INTERNET CENSORSHIP

Honor Pledge: I acknowledge that the Capstone Project is an independent study project to be completed individually. On my honor, I have not received aid on my Capstone Project other than what was provided by my faculty mentor and any persons explicitly cited in my work. I further acknowledge that if I have given any aid to another student in this course, the instructor of this course was made aware of my contributions.

Table of Contents

Project Objective

At one point in time, there was no Internet; no way for computers to communicate to with each other. The idea of computers communicating with one another was invented in 1962, when scientists and military experts were concerned about what would happen if the nation's telephone system was destroyed from an attack made by the Soviet Union. They believed that one missile could destroy the network of wires that made it possible to communicate from long distances. A scientist named J.C.R. Licklider from M.I.T. and APRA proposed the idea of a "galactic network" of computers that could communicate with each other as a solution to the issue and allow government officials and leaders to communicate even if the Soviets destroyed the telephone system. About three years later in 1965, another scientist from M.I.T. developed a way that computers could send information to one another - he called this technology "packet switching". Packet switching is when the data is broken down into small chunks before sending it to its destination. This prevented the government computer network from being as vulnerable as the telephone system. In the early 1970's the APRAnet network began to grow by adding computers from different universities around the world, but it was hard for them to integrate into one worldwide network. By the end of the 1970's a computer scientist named Vinton Cerf began to solve this problem by inventing the Transmission Control Protocol (TCP), which allowed all of the computers on the world's network to communicate with each other. In 1991, a computer programmer named Tim Berners-Lee introduced the World Wide Web, which was more than just a way to send files from one computer to another - it was information that anyone could access and retrieve. From there, the Internet became what we know it as today. With the growing amount of information that can be viewed, accessed, and published on the Internet, it is

becoming more dangerous. A novice in this area should be aware of the number of cyber-crimes committed around the world and the amount of information that these criminals have access.

Internet censorship is the control of what may be accessed, viewed, or published on the internet. This censorship can be regulated by the government or a private company on behalf of the government. My original belief was that with more control over what can be published and accessed on the internet, it would help control the amount of cyber-crimes that are committed. However, after discussing my ideas with my faculty mentor, Dr. Michelle Liu, I realized that my thesis did not cover the whole concept of internet censorship. After more careful research, I've learned that different countries have different laws regulating the internet. I believe that the governments in these countries, such as China and Iran loosen their reign on what users can access on the internet.

Client

In this paper, I plan to discuss the different laws and policies that China and Iran regulating the Internet and what citizens can and cannot access on it. I believe that the Internet should be less censored in the countries where content is heavily filtered because it negatively impacts the citizens of the country and possibly users from outside of those countries.

Faculty Advisor

My faculty advisor is Dr. Michelle Liu. She received her Bachelor of Engineering degree in International Trade of Textiles from Nankai University in China; she earned her master's degree in Management from Tianjin Polytechnic University, and her doctoral degree in Information Systems from Boston University. She joined Marymount University in 2008 as an

assistant professor. Her research interests broadly center on the areas of design, enterprise architecture, and the uses and impacts of emerging technologies on social activities and behaviors.

Project Plan

I plan to research how different countries censor the internet and the effects it has on its users. I will accomplish this by consulting with different resources including speaking with people from countries with heavily censored internet access and gaining information from several different academic journals. My planned schedule is as follows:

Week of Sept. 21 – Complete and turn in Peer Review 1

Week of Sept. 28 – Find three sources and complete the first three sections of draft

Week of Oct. 5 - Find three sources and complete three more sections of my draft

Week of Oct. 12 - Find two sources and complete two more sections of my draft

Week of Oct. 19 - Find two sources and complete the final two sections of my draft; turn in draft on October 22

Week of Oct. 26 – Complete Peer Review 2

Week of Nov. 2 – Begin editing draft (pgs. 1-3)

Week of Nov. 9 – Break

Week of Nov. 16 – Continuing editing draft (Pg.4-6)

Week of Nov. 23 – Break

Week of Nov. 30 – Finish editing and turn in final (Pg.7-10)

Week of Dec. 7 – Prepare for presentation and project retrospective

Resources

I do not plan on using any special resources. I plan on conducting research using the internet, the library, and information given by word of mouth.

Project Details

Different countries have different rules, attitudes, and laws regulating internet censorship. Although internet censorship may be beneficial to the governments of the countries that practice it, it prevents internet uses from having freedom of speech and the ability to gain knowledge from outside of their country. There are three countries in particular that have very strict policies regarding the internet and what may be accessed: China and Iran.

Internet Censorship in China

China has over 500 million Internet users, however, they are very limited in what they can access: more than 18,000 websites are blocked in Mainland China (Yang & Liu, 2014). China's system of limiting access to foreign sites is often called the Great Firewall. The Great Firewall is "reinforced by a thicket of laws, policies, and regulations" (Deibert, 2013). There are four dimensions of internet censorship in China: network filtering, chat censorship, search filtering, and blog censorship (Yang & Liu, 2014). Network filtering is based on Internet Protocols (IPs) and Domain Name Servers (DNS) and routers automatically inspect all traffic moving in and out of Mainland China. This type of filtering prevents users in Mainland China from connecting to certain websites (Yang & Liu, 2014). Search filtering censors what users can

search for on the Internet. China's filters are so sophisticated that they can selectively block specific pages within websites, instead of making the whole website inaccessible. Users who search for blocked terms are blocked from the Internet for about 90 seconds before they can continue usage (How does China censor the internet?, 2013). In addition to that, when a user searches for a forbidden term or topic, the Great Firewall "sends a reset packet" which disables the connection and sends back a "standard error message" that manages to give the user the impression that the forbidden content that they requested does not exist or that the file was not file was not found: it does not outright say that the content is blocked (Deibert, 2013). Chat censorship is how the government censors the chat conversations that users have: this prevents users from chatting about certain topics. Blog censorship filters what can be posted online by bloggers. Certain topics are forbidden and people who attempt to post topics in blogs or comments in forums relating to terms such as democracy or foreign issues will be prevented from posting.

The censorship causes interruptions with the Internet and connections to certain websites. These interruptions are unpredictable. For example, if a user is using a news website and it is working one minute, it may be unavailable the next minute if the site publishes an article or blog posting about a topic that is banned by China. This can be very frustrating to users who are interested in foreign news or current topics. This also hinders the citizens from learning.

Despite the oppressive hardships caused by the strict Internet censorship, users in Mainland China find ways to get around the blocked sites. Many users resort to many different applications and software to bypass the censors. In fact, in hotels where foreigners may visit, Internet service providers alter the service and tweak the routers in order to provide the

foreigners with open access to the Internet. This gives the foreigners a different idea of the Internet accessibility that is available to the citizens of Mainland China.

China's tight control over what can and cannot be accessed on the Internet causes frustration to the over 500 million users in the country and limits their education to what the Chinese governments wants them to know. While this may strengthen the Chinese government and economy, it is detrimental to the users inside and outside of Mainland China who cannot easily and legally (in some cases) communicate with the outside world.

Internet Censorship in Iran

Even more restrictive than China in regards to censorship of the Internet is Iran. Iran is said to be one of the least free countries in terms of internet freedom. Iran's censorship of the Internet is more documented than China. The country has a triangulated approach to Internet censorship. Their strategies to control the Internet involve interceptive, preventative, and reactive methods (Bowen & Marchant). They have created a cyber police unit and several other units that help enforce the country's internet censorship laws. In 2012, Iran's government created the Supreme Council of Cyberspace that is responsible for managing the country's cyber policies. This Council controls three other bodies that are associated with the Iran's Internet censorship. These bodies consist of the Committee for Determining Offensive Contents, the Iran Cyber Police which is also known as the FATA Police, and the Revolutionary Guard Cyber Defense Command, which is also known as the Iran Cyber Army. The Committee for Determining Offensive Contents controls censorship policies in Iran. It is also responsible for maintaining and updating lists of censored websites and also for enforcing Internet communication policies (Aryan, Aryan, & Halderman, 2013). The Iran Cyber Police monitors the country's online activities and prosecutes nonconformists or users that are involved in illegal

activities on the Internet that are described by the Committee for Determining Offensive Contents (Aryan, Aryan, & Halderman, 2013). The Revolutionary Guard Cyber Defense is responsible for defending Iran against cyber-attacks and executing countermeasures (Aryan, Aryan, & Halderman, 2013). It is said that although each of these governing is supposed to have a purpose, they each hold poorly defined powers and responsibility, which results in many conflicts over policies regarding Internet control. Although we have information about the structure in which the Iranians prosecute violators of Internet censorship, it is harder to gain information about how they actually censor the Internet.

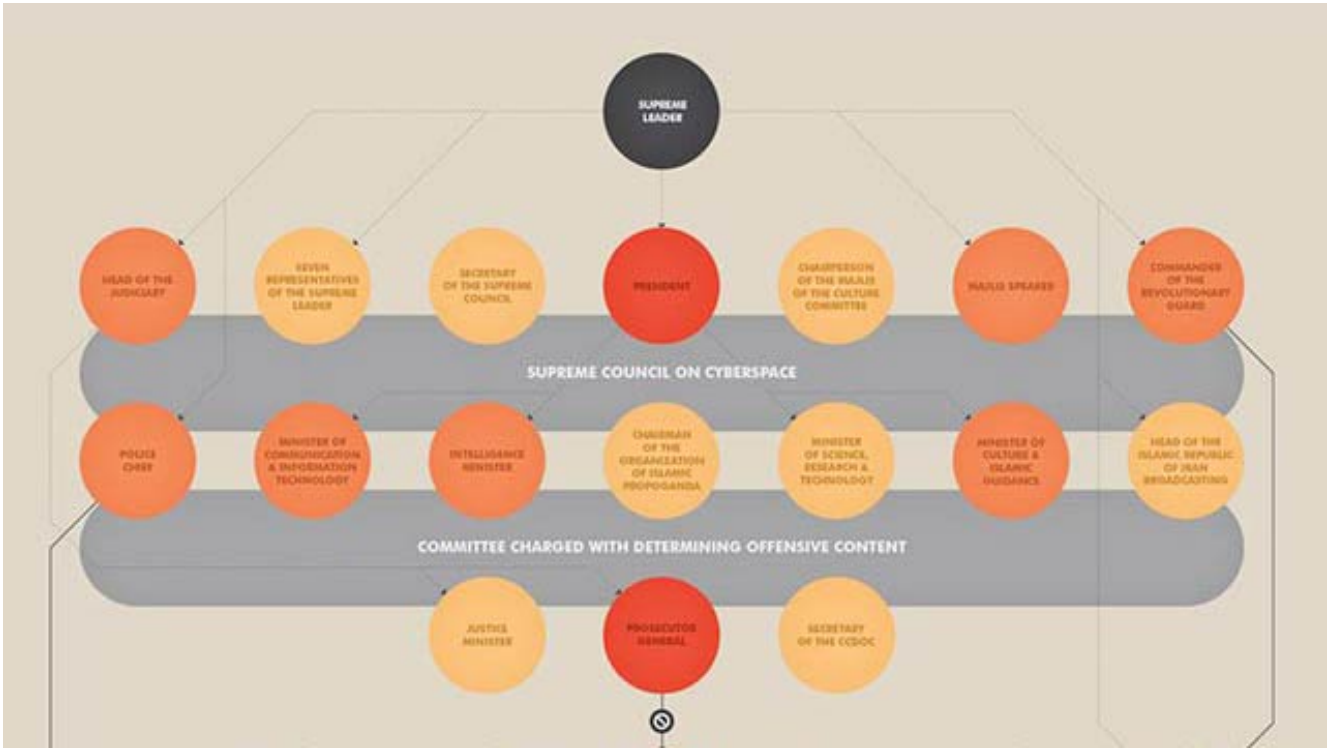

Figure 1 illustrates the bodies involved in Internet censorship in Iran (http://iranmediaresearch.org/sites/default/files/research/pdf/1363180689/1385/internet_censorship_in_iran.pdf)

Very little research about Iran's technology and network topology used to censor the Internet because penetrating their network from the inside of the country is very dangerous due all of the government bodies dedicated to enforcing the Internet censorship policies and the risks

to the Iranian citizens who help (Aryan, Aryan, & Halderman, 2013). However, Simurgh Aryan, Homa Aryan, and J. Alex Halderman were able to conduct a small study in order to better understand how the Iranians filter the Internet. They did this by "[analyzing] traffic to blocked and non-blocked hosts at the packet level, and [they] used traceroutes to study hops inside the country's infrastructure" (Aryan, Aryan, & Halderman, 2013). They assessed the degree of censorship in Iran by surveying the "most-visited websites based on Alexa web traffic rankings" (Aryan, Aryan, & Halderman, 2013). Predictably, the most censored category of websites is Adult; only 23 out of 473 websites were considered OK (Aryan, Aryan, & Halderman, 2013). The study determined that over 500 of the world's most popular websites were blocked. When users search for a banned topic, term, or website, they are redirected to a page that looks like this:

Figure 2 shows the page that users get when they attempt to access a blocked website from Aryan, Aryan, & Halderman, 2013

This page is located at http://10.10.34.34. It explains to the user that access to the website to the requested website is no possible. It also gives them a link to click to make complaints. After 30 seconds, the user is then forwarded to a second censorship website located at peyvandha.ir.

The Iranian government also has ways of discouraging its users from certain online activities. Their restrictions on bandwidth take the uploading of photos and videos very slow (Calingaert, 2010). Because it takes so long to complete these activities, it makes the users not want to go through the trouble of doing it.

Up to this point, I have researched Internet censorship in China and Iran extensively and attempted to find ways that I might conduct a study myself, although I have found this to be quite difficult. I still need to conduct interviews with one or two people from each of the countries to gain a better understanding of the effect of censorship from a personal perspective. I would also like to research Internet censorship in the United States, which I believe to have relatively relaxed Internet censorship policies.

Knowledge Being Applied

I will be applying my knowledge of computer networking to help me better understand how countries are able to filter content and block access to and from websites. This understanding comes from my knowledge of network topology.

Risk Factors

My project will be negatively impacted by the fact that I am not able to actually build upon or experiment for myself the degree to which other countries are censoring the Internet. This severely limits my research to other resources, such as previous studies completed by professionals.

Work Provided by Others

I will be using the studies conducted by professionals to gain a better understanding of Internet censorship in other countries. Because of the risks and difficulty involved with conducting my own studies on this matter, I will use previous studies and attempt to find people who are from these countries (China and Iran) and interview them to gain a better understanding on how the censorship personally affects them and the majority of users in their country.

References

Aryan, S., Aryan, H., & Halderman, J. (2013, August). Internet Censorship in Iran: A First Look. *Proceedings of the 3rd USENIX Workshop on Free and Open Communication on the Internet*. Retrieved October 16, 2015

Bowen, K., & Marchant, J. (n.d.). Internet Censorship in Iran: Preventative, Interceptive, and Reactive. *Revolution Decoded*. Small Media. Retrieved October 15, 2015, from http://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded_Ch2_InternetCensorship.pdf

Calingaert, D. (2010). Authoritarianism vs. the Internet. *Policy Review*, 63-75. Retrieved October 15, 2015, from http://search.proquest.com/docview/216443761?accountid=27975

Deibert, R. (2013, June). Trouble at the border: China's internet. *Index on Censorship, 42(2)*, 132-135. doi:10.1177/0306422013495334

How does China censor the internet? (2013, April 21). *The Economist*. The Economist. Retrieved October 10, 2015, from http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-china-censors-internet

Yang, Q., & Liu, Y. (2014, August). What's on the other side of the great firewall? Chinese web users' motivations for bypassing the Internet Censorship. *Computers in Human Behavior, 37*, 249-257. Elsevier Ltd. Retrieved October 15, 2015