "Bloggers Law" made bloggers 'media outlets', thereby requiring all web-based writers with posts that exceed more than 3,000 page views to register with the government (Soldatov, 2017; Duffy, 2015). In June of 2014, the Russian government further restricted speech by passing a law which limits the ability of Internet users to disseminate content deemed 'threatening' or 'extremist', as well as allowing the government to imprison any individual 'caught' breaking the law for up to 5 years (Duffy, 2015). In July of 2014, the Russian government passed a law mandating the local storage and retention of Russian user data not only by national companies but also international companies, such as Facebook, Google, Twitter, etc. (Duffy, 2015). This law mandated that International companies

move servers dealing with Russian Internet traffic to Russia, as well as store the data on the servers for a minimum of 6 months. Later in July 2014, a law was passed stating that access to anonymous wi-fi in public areas was prohibited (Duffy, 2015). Additionally, Russian wi-fi users were forced to register with their phone numbers in order to obtain wi-fi access, and, most shockingly – the law required individuals purchasing SIM cards for mobile phones in Russia to provide their passport information to purchase a SIM card (Duffy, 2015).

Interestingly, while the Russian government has ruthlessly passed and enacted sweeping Internet Censorship laws, the ISPs within Russia have been incredibly forthcoming and helpful in creating a system of Internet censorship for the Russian government (Soldatov, 2017). Driven primarily by fear of being targeted by the newly passed laws, the privately-owned ISPs came to the Russian government and willingly helped them implement censorship technologies (Soldatov, 2017). Astonishingly, the Russian government's tactics worked so well that the companies themselves bore the costs of deploying censorship technologies on their networks and others (Soldatov, 2017). Nowhere is this more apparent as it is in the implementation of Deep-Packet-Inspection (DPI) technologies by ISPs within Russia. Typically, filtering technologies can only look at the information in the IP header, the source origin and the destination (Soldatov, 2017). DPI, on the other hand, allows individuals to look inside at the actual content of the IP packets, greatly expanding the granularity used in filtering techniques (Soldatov, 2017). The ICTs, while not as incredibly sophisticated and systematic as the Chinese or Iranian governments, are nonetheless continually being adopted throughout Russia (Soldatov, 2017). They are daily becoming more sophisticated and pervasive. Because of the speed and ruthlessness with which the Russian government is censoring the Internet, ISPs live in constant

fear of what the regime may do next, and as such, are constantly evaluating themselves to make sure they are in check with the regime (Soldatov, 2017).

Circumvention Technologies

The Onion Router (TOR)

Censorship technologies are daily becoming more sophisticated and more pervasive. Totalitarian governments are becoming much more blatant in their censorship of the Internet, but not without user backlash. A plethora of circumvention technologies (CTs) have been created that enable users to effectively limit or completely nullify ICTs. One of the most popular CTs is alternate browsers, and specifically among them, the Onion Router (TOR) is one of the most pervasive and widespread (Winter & Crandall, 2012). At its core, TOR is a privacy-enhancing system that anonymizes users as they use the Internet (McCoy, Bauer, Grunwald, Kohno, & Sicker, 2008). TOR is popular not only for the anonymity it provides but also because it provides such anonymity while maintaining low latency (McCoy, 2008). TOR functions by providing what is known as an ‘anonymity layer’ for TCP by using a three-hop system (McCoy, 2008). When using the TOR browser, user traffic is encrypted in a layered manner, and then sent through nodes across the country (McCoy, 2008). The three-hop system functions in the following manner: data is encrypted, sent to the first node, who peels back one layer of encryption and sends it to the middle node. The first node knows the origin of the data, but not the destination. The middle node peels back another layer of encryption and sends it to the last node. The last node then peels back the final layer of encryption and sends the data to the desired location (McCoy, 2008). The last node knows the destination server and can also examine the contents of the data but does not know the source of the data (McCoy, 2008). It should be noted that the last node does raise a security concern because once the data leaves the exit node it is no

longer encrypted. Even in light of this, it remains difficult to track data sent through the TOR network.

TOR runs off a network of volunteered computers all over the world (Jardine, 2017). While some may believe it is a security risk because of the volunteer nature of computer nodes, and there are arguments to be made in favor of such a belief, because of the encryption TOR provides, and the fact that no one router knows the source and destination, the anonymity provided is legitimate. Primarily, TOR is used by individuals with the need to remain hidden, or in oppressive regimes, such as China (Jardine, 2017). Studies show that oppressive governments drive the usage of TOR above all else, with use dropping rather sharply outside of oppressive regimes (Jardine, 2017). In light of its use, the government of China has tried to completely block its use many times (Winter & Crandall, 2012). While there are ways around the blocking mechanisms, such as adding layers of obfuscation between the transport and application layer protocols (Winter & Crandall, 2012), but such techniques are generally beyond the scope of a normal user.

Virtual Private Networks (VPNs)

In today's age, the use of Virtual Private Networks is not only limited to individuals attempting to bypass ICTs, but also by the everyday consumer. They are one of the most widespread circumvention technologies on the market, primarily due to the fact that they are relatively easy to use, and they (generally) provide a robust level of anonymity when using the Internet. At its core, a VPN allows a user to extend a private network across a public network (Jyothi & Reddy, 2018). Basically, a user can gain access to a network they otherwise would not be able to access, either because of proximity or for security reasons, through VPNs. Because the connection is private, the user's data is also secured as it traverses atop the public network.

Fundamentally, when an individual is using a VPN, it is like a private tunnel that their data is being sent through, and the private tunnel exists on the main network, but no one can access it (Jyothi & Reddy, 2018). To keep data secure, data packets are encapsulated within one another Jyothi & Reddy, 2018). Each packet has two layers of headers when used with a VPN: the outer layer, which is the encapsulating layer, has the information that pertains to the VPN, including the source and the destination. The inner layer has the original source and destination but is completely encrypted at the lowest level; that being the link level (Jyothi & Reddy, 2018). When the data is transferred across the Internet, even if an attacker managed to penetrate the connection, because of the multiple layers, their ability to read the original data would be greatly hindered, if not completely nullified. Once data arrives at the desired destination, the VPN client and server exchange information, the data is decrypted, and then sent to the appropriate recipient (Jyothi & Reddy, 2018). Certain VPN configurations, specifically commercial VPNs also route data through multiple different servers, so anyone monitoring cannot determine the true source of the data.

There are many different types of VPNs, each with their own strengths and weaknesses. For example, take the remote access VPN: in this configuration, the remote client, or the user's device connects from an off-site location via a dedicated VPN server which is connected to the network (Jyothi & Reddy, 2018). Or, in the case of site-to-site VPN, the VPN connects portions of a private network together without the need to run client software on each machine (Jyothi & Reddy, 2018). Contrasting against the first two, peer-to-peer VPNs (P2P) only allow access to the VPN from mutually trusted peers, which is generally achieved via a central server that authenticates users (Jyothi & Reddy, 2018). Or, instead of a centralized authenticating service, users can exchange passwords and cryptographic keys to authenticate (Jyothi & Reddy, 2018).

One of the most complex VPN configurations is the Multi-Protocol Label Switching (MPLS) VPN, which uses is a flexible method for transporting and routing different types of network traffic (Jyothi & Reddy, 2018). MPLS VPNs use the BGP and MPLS to provide routes and transports over a public network using multiple different pieces of hardware (Jyothi & Reddy, 2018).

In light of global government restrictions on user privacy over the Internet, VPNs are fast becoming widely adopted (Farnan Darer, & Wright, 2019). The general consumer is inundated with ads about user privacy and the necessity of VPNs to protect one's data near-daily (Khan et al., 2018). but they are primarily of interest to individuals with oppressive governments. They are a common method of circumvention, especially in countries such as China, Iran, and other countries with particularly oppressive governments. But as their popularity rises, so too does their regulation (Chen & Yang, 2018). For example, China recently passed a law that outlaws unauthorized use of VPNs and required that any connection to any server hosted outside of China must be registered with the telecommunications authorities in China (Chen & Yang, 2018), effectively making access to VNPs and proxy servers illegal.

Proxy Servers

In some ways much similar to VPNs, proxy servers allow users to communicate over censored networks by using three-way communication, or a man-in-the-middle, to pass information between the user and a banned resource or location (Al-Saqaf, 2016). Originally used by ISPs and other businesses as caching systems to decrease server loads, proxy servers were soon noticed for their ability to circumvent filtering technologies (Abiona et al., 2014). Proxy servers can be thought of as intermediary agents between the user and the resource they are trying to access (Al-Saqaf, 2016). In situations where proxy servers are used to circumvent

ICTs, the client and the server are not allowed to interact because the connection is blocked by an ICT. But proxy servers are not directly associated with the client, and therefore, barring any specific rules the proxy server has, it can interact with the destination server on behalf of the client, and then send the information back (Al-Saqaf, 2016). For example, if a user in China wants to access Facebook, which isn't possible in China, the client can bounce their request off a proxy server in or outside of China, the proxy server can go communicate with the web server, and then send data back to the user because the proxy server and the client are allowed to communicate (Al-Saqaf, 2016). Further use-cases are numerous. For example, a common use-case of proxy servers is to create a local proxy server for applications hosted within a restrictive area, send traffic to the proxy server, who then sends the information to a server outside the restricted area, who then sends it back to the user. (Callanan, Dries-Ziekenheiner, Escudero-Pascua, & Guerra, 2011). The benefit of such an approach is that the user can create their own proxy server, not needing to rely on others to maintain access. Likewise, if a user desires to use proxy servers already in place, it is not an issue because of the sheer amount available all over the world (Al-Saqaf, 2016).

While proxy servers are abundant and relatively simple to access and use, they are not without their faults (Callanan et al., 2011). Technically, a government could block proxy servers within a specific area, but such an action would come at the expense of crippling large swaths of the Internet within the area (Al-Saqaf, 2016). Additionally, if the application used is not "proxy-aware", users will be unable to access proxy servers because the application does not recognize proxy servers, or possibly the protocols running on them (Callanan et al., 2011). Also, data being sent to and from proxy servers is not naturally encrypted, meaning that if data were to be intercepted, it would be relatively easy to trace the source origin. But even when considering

such technical difficulties, proxy servers are nevertheless robust CTs. To keep traffic even more secure, the client accessing the proxy server can encrypt traffic to and from the proxy via specific proxy protocols, making interception of data between endpoints more difficult. Proxy server mediums are abundant, and users can choose to directly set up a connection to a proxy server via their home operating system, or they can use software such as Freegate, WinGate, Ultrasurf, or even their web browser to create a connection (Callanan et al., 2011).

Effects of Internet Censorship

The effects Internet censorship has on a populace are multi-faceted and incredibly varied. Different cultures respond differently, and subsets of groups within the varying cultures have massively different responses towards Internet censorship. One of the recurrent findings throughout a number of studies indicates that individuals within censored countries are so methodically inundated with the idea of Internet censorship that they are either indifferent, or they actually support Internet censorship (Duffy, 2015; Chen & Yang, 2018; Wang & Mark, 2015). For example, in Russia, studies found that the Russian public expected the state to take primary responsibility for policing content on the Internet and in other media institutions, and as such, there is largely support for state censorship of media (Zhong et al., 2017). For Russian citizens, the primary rationale for state censorship seems to stem from an inherent fear of new things and the idea that government is their primary protector. (Zhong et al., 2017). The findings of such studies, if extrapolated out, indicate that censorship polices, and the mass transmission of state-sponsored narratives, have worked overwhelmingly well.

A study conducted in 2012 showed that out of 56 million messages sent through the popular social media app, Weibo, 16% (roughly 9 million messages) were removed and never reached their destination due to ‘politically sensitive’ material (Zhong, Wang, & Huang, 2017).

Even more concerning, studies indicate that Internet censorship effects not only what individuals say online, but offline as well (Zhong et al., 2017). Media institutions, specifically in China, are extremely adamant about such self-censorship, primarily for the purpose of avoiding punishment and possibly currying favor with governmental leaders (Zhong et al., 2017). Indeed, much of the population seems to take such an approach – self-censoring not out of an innate desire, but rather out of a desire to keep themselves free from harm (Zhong et al., 2017). While some of the population seems to realize they have limited access to the Internet, studies show that large swathes actually believe they have full access to all the Internet has to offer (Zhong et al., 2017). Additionally, due to the fact that censorship at all levels is pervasive, China has a high rate of collectivism, which in turn seems to diminish individual netizen's desire to access the full Internet (Zhong et al., 2017). The lack of desire seems to stem from the fact that netizens believe everyone else lives within the censorship, so they should as well (Zhong et al., 2017). While apathy and nationalism are most definitely factors in the acceptance of Internet censorship, although studies indicate that the base rationale seems to be fear of personal repercussion from power figures (Zhong et al., 2017).

Although inundated cultures often seem apathetic to Internet censorship, studies have been conducted which have examined the effects of user's gaining unhindered access to the Internet in China, and their findings are rather promising. The findings indicate that when given the opportunity to use the uncensored web, far from complacent, users became much more aware of problems with the Chinese government, visit foreign media outlets more, (increases of 435%), become more aware of current events, discuss political events more, and fundamentally shift their attitudes, behaviors, and beliefs (Chen & Yang, 2018).

The research highlighted throughout clearly shows the effects of Internet censorship on

freedom of speech and political expression. China, Russia, and other authoritarian regimes perfectly highlight the damaging effects of Internet Censorship. Internet censorship effects populaces at a fundamental level by taking away their ability to individually express themselves, particularly in opposition to the government. It enables authoritarian regimes to monitor, suppress, and limit political dissent. It allows governments to stalk entire populaces, with or without cause, no legal due-process, or checks and balances. It enables governments to throw their citizens in jail or curtail their speech simply because the rhetoric is deemed harmful. Internet censorship has and continues to concentrate power among specific groups at the expense of the populace. Such power, when continually concentrated, can only lead to violations of human's fundamental rights and continual degradation of personal and societal liberties. Internet censorship, even when enacted under the auspices of good intentions, drastically harms populaces and empowers authoritarian regimes to strip fundamental rights from their citizens.

Conclusion

Internet censorship is pervasive, highly sophisticated, and ever-expanding daily. From social media monitoring to blocking access to educational sites, the list of restrictions grows daily. From the perspective of authoritarian regimes such as China, Iran, and Russia, it is perfectly understandable why limiting their populace's ability to access an open Internet is of such importance. If they were to allow such access, change would occur, the power of the individuals who implemented such ICTs as BGP Hijacking, DNS Poisoning, TCP RST attacks, bandwidth throttling, DPI, and others, would be challenged. They would no longer be able to monitor and inspect every action of their citizens. The ICTs employed rely on a multitude of complex systems and procedures – none being more important than centralized control of backbone ISPs, which then extends down the hierarchy of ISPs. Thankfully, circumvention

technologies such as TOR, VPNs, Proxy Servers, and others are available to route around the ICTs used. The effects of Internet censorship are wide-ranging and incredibly harmful. But more than anything, Internet censorship is dangerous because destroys democracy and strips individuals of their freedoms. Freedom of expression, freedom of choice, freedom to not be monitored – all are hallmarks of freedom which Internet censorship destroys, both covertly and explicitly. The Internet has become one of the most democratizing forces to have ever existed. But when authoritarian governments to access and freely use it, tyranny ensues.

References

Abiona1, O., Oluwaranti, A., Oluwatope, A., Bello, S., Onime, C., Sanni, M., & Ke-hinde, L. (2014). Proxy Server Experiment and Network Security with Changing Nature of the Web. *International Journal of Communications, Network and System Sciences, 7*(12), 519-528.

Aceto, G., & Pescape, A. (2015). Internet censorship detection: A survey. *Computer Networks, 83*, 381-421.

Al-Saqaf, W. (2016). Internet censorship circumvention tools: Escaping the control of the Syrian regime. Media and Communication, *4*(1), 39-50.

Anderson, C. (2013). Dimming the internet: Detecting throttling as a mechanism of censorship in Iran. *Arxiv pre-print, 3-31*.

Anderson, D. (2012). Splinternet behind the great firewall of China. *ACM Queue, 10*(11), 40-49.

Anonymous. (2012). The collateral damage of internet censorship by DNS injection. *ACM SIGCOMM Communication Review, 42*(3), 21-27.

Aryan, S., Aryan, H., & Halderman, J. A. (2013). Internet censorship in Iran: A first look. *Usenix: The Advanced Computing Association,* 1-8.

Balakrishnan, H. (2009). How YouTube was hijacked. *Massachusetts of Technology, Department of Electrical Engineering and Computer Science*.

Bora, G., Bora, S., Sing, S., & Arsalan, S. M. (2014). OSI reference model: An overview. *International Journal of Computer Trends and Technology, 7*(4), 214-218.

Bradbury, D. (2011). Routing around censorship. *Network Security, 2011*(5), 5-8.

Callanan, C., Dries-Ziekenheiner, H., Escudero-Pascual, A., & Guerra, R. (2011). Leaping over the firewall: A review of censorship circumvention tools. *Freedom House Report*.

Chen, Y., & Yang, D. Y. (2018). The impact of Media censorship: Evidence from a field experiment in China. *Stanford Department of Economics*.

Chiesa, M., Di Battista, G., Erlebach, T., & Patrignani, M. (2015). Computational complexity of traffic hijacking under BGP and S-BGP. *Theoretical Computer Science, 600,* 143-154.

China Internet Network Information Center. (2017). Statistical report on internet development in China: 2017. *CNNIC*.

China Internet Network Information Center. (2019). Statistical report on internet development in China: 2019. *CNNIC*.

Clayton, R., Murdoch, S. J., & Watson, R. N. M. (2006). Ignoring the great firewall of China. *International Workshop on Privacy Enhancing Technologies,* 20-35.

Demchak, C., & Shavitt, Y. (2018). China's maxim – Leave no access point unexploited: The hidden story of China Telecom's BGP hijacking. *The Journal of the Military Cyber Professionals Association, 3*(1), 1-9.

Duffy, N. (2015). Internet freedom in Vladimir Putin's Russia: the noose tightens. American Enterprise Institute.

Farnan, O., Darer, A., & Wright, J. (2016). Poisoning the Well: Exploring the great firewall's poisoned DNS responses. Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, 95-98.

Farnan, O., Darer. A., & Wright, J. (2019). Analysing censorship circumvention with VPNs via DNS cache spoofing. *IEEE Security and Privacy Workshop,* 205-211.

Feng, G. C., & Guo, S. Z. (2013). Tracing the route of China's internet censorship: An empirical study. *Telematics and Informatics, 30*(4), 335-345.

Hall, J. & Zhou, Y. (2017). The sinuous dragon: Economic freedom and economic growth in China. *Department of Economics, West Virginia University*.

Hu, J., & Zheng, Y. (2019). Social media, state control and religious freedom in China. *Political Theology, 20*(5), 382-391.

Jardine, E. (2018). Privacy, censorship, data breaches and internet freedom: The drivers of support and opposition to dark web technologies. News Media and Society, 20(8), 2824-2443.

Jiang, M. (2014). The business and politics of search engines: A comparative study of baidu and Google's search results of internet events in China. *New Media & Society, 16*(2), 212-233.

Jyothi, K. K., & Reddy, I. B. (2018). Study on virtual private network (VPN), VPN's protocols and security. *International Journal of Scientific Research in Computer Science, Engineering, and Information Technology, 3*(5), 919-932.

Kent, S., Lynn, C., & Seo, K. (2000). Secure border gateway protocol (S-BGP). *IEEE Journal on Selected Areas in Communications, 18*(4), 582-592.

Khan, M. T., DeBlasio, J., Voelker, G. M., Snoeren, A. C., Kanich, C., & Vallinia-Rogriguez, N. (2018). An empirical analysis of the commercial VPN ecosystem. *IMC Proceedings of the Internet Measurement Conference*, 443-456.

Lowe, G., Winters, P., & Marcus, M. L. (2007). The great DNS wall of China. *New York University*.

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008). Shining light in dark places: Understanding the TOR network. *Lecture Notes in Computer Science*, 63-76.

Naughton, J. (2016). The evolution of the internet: From military experiment to general purpose technology. *Journal of Cyber Policy, 1*(1), 5-35.

Rahimi, B. (2015). Censorship and the Islamic republic: Two modes of regulatory measures for media in Iran. *Middle East Journal, 69*(3), 358-378.

Ramadan, Z. (2018). The gamification of trust: the case of China's "social credit". Marketing Intelligence & Planning, 36(1). 93-107.

Ruan, L., Knockel, J., Ng, J. Q., & Crete-Nishihata M. (2016). One app, two systems: How WeChat uses one censorship policy in China and another internationally. *University of Toronto, Citizen Lab Research Report, 84*. 1-32.

Shinder, D., & Cross, M. (2008). *Scene of the Cybercrime, 2nd Edition*.

Soldatov, A. (2017). The taming of the Internet. *Russian Social Science Review, 58*(1), 39-59.

Wan, T., Oorschot, P. C., & Kranakis, E. (2005). A selective introduction to border gateway protocol (BGP) security issues. *Carleton University School of Computer Science*.

Warf, B. (2011). Geographies of global internet censorship. *Geojournal, 76*(1), 1-23.

Winter, P., & Crandall, J. R. (2012). The great firewall of China: How it blocks TOR and why it is hard to pinpoint. *Usenix – The Advanced Computing Systems Association*, *37*(6), 42-50.

Zhong, Z., Wang, T., & Huang, M. (2017). Does the great fire wall cause self-censorship? The effects of perceived internet regulation and the justification of regulation. *Internet Research*, *27*(4), 974-990.