BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF INFORMATION SYSTEMS
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

CENSORSHIP ON THE INTERNET

CENZURA NA INTERNETU

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR **JÁCHYM POSTOLKA**
AUTOR PRÁCE

SUPERVISOR **Mgr. PAVEL OČENÁŠEK, Ph.D.**
VEDOUCÍ PRÁCE

BRNO 2024

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Bachelor's Thesis Assignment

156776

Institut:	Department of Information Systems (DIFS)
Student:	**Postolka Jáchym**
Programme:	Information Technology
Title:	**Censorship on the Internet**
Category:	Web applications
Academic year:	2023/24

Assignment:

1. Study the current issue of censorship on the Internet in selected countries. After consultation with the supervisor, select one country and solve the following points for it.
2. Conduct a thorough study of the censorship tools currently in use. Study existing resources and projects for detection and analysis of censorship.
3. Based on the results of the analysis, propose an application for practical verification, or mapping of specific censorship means in the given area.
4. Implement and verify the designed application in practical conditions.
5. Discuss the results obtained.
6. In cooperation with the supervisor, summarize the results in a final report that will be published in foreign professional sources.

Literature:

- Kurose, J. F. Computer networking: A top-down approach. Pearson, Essex, 2017, ISBN 978-1-292-15359-9.
- Stallings, W. Network security essentials: Applications and standards. Hoboken, 2016, ISBN 978-0-13-452733-8.
- Bishop, M. Computer security: Art & Science. Addison-Wesley, Boston, 2003, ISBN 0-201-44099-7.

Detailed formal requirements can be found at https://www.fit.vut.cz/study/theses/

Supervisor:	**Očenášek Pavel, Mgr. Ing., Ph.D.**
Head of Department:	Kolář Dušan, doc. Dr. Ing.
Beginning of work:	1.11.2023
Submission deadline:	9.5.2024
Approval date:	30.10.2023

Abstract

Internet censorship is a very relevant topic in modern society. Increasingly, the internet is being used to control access to information and to monitor its users. The goal of this thesis is to document the methods of censorship in the United Arab Emirates and the reasons why the internet is censored in this country. Additionally, it aims to explore the impacts of this censorship in terms of user access to the internet, how internet censorship restricts access to free information, and how it is used as a tool of repression.

Part of this thesis involves designing and implementing a tool to detect the presence of censorship and how the internet is censored. This tool is composed of several tests, each focused on testing a different method of censorship. By modifying the inputs, this tool can be used to test censorship in countries other than the United Arab Emirates.

The tool was unable to detect any signs of censorship because it was run on a virtual private server, which due to its location within the network, bypassed the censorship measures of internet service providers, who are the primary means of censorship within this country. To test its functionality as a tool for detection and analysis of censorship in the United Arab Emirates, it would require user level access to the internet within the country.

Abstrakt

Cenzura internetu je velmi relevantní téma moderní společnosti. Stále více se internet využívá ke kontrole přístupu k informacím a sledováním jeho uživatelů. Cílem této práce je zdokumentovat způsoby cenzury ve Spojených Arabských Emirátech a za jakým účelem je internet v této zemi cenzurován. Dále je to také prozkoumání dopadů této cenzury na přístup uživatelů k internetu, jakým způsobem cenzura internetu omezuje přístup k svobodným informacím a jak je využívána jako nástroj represe.

Součástí této práce je návrh a implementace nástroje na zjištění přítomnosti cenzury a jakým způsobem je internet cenzurován. Tento nástroj je sestaven z několika testů, kde každý je zaměřen na otestování jiného způsobu cenzury. Tento nástoj lze úpravou vstupů využít pro testování cenzury i v jiných zemích, než jsou Spojené Arabské Emiráty.

Nástroj nebyl schopen zjistit známky cenzury, kvůli jeho spouštění na virtuálním privátním serveru, který svým umístěním v síti obchází cenzorské prostředky dodavatelů internetového připojení, které jsou hlavním způsobem cenzury této země. Pro otestování jeho funkčnosti jako nástroje detekce a analýzy cenzury ve Spojených Arabských Emirátech, by vyžadovalo lokální uživatelský přístup k internetu.

Keywords

Internet, censorship, firewall, Tor, United Arab Emirates, Saudi Arabia

Klíčová slova

Internet, cenzura, firewall, Tor, Spojené Arabské Emiráty, Saudská Arábie

Reference

POSTOLKA, Jáchym. *Censorship on the Internet.* Brno, 2024. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Mgr. Pavel Očenášek, Ph.D.

Rozšířený abstrakt

Internet, který díky jeho stále většího průniku do každodenního života, je velice mocný nástroj z pohledu dopadu na společnost. Jeho cenzurování a monitorování má tedy velké dopady a často bývá používáno k represi.

Hlavním cílem této práce je zanalyzovat situaci cenzury internetu ve Spojených Arabských Emirátech a vytvořit nástroj, kterým je možné tyto cenzurní praktiky ověřit. Nástroj by mělo být možné použít v libovolné zemi, závisí tedy pouze na vstupech a je možné ho spustit v libovolné síti.

Spojené Arabské Emiráty cenzurují internet v rozsáhlém měřítku. V zemi je efektivně duopol poskytovatelů internetového připojení, kde Spojené Arabské Emiráty vlastní obě tyto firmy alespoň z 50% a využívájí jejich kontrolu nad infrastrukturou ke kontrole a ovládání přístupu k internetu. Mají telekomunikační regulační autoritu, která určuje pravidla povoleného obsahu a spravuje seznam stránek které blokovat. Tato cenzura je prováděna na úrovni poskytovatelů internetového připojení. Přístup ke mnohým službám je blokován, jedním z příkladů jsou služby Voice over Internet Protocol (VoIP). Je povolen pouze krátký seznam těchto služeb, který byl v roce 2023 rozšířen o 17 položek včetně Microsoft Teams a Slack, ale většina těchto služeb zůstává omezena.

Saudská Arábie je další zemí v region, která má velmi podobná pravidla cenzury internetu a v mnohých směrech jsou parktiky těchto dvou zemí stejné. Jedná se například o cenzuru iránských stránek, kde Saudská Arábie má tvrdší pravidla než Spojené Arabské Emiráty a obě země cenzurují obsah týkající se skupin, které vnímají jako rizikové, jako Hezbollah nebo Muslimské Bratrstvo. Obě země během Katarské diplomatické krize v roce 2017 také rozšířili cenzuru katarských médií a jiných stránek kvůli diplomatickým vztahům Kataru s Íránem, který obě země vnímají jako hrozbu.

Druhou částí práce bylo vytvořit nástroj pro otestování cenzury internetu. Výsledný nástroj má následující funkcionalitu:

- Testování webových stránek a validaci výsledku
- Testování dostupnosti sítě Tor
- Testování dostupnosti služby Telegram
- Vyhledání výsledků pomocí Google a jejich uložení

Pro experimenty bylo třeba si sehnat lokální počítač ve Spojených Arabských Emirátech. Byl využit virtuální privátní server nacházející se v Dubaji. Díky způsobu cenzury v této zemi, a to na úrovni poskytovatelů internetového připojení, tento server již svým umístěním v síti obchází cenzorské metody. Nebylo možné pomocí navhnutého nástroje potvrdit výskyt cenzury v dané zemi. Dále byl pokus proveden na druhém VPS serveru se stejným výsledkem. Kontrola byla provedena i manuálně pokusy přístupu ke známým zakázaným stránkám. Test výskytu cenzury byl proveden i přes připojení k virtuální privátní síti, opět se stejným výsledkem.

Závěrem je, že využití virtuálního privátního serveru nebo virtuální privátní sítě vede k obcházení cenzorských prostředků. Přesto, že nebyly zjištěny mým testováním, cenzura internetu je využívána ve Spoejných Arabských Emirátech.

Censorship on the Internet

Declaration

I hereby declare that this Bachelor's thesis was prepared as an original work by the author under the supervision of Mr. Mgr. Pavel Očenášek Ph.D. I have listed all the literary sources, publications and other sources, which were used during the preparation of this thesis.

.....
Jáchym Postolka
May 16, 2024

Acknowledgements

I would like to thank my supervisor Mgr. Pavel Očenášek Ph.D. for his guidance and consultation, as well as the assignment of this thesis. I would like to thank my family for their support.

Contents

List of Figures

todonotes

Chapter 1

Introduction

Censorship has existed long before the harnessing of electricity, much less the creation of the digital computer. As such, it's unsurprising that censorship has extended it's influence to the internet as well. In the modern day, it is practiced by virtually every country in one way or another. However countries with a closer tie to authoritarianism tend to be more restrictive and have more measures in place to control what content can be accessed by their respective populations.

The technologies used for censorship are varied in the way they function, primarily based on what part of the internet they affect, which has a knock-on effect for their scalability. This is also an important factor when it comes to enforcing the rules in place as well as the methods used to bypass them.

This thesis will be focusing on the country of the United Arab Emirates (UAE). My reasoning for this decision is that it is one of the most developed countries in it's region and it's population is very well connected to the internet, while also having a significant amount of censorship. This is also true for it's neighbours such as Qatar and Saudi Arabia which share many other cultural similarities as well.

The UAE has previously spent a significant amount of money to promote it's image through traditional means, such as sponsoring sporting events including an F1 race or effectively owning the Premier League team Manchester City F.C. It has began expanding it's influence when it comes to the online world as well. Some examples of this are investments in e-sports, where it hosts numerous large Esports events. This shows, that the UAE is interested in spreading it's impact on the world, making it even more important to scrutinize the country and it's practices, to ensure a more complete image of their activities and morals.

Being a Muslim country, it bans much of the same content as it's neighbours. These include pornography, political content critical of the government, gambling and content related to the LGBT community. Along with the many allegations of human rights violations, limiting free access to the internet and the above stated expansions make it a good subject for this work. The goals of this thesis are to explore the measures that are used for censorship, their technical implementation and the creation of a tool to test their impact on free access to the internet.

The general topic of censorship is of great interest to me, as I find it interesting both due to it's historical context of how it affected many historical scenarios, as well as it's evolution into what we encounter today and the effects it has on our daily lives. I would even argue, that it is more relevant than ever, since in the age of easy access to information, the control of what and how information is shown has a massive impact on society.

Chapter 2 provides an introduction to the internet and a brief overview of it's aspects that will be followed upon in later chapters. Chapter 3 gives a more technical look at the layers of the internet based on the TCP/IP model. Chapter 4 will then discuss actual internet censorship and how it works. It will also give a more in-depth image of how this is done in Saudi Arabia and the UAE. It will also discuss methods used to circumvent these censorship methods. Chapters 5 will focus on the design and implementation of a tool to test the above-stated censorship methods. The evaluation of gathered data will be the content of chapter 6. Final evaluation of this work will be in chapter 7.

Chapter 2

Understanding the Internet and it's communication

The internet is without a doubt one of the most important and powerful pieces of technology in the modern day. The impact it has had on almost every person in the world cannot be denied, completely changing many aspects of our lives. Most relevant to this thesis is the way we gain information, be it from online news outlets, educative content, or even providing knowledge that used to be primarily by word of mouth, such as recommendations for books. While providing it's users with a lot of power, agency and breadth of knowledge they can access, it also creates a vulnerability. Due to how much the internet is utilized and relied on it is very lucrative for interested parties to be able to control what information it can provide.

The Internet is a computer network that interconnects billions of computing devices throughout the world. Not too long ago, these computing devices were primarily traditional desktop computers, Linux workstations and servers that store and transmit information such as Web pages and e-mail messages. Increasingly, however, users connect to the Internet with smartphones and tablets [24]. To be able to dissect how internet censorship works an introduction to the internet as a whole is important.

2.1 Short historical overview of the internet

The beginning of the modern day internet is the project ARPANET or the Advanced Research Projects Agency Network. It was established by the United States Department of Defense Advanced Research Project Agency in 1969. In it's 1983 later iteration it also started using the TCP/IP protocol suite also known as the Internet protocol suite, which is still in use today and a key technology upon which the internet is built upon. Further spread and growth was then the result of universities making their own networks. Expansions further led to the commercialization of the technology. With more research, such as the World Wide Web in 1991, it gained even more users and kept accelerating it's growth [18].

That growth has continued at a rapid pace, both in terms of the amount of people adopting the technology and the amount of data transmitted. All the way from the beginning in the 1970s the bandwidth has doubled roughly every 18 months, being coined as Edholm's law (similar in this sense to Moore's law)[6]. In the modern day, accessing the internet has made a significant move from personal computers and laptops, to mobile

devices and even more recently a large amount of electrical devices of all shapes and forms have an internet connection.

2.2 Key technologies of the internet

The internet is made up of key technologies, that are widely adopted, and allow everyone to understand how it works, as well as provide a unified approach. They will be described in more detail in the following subsections.

2.2.1 Protocols

All activity on the Internet that involves two or more communicating remote entities is governed by a protocol. Given the importance of protocols to the Internet, it's important that everyone agree on what each and every protocol does, so that people can create systems and products that interoperate [24].

The Internet protocol suite is a crucial set of protocols for the internet. The vast majority of communication protocols used today are from this protocol suite. It will be discussed more in detail in chapter 3

2.2.2 Packet switching

Packet switching is used to transmit data over the internet by dividing it into so called packets. Each packet contains it's part of the data being sent, as well as information about itself that is used for navigating it through the network. The advantage of this approach is that packets are sent independently through the network, with each making it's own way to the destination. There they are once again combined to reconstruct the original data being sent.

This technology is fundamental to the internet, as it allows for more efficient use of the available bandwidth and increases the reliability of data transmission. This is because it allows for multiple communications over the same infrastructure and even creating alternative routing in cases of damaged or overloaded parts of the network.

2.2.3 ISPs

Internet service providers (ISPs) provide access to the internet for individuals and organizations. They manage the infrastructure required for internet connectivity and are responsible for transmission of traffic from end users to the internet and vice versa. ISPs also provide services such as domain registration, web hosting or email services. All of this gives them a large amount of control when accessing the internet, where they can implement policies to affect access to certain parts of the internet as well as control over the speed and security of those connections. This provides them a lot of power in terms of direct censorship, especially in authoritarian regimes. However, there is also the possibility of exercising this power in democratic countries, primarily for financial gain, where protections against this come in the form of Network neutrality legislation.

2.2.4 Network security and firewall

Network security is a set of policies, procedures and technologies created and enforced to protect the integrity, confidentiality as well as controlled access to a computer network. A firewall is used to enforce this set of rules. It works by monitoring network traffic between two networks, commonly a local network and the internet [7].

Firewall is an umbrella term as they can vastly differ in both the technology used to make them as well as their complexity. The principle method used is always about evaluating packets and whether or not they can be allowed past the firewall. They started as simple packet filters, where the filtering was done by inspecting just the packet headers and using data such as the protocol, source and destination IP address or the same information about ports to make their decision [7]. The ability to monitor and track active connections and monitor the payload as well as the header was added as the need arose in the 1990s. After came the so-called next-generation firewalls which added functionalities such as intrusion prevention systems and deep packet inspection, which allow even more protection against attacks as well as adding more monitoring and control about information that passes through such a firewall [7].

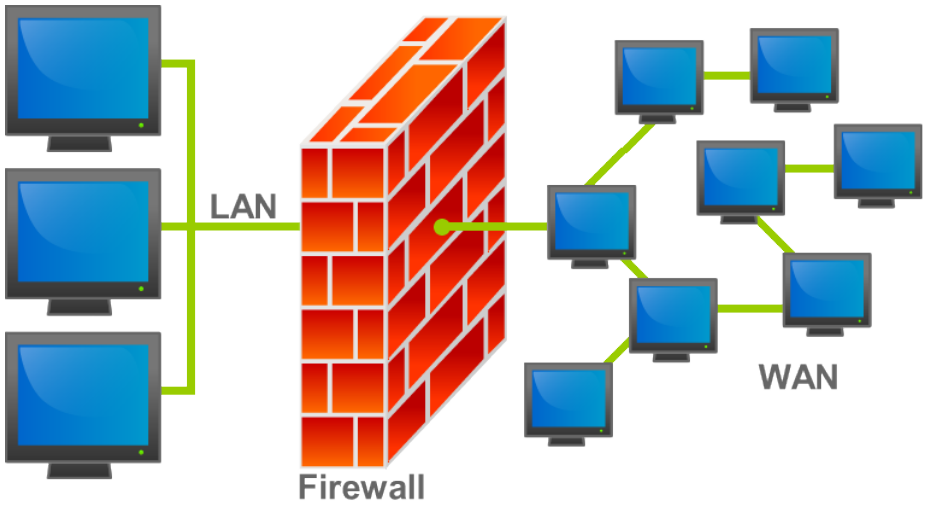

Figure 2.1: A schematic diagram of a firewall. Source: Wikimedia Commons [10].

Chapter 3

Layered model of the internet

The internet is structured around a layered model, primarily to simplify complexity in network communications. This approach compartmentalizes different network functions into separate layers, each handling a specific aspect of network communication.

The most important layered models in regards to the internet are the Open Systems Interconnection (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP). The OSI model, developed by the International Organization for Standardization (ISO), is a theoretical framework consisting of seven layers. It was designed to support universal compatibility in network systems. The TCP/IP model was developed by DARPA and due to it's more practical approach it has been adopted over the more theoretical OSI model. It is generally used today and unlike the OSI model's seven layers, it condenses them into four. The comparison between both models is shown in Figure 3.1.

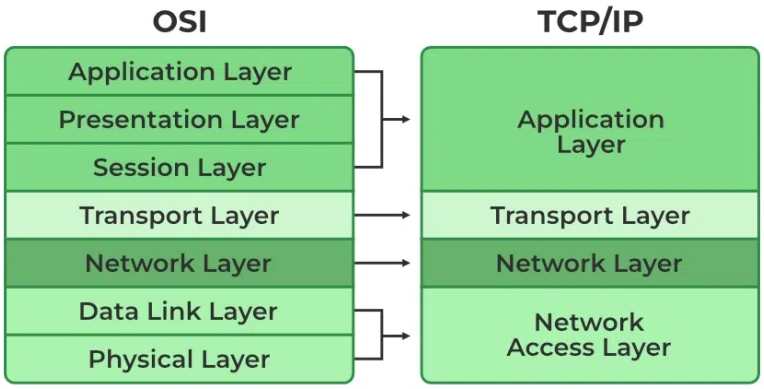

Figure 3.1: A TCP/IP vs OSI comparative model. Source: GeeksforGeeks [15].

The reason for the adoption of the TCP/IP model is due to it's simpler and more flexible architecture making it more feasible to implement and adapt to the real world. The OSI model is more defined and detailed, however this makes it too constrictive and difficult to use realistically. As such this chapter will focus on the TCP/IP model. Following it's design it will be structured by layers allowing to go more in-depth on all of them. End systems, packet switches, and other pieces of the Internet run protocols that control the sending and

receiving of information within the Internet. The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are two of the most important protocols in the Internet[24].

3.1 Link layer

The Link Layer, is the lowest layer of the TCP/IP model. It encompasses the protocols involved in the linking of devices that are physically connected. This layer is responsible for the actual transmission of data over network connections, including the handling of bits over a physical medium, providing a means for exchanging data between connected network nodes. It is also sometimes known as the network interface layer. When comparing the TCP/IP model and the OSI model it is sometimes described as the combination of the OSI layers physical layer (layer 1) and the data link layer (layer 2).

3.1.1 Involved technologies

Examples of technologies within the link layer include.

- Ethernet is used for Local Area Networks (LANs).
- WiFi is used for Wireless Local Area Networks (WLANs) and is standardized by the IEEE 802.11x standards.
- Other technologies include Digital Subscribe line (DSL), Point-to-Point Protocol (PPP) and others.

3.1.2 Functionality

The Link Layer's primary function is to move packets between the Internet Layer interfaces of two different hosts on the same network. Packets from the internet layer are packaged into frames. Each frame contains header information, such as source and destination MAC addresses, which are necessary for transporting the packet to the next device along the path. They also contain trailer information used for ensuring their integrity. Frames are checked for errors typically introduced by the physical medium, like noise or interference. Protocols such as ARP (Address Resolution Protocol) are used within this layer to map an IP address to a physical machine's address that is recognized in the local network.

By handling the direct transfer of data between devices on the same network, this layer ensures that higher layers can function without needing to manage the specifics of what hardware is being used or how connections are maintained physically. This abstraction allows focus on higher-level network strategies and data management.

3.2 Internet layer

The Internet Layer enables data in the form of packets to navigate multi-network connections that make up the internet. This layer handles the logical transmission of data packets through routing, ensuring that data sent from one device reaches its intended destination regardless of the physical network type. It's very similar to the OSI model's network layer (layer 3) and is sometimes referred to as such.

3.2.1 Involved technologies

- Internet Protocol (IP) is the fundamental protocol in this layer and is responsible for addressing and routing data packets. IP addresses are unique identifiers assigned to each device on the network, allowing for data to be directed appropriately.
- Internet Control Message Protocol (ICMP) works alongside IP, it provides error reporting and operational information capabilities, helping to manage and maintain network flows.

3.2.2 Functionality

The main purpose of the Internet Layer is for addressing and routing, where every packet sent through the network contains a header with it's source and destination IP addresses. Routers then use this information to decide the next point in the network to send the packet to. This is affected by the current condition of the network and the routers current routing table.

In case the packet is too large and exceeds the Maximum Transmission Unit (MTU) of the network, IP packets may need to be broken down into smaller fragments to be transmitted. These fragments are reassembled into the original packet format once they reach their destination.

The Internet Layer is responsible for making the internet scale-able as well as provides robustness to data transmission. It allows packets to use different types of networks from LANs to global networks.

3.3 Transport layer

The Transport Layer functions as an intermediary between the routing of the Internet Layer and the applications at the Application Layer. This layer is responsible for managing data delivery across the internet between sending and receiving applications. It ensures that the data arrives to the appropriate process.

3.3.1 Involved technologies

- Transmission Control Protocol (TCP) is a connection-oriented protocol that guarantees reliable, ordered, and error-free data transmission between two communicating applications. It uses a three-way handshake to establish a connection (shown in Figure 3.2), checks packet delivery through acknowledgments, and re-transmits lost packets. Unlike UDP it provides end-to-end reliable communication. TCP packets are called segments.
- User Datagram Protocol (UDP) is a connectionless protocol that provides a lightweight method for transmitting data without guaranteeing reliability. It is primarily used where speed is critical, such as in real-time applications like video streaming or VoIP. Reliability of the communication can still be managed by the application. UDP packets are called datagrams.

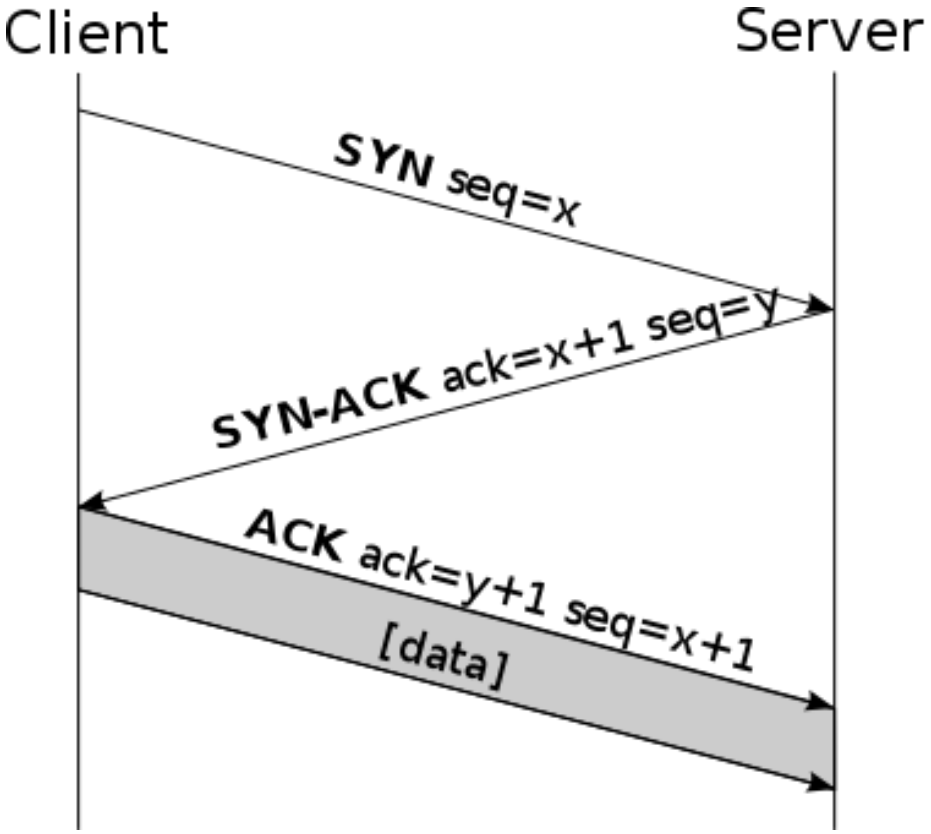

Figure 3.2: The process of a TCP handshake. Source: Wikipedia Commons [11].

3.3.2 Functionality

The Transport Layer assigns port numbers to different applications to distinguish data flows. They serve as logical endpoints that help distinguish multiple communication streams or services running on the same network device. Each port is associated with a specific application or service, allowing multiple applications to share a single network connection.

For UDP communication, each packet of data is handled independently of the others, without checking for the completeness of the data or the order it was delivered in. TCP on the other hand establishes connections via a three-way handshake, where the sender and the receiver both agree on the communication parameters. This persistent connection allows the monitoring of the transmission for errors, re-sending any lost packets and allows for the ordering of the data by the receiver in the order that it was sent. TCP also allows for flow control, which can prevent a fast sender from overwhelming a slow receiver.

3.4 Application layer

The Application Layer is the topmost layer in the TCP/IP model and is directly responsible for delivering network services to end-users. It provides the protocols and services that enable user applications to communicate over the network.

3.4.1 Involved technologies

- Hypertext Transfer Protocol/Secure (HTTP/S) is the most important protocol for browsing the web. It is used to request the content of web pages from a server by the client. In the modern day the secure version HTTPS is used more, it adds a security layer by encrypting the transported data providing confidentiality and data integrity during transmission.
- Domain Name System (DNS) associates information with domain names, for end-users most importantly allowing them to type in the name of a website, rather than having to know it's IP address.
- Transport Layer Security (TLS) is a protocol used to encrypt data on the application layer. It establishes secure sessions, providing privacy, authentication, and data integrity for protocols like HTTPS, ensuring privacy and security. It is the successor of the deprecated Secure Sockets Layer (SSL).
- File Transfer Protocol (FTP) provides a method of transferring files between computers over the internet. It is used for uploading, downloading, and organizing files on remote servers.
- Protocols concerning email communication are also a part of the application layer.

3.4.2 Functionality

The application layer implements protocols, that define how data should be handled. These protocols also standardize how applications can communicate between each other on the network. For example HTTP specifies how the content of a web page is requested and transferred, or DNS mapping domain names to IP addresses providing a more convenient way of navigating the internet for users.

Session management can also be done at the application layer for example through the use of a session token. This can be useful for storing user specific data between requests such as not requiring authentication with every new request.

How applications handle data is also a part of the application layer. Commonly web pages have a different layout for mobile and PC devices. Another aspect of this is authentication and authorization of the application between the server and the client applications.

Chapter 4

Internet censorship

With ever more people being connected to the internet, so too does it's censorship have a greater impact. Governments, organizations, and even private entities implement varying degrees of control over online content, and they often justify them as measures to maintain national security, prevent illegal activities, or protect societal values. These controls can however frequently lead to the suppression of free speech and limit access to information. The purpose of this chapter is to explore how internet censorship is implemented and provide the information necessary to understand what effect these practices have on individual users and whole societies.

4.1 Historical evolution of internet censorship

Censorship has been a part of the internet since it's early days. As it evolved from a small network connecting academic and research institutions into a global one used by the masses, there quickly surfaced concerns over content regulation and control. Governments and organizations began developing ways to monitor, filter, and restrict online content.

Control over various forms of media, such as books and other printed publications, has been practiced before the global adoption of the internet. Censorship on the internet followed in a similar manner, with control over it's content. In the late 1990s, some governments began establishing the first formal systems for monitoring online activity. A notable example is the „Great Firewall“ in China[3], which started blocking websites critical of the government.

As the internet grew in scale in the 2000s, so too did censorship expand it's reach. Governments imposed stricter controls, particularly targeting political dissent, religious content, and sexual material. During this period, cooperation between tech companies and governments grew to ensure compliance with their regulatory standards. An example of this is the arrest and conviction of a Chinese journalist convicted and sentenced based on his email correspondence. This was done thanks to the cooperation of Yahoo!, which is also known to have cooperated after the September 11th 2001 terrorist attacks[26]. In some cases, companies began to censor content proactively, leading to debates over corporate responsibility versus government mandates.

By the 2010s surveillance and automated content moderation became more sophisticated. Some governments began implementing more extensive surveillance methods as well as introducing new legislation to assert more control. In this time social media grew massively and so too did the interest of governments in them. Social media networks are home

to some very advanced algorithms used for flagging and removing problematic content. This also led to the rise of self-censorship where users can feel pressured to not share certain opinions due to the risks related with publishing them.

Sometimes even more direct methods are employed such as shutting down access to the internet entirely as could be seen in the military coup of Myanmar in 2021. These were also followed by blocking access to the social media Facebook, which had been used by dissenters of the coup to coordinate opposition[16].

4.2 Methods of censorship

As stated above, censorship can take shape in many forms using different methods. The following section will look at different methods of censoring the internet as well as the way they are implemented and in relevant cases describe how they fit into a layer within the TCP/IP model.

4.2.1 IP blocking

IP blocking is a method of censorship where specific IP addresses are intentionally prevented from accessing a network or particular websites. An IP address is a unique identifier for a device on the internet, and blocking it restricts that device's ability to send and receive data with certain networks or services. Working with IP addresses, IP blocking works on the internet layer of the TCP/IP model.

IP blocking works via configured firewalls or routers, usually set up by an ISP or a network administrator, that have a list of IP addresses to deny incoming and outgoing traffic from. When a device tries to connect to a blacklisted IP, the firewall checks this list and drops or rejects the request. This is commonly done to enforce geographical restrictions, preventing access to services or websites available only in certain regions.

This method is very effective for connections with static IP addresses, such as those used by web servers. By denying access to a single IP address, entire websites or services can be blocked. This means that with the rise of dynamic IP allocation the effectiveness of this method is lessened in certain situations.

Other methods of intentionally bypassing IP blocking are the use of Virtual Private Networks (VPNs) or proxy servers which allow users to route their traffic through a different server, thus masking their own IP address. This is commonly done for changing a users region and bypassing geolocation restrictions.

Examples of widespread use of IP blocking are the Chinese Great Firewall and Russia utilized it to combat political dissent by blocking access to the messaging app Telegram[28]. It still remains a widely used method of censorship today. The implementation is relatively straightforward and is effective for general filtering of online content.

4.2.2 DNS for censorship purposes

This method makes use of the way web browsers translate domain names to IP addresses. It works by manipulating the translation process of DNS to block access to specific websites. Working with DNS it works at the application level of the TCP/IP model.

Similar to IP blocking works with a blacklist of domain names. If a DNS resolver gets a request to translate a domain name on it's blacklist it may refuse to resolve it. Alternatively it can be configured to resolve certain domain names but return a different IP address, either

to misdirect the user or redirect the user to a different page such as a government warning page. By altering the way DNS works it can be effective at blocking problematic content.

Since it is also a straightforward approach to filtering content, the methods of bypassing it are similarly straightforward. Users can configure their devices to use alternate DNS servers that do not have the same rule-set, thus getting the desired DNS resolution. Modern browsers like Mozilla Firefox and Google Chrome also offer DNS over HTTPS (DoH), where the DNS requests are encrypted using HTTPS and resolved by the browsers specified DNS server before being encrypted again and sent back. VPNs and proxy servers can also be used to bypass DNS filtering.

Many governments like China and Iran use DNS filtering to restrict access to undesired websites containing for them sensitive content. In the case of China the use of foreign public DNS resolvers is not blocked, however if the DNS query matches a banned keyword, the firewall will inject a fake DNS reply[20].

4.2.3 URL filtering

URL filtering is a method of censorship that targets specific web pages based on their Uniform Resource Locator (URL). A URL is a web address that provides information about the location of a resource on the internet. With URL filtering, ISPs or network administrators create rulesets that prevent access to specific web pages or sites that match predetermined patterns.

URL filtering systems compare requested web addresses against a list of banned URLs or URL patterns. The blocklist can contain individual URLs or have blocked keywords. For instance, any URL containing certain words, phrases, or subdomains could be restricted. URL filtering systems can also group URLs into categories, such as gambling, and block whole categories based on the network administrator's preferences or government policies.

Because URL filtering blocks specific web pages there is a finer level of control over blocking whole domain names using DNS filtering. Using HTTPS can mitigate URL filtering as HTTPS encrypts the URL, making filtering more difficult. The Server Name Identification (SNI) can still be scanned for keywords during the handshake process as it is plain text. This again can be mitigated through Encrypted client hello (ECH) which enables encryption of the client hello message. ECH is a replacement of encrypted SNI (ESNI) which ended up having drawbacks with reliability. URL filtering can also be mitigated through the use of a VPN or proxy server. Since it also relies on a list of blocked URLs, the maintenance of this list can be labour-intensive.

The governments of Saudi Arabia and the United Arab Emirates make use of URL filtering to block websites containing pornography, gambling, and politically sensitive material. The Great Firewall makes use of it as well, scanning the content of the web page for HTTP requests and the SNI for HTTPS requests[4].

4.2.4 Deep packet inspection

Deep packet inspection (DPI) is an advanced method of network filtering that examines the content of data packets being transmitted over a network. Unlike traditional firewalls that inspect packet headers only, DPI analyzes the entire packet, enabling it to detect and filter specific keywords, protocols, or data patterns. Governments, ISPs, and organizations often use DPI to enforce censorship or monitor compliance with policies.

DPI works by inspecting caught packet's header and payload information for specific attributes or patterns that can trigger further actions to be taken. The data portion of

each packet is compared against predefined patterns, keywords, or signatures associated with undesirable content. This analysis allows DPI to identify specific types of traffic, like peer-to-peer (P2P) file sharing or encrypted traffic, as well as particular phrases. The results of the analysis can prompt further action including blocking the traffic entirely if it contains forbidden patterns, throttling the traffic which is often used to discourage P2P file transfers or simply logging the traffic for further analysis or to be used as evidence.

Since DPI provides a deeper look into the traffic it can be configured to act on specific traffic or keywords providing more control. It's effectiveness can however be lessened by the use of encryption, such as HTTPS or the use of VPNs, which makes analyzing the payload of the packets more difficult. Another disadvantage is it being more resource intensive than methods such as IP blocking because the data has to be examined which in a large volume of traffic can require significant computational power.

The National Information Network of Iran makes use of DPI for surveillance and censorship purposes such as filtering keywords and blocking sensitive content[2]. The Great Firewall also employs DPI for monitoring messaging services and social media. Ethiopia also uses DPI in times of unrest to control access to many services, especially media outlets[41]. It also identifies VPN traffic for blocking or throttling. While DPI can be highly effective for censoring the internet, advancements in the adoption of encryption and anonymization technologies could limit it's efficacy.

4.2.5 Firewalls

Firewalls can be used as tools for censorship by setting up their security rules as such. Since they form a barrier between networks they can be configured to block or restrict specific types of traffic making them one of the most used tools in terms of censorship.

Packet filtering

Firewalls as packet filters work by examining the headers of the packets passing through them and checking with their rules whether to allow or block it's passage. Packet filters can provide a cheap and useful level of gateway security [7]. The possible header information to be used in rules for packet filter is:

- Source and destination IP addresses
- Source and destination ports
- Protocol used

Combinations allowed ports for certain protocols is also used, if there is a mismatch of the port for the protocol the packet will be dropped. Packet filters can be used to filter out whole IP ranges such as in the cane of the Great Firewall.

Packet filtering firewalls are often stateless, meaning they inspect packets independently without considering the context of previous traffic. This simplicity makes them fast but limited in detecting sophisticated threats.

Stateful firewall

Stateful firewalls improve upon stateless packet filtering by maintaining information about ongoing connections. They track the state of network sessions to make more informed decisions about which packets to allow or block. This is done by maintaining a connection

table, which keeps track of active sessions and their state (e.g., handshake, data transfer, termination). Each packet is compared against this table to verify that it belongs to an established or expected session. By tracking the state of connections stateful firewalls can drop packets that emit unexpected behaviour.

A stateful firewall provides more control over a packet filer, however this is at the cost of also being more resource intensive to maintain.

Application firewall

Application-level filters deal with the details of the particular service they are checking, and are usually more complex than packet filters. Rather than using a general-purpose mechanism to allow many different kinds of traffic to flow, special-purpose code can be used for each desired application[7].

Application firewalls are a prime example of using DPI, for example for scanning email communication for keywords that might set off a flag for blocking or logging and further monitoring. Due to working at the application layer they provide even more fine control over services such as blocking particular features of web services. They are also used for malware detection.

Logging with firewalls

Logging is a standard feature of firewalls that records information about network traffic passing through them. This feature is designed to monitor activity for security and troubleshooting purposes. It is also often used for censorship purposes, firewall logging enables authorities or organizations to identify, trace, and potentially suppress undesirable online behavior.

Firewalls can log metadata such as source and destination IP addresses, port numbers, protocols, timestamps, and packet sizes. This data can be used to of who is accessing which resources, when, and how often. They can also log specific events such as rule violations, blocked access attempts, or the use of banned protocols. These logs can be used to find users that might be trying to circumvent censorship or interact in other undesirable activity. This could happen if a user attempts to access blacklisted websites or VPN services.

By analyzing logs, censors can identify users frequently visiting restricted websites or communicating via banned messaging services. This information can then be used to flag users for further surveillance or investigation. These logs can then also serve as evidence to prosecute these users, especially in countries with heavily restricted internet use. Another example of using those logs can be for the detection of censorship circumvention methods such as identifying VPN usage.

4.2.6 Content removal

Content removal is the practice of taking down or censoring specific online material that has already been published. This approach can be initiated by governments, social media platforms, or website owners themselves, often through formal legal requests, direct pressure, or by applying platform-specific policies. Content removal can range from deleting individual posts to disabling entire user accounts or shutting down websites.

Governments can issue legal orders to internet service providers, social media platforms, or website operators to remove content deemed illegal or in violation of local regulations. In a similar manner social media platforms have their own content policies that align with

government regulations or their own community standards. Automated systems and content moderators then flag and remove posts violating these policies. Some website owners also preemptively remove or censor content to avoid potential legal consequences, particularly in countries with strict censorship laws.

Policing of available content is highly effective for directly suppressing specific types of information, particularly when backed by legal orders. It can minimize the dissemination of certain narratives or sensitive materials. It is however limited by it's spread through other means such as other social media or websites making complete suppression difficult. Some users may use anonymous accounts, encrypted messaging, and decentralized platforms to evade identification and continue sharing banned content.

An example of content removal legislation is the EU requiring social media companies to remove hate speech and terrorist propaganda within 24 hours of being flagged. In other countries removal can be ordered for posts critical of the government or may be deemed undesirable, examples of this being the case are India and Turkey.

4.2.7 Regulation

Regulatory tools used by governments to control internet content and access by requiring online platforms, publishers, and service providers to obtain government-issued permits. These requirements often impose strict conditions that can influence how these entities operate and what kind of content they can host or produce.

Governments may mandate that ISPs and websites obtain special licenses to operate legally. Licensing conditions often include compliance with censorship laws, granting government access to data, and blocking or removing specific content. Governments sometimes require users to verify their identity before accessing certain services. For instance, social media platforms may need to link accounts to real-world identification documents. Another instance being China requiring registration to play online games in an attempt to limit the amount of time underage people spend playing them[8].

Licensing and registration can prove effective at keeping various platforms compliant with government requests. This can mean providing them with user data and surveillance of their users. This may be harder with international platforms and sometimes the chosen solution is to ban them within the country.

4.2.8 Surveillance

Surveillance is a method of censorship where governments or organizations keep track of user activity to identify, suppress, or punish the distribution of undesirable content. These methods can include methods such as tracking IP addresses or keywords, as well as direct monitoring of online behavior of specific individuals.

Monitoring of which IP address is responsible for certain behaviour can also enable the government to identify the user responsible. This monitoring can be set off by a flagged keyword or attempt to visit a certain website, logged and then used further. Analyzing internet traffic can also lead to such a scenario. Governments can directly pass and enforce data retention laws that require ISPs and other companies to retain data about it's users and provide it to the authorities upon request. Some countries take this a step further by requiring their citizens to register to online platforms before being able to use them.

The Chinese government has developed the Golden Shield Project for monitoring their domestic internet. It is used for monitoring the activities of their netizens. The United States also operate a surveillance program called PRISM.

4.3 Circumnavigating internet censorship

In regions where internet censorship is heavily enforced governments often deploy numerous censorship measures, such as IP blocking, deep packet inspection, and content takedowns, in an attempt to suppress dissenting opinions, restrict access to information, and monitor online behavior. Individuals wishing to access blocked information, communicate securely or preserve their online privacy use various tools to get around these censorship methods.

4.3.1 Tunneling

Tunneling is a method of transmitting data across the internet through an encrypted channel, effectively encapsulating the data within another protocol to protect it from inspection or modification. Tunneling techniques are useful for getting around internet censorship, as they mask the content of the traffic passing through them. They provide a secure way to bypass network restrictions and access blocked content.

VPNs

VPNs are one of the most popular and accessible tools for circumventing censorship today. They establish an encrypted tunnel between a user's device and a remote server located outside the censoring network. By routing internet traffic through this server, users can mask their true location and appear to be accessing the internet from a different region. This allows them to bypass regional content restrictions and access blocked websites.

Thanks to encrypting the sent data between the user's device and the VPN server, it makes it difficult for censors to inspect the content of the data packets. The censor can only see where the traffic is coming from and the VPN server as the destination, but cannot see where it will head from the VPN server. This also works from the other side where the user's IP address is masked from the destination service as it only sees itself as sending the data to the VPN server.

VPNs use different systems for establishing secure tunnels including:

- OpenVPN - free software, uses the OpenSSL library for encryption
- IKEv2/IPSec - a combination of Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec)
- WireGuard - aims to replace existing tunneling solutions like IPsec and OpenVPN, while requiring less code, being more secure, more performant, and easier to use [31].

The advantage of using VPNs to bypass censorship methods are their relative ease of use and high efficacy at bypassing those methods. By also providing privacy they increase the safety of their user's in the case of authoritarian regimes. They however also have several limitations such as their servers being detected and blocking traffic to and from them. A lot of VPN providers also keep logs on their user's and may be mandated by authorities to provide a user's traffic.

SSH tunneling and SOCKS proxy

SSH Tunneling, or SSH port forwarding, encapsulates data traffic within a secure SSH protocol connection. This encrypted tunnel then passes the data between the server and

client. It can be used to bypass firewalls by connecting to a different network, although by itself it is not one of the most popular methods of getting around censorship.

A SOCKS proxy is an internet protocol that facilitates communication between a client and a server by routing network packets. These are application level proxies that funnel network traffic through protocols designed to allow web traffic to pass through firewalls [33].

Shadowsocks A popular tool for bypassing firewalls is shadowsocks. It is an open-source project originally developed by a Chinese programmer to get around censorship. It is loosely based on the SOCKS5 protocol and reroutes the clients encrypted traffic through a configured proxy server [34].

Domain fronting

Using domain fronting, a user connects to a server by disguising the actual destination server using a hosting provider or content delivery network (CDN). The traffic looks like it is directed to the CDN server, however there it gets redirected to it's true destination. This also makes domain fronting difficult to combat as it comes with heavy collateral damage. This is because to effectively block domain fronting, it is necessary to block the entire fronts, which are also relied upon by many other services. For example to block Snowflake, which is discussed further below, it would be necessary to block the entirety of Google or every foreign IP address, which makes it a pretty high cost to pay for blocking the service[32].

4.3.2 Tor Network and Onion Routing

Onion routing is a technique where data is encapsulated in multiple layers of encryption before being transmitted through a series of network nodes called onion routers. As the data packet passes through each relay, a layer of encryption is peeled away, revealing the destination of the next relay. This ensures that every node knows only the preceding and subsequent nodes with no knowledge as to the rest of the path. This makes it difficult to trace the origin and destination of the traffic. Onion Routing's anonymous connections are protocol independent and exist in three phases: connection setup, data movement, and connection tear-down[17].

The Onion Router (Tor) is a decentralized network that anonymizes internet traffic by routing it through a series of volunteer-operated nodes known as relays. It was originally developed by the United States Naval Research Laboratory in the mid-1990s and is currently managed by the Tor Project. The network uses the principles of onion routing to anonymize data and hide the identities of it's users.

To connect to the Tor network a modified version of Firefox the Tor Browser is used. The network also offers a way to provide anonymity for websites, known as onion services. This is done by allowing these sites to only be accessed through their .onion domain which hides the true identity of the website. .onion domains are only accessible through the Tor network.

Despite it's importance and success in providing an anonymous way of interacting with the internet, the Tor network still has several limitations. Due to communication going through multiple relays the speed of the communication is significantly hindered. Since the final layer of encryption is peeled off at the exit node, the data can be intercepted[42].

Another weakness is the blocking of Tor. Some websites may not accept traffic from Tor exit nodes. There have also been attempts to completely block Tor access, very successfully

in China, due to it's very centralised internet architecture, and less so in Russia[5]. Blocking is done by blocking access to entry nodes, thus traffic cannot enter the Tor network.

In those countries people have to use what are known as "Tor Bridges" to circumvent national firewalls. Tens of thousands of people use bridges regularly to circumvent censorship and national or regional restrictions [32]. Tor bridges are disguised Tor entry nodes and censors attempt to identify and block them using DPI.

Snowflake is another attempt by the Tor project to mitigate the blocking issue by allowing users in areas with blocked access to connect to the Tor network. Snowflake is made up of volunteer-operated proxy servers that users can join by using the Snowflake client, that is packaged within the Tor Browser. Tor users that want to connect to the network first connect to a broker that provides them with a Snowflake proxy through which they can then connect to the network. Brokers difficult to take down because they make use of domain fronting[32]. Due to rapidly changing proxies, with the Tor project providing methods for users to act as proxies, it is very difficult to block access to all of them[39]. Snowflake was widely used in Iran in 2022 and is successfully being used in Russia. Russian censors attempt to combat this by using fingerprinting[5].

4.3.3 Encryption

Encryption tools provide a secure way to communicate and share information over the internet. By converting data into an unreadable format, encryption protects it from unauthorized access and allows users to maintain confidentiality. Many censorship circumvention tools rely on encryption to secure traffic and prevent network surveillance. For example the widespread adoption of HTTPS over HTTP has made some censorship methods more difficult.

End-to-End Encrypted messaging

End-to-End Encrypted (E2EE) messaging ensures that only the sending and receiving parties can view the content of the sent traffic. This can be used to prevent eavesdropping of the communication. The sender's device encrypts the message and only the receiver's device can decrypt it.

Secure Email

Encrypting email communication can be vital for people being targeted by their governments such as journalists to send incriminatory information with less risk of being discovered and prosecuted.

4.3.4 Dangers with privacy and anonymity

In regions with extensive surveillance and strict online regulation, maintaining privacy can be essential for users seeking to access blocked content or communicate securely. Using tools like VPNs or Tor, but often it is important for users to take multiple steps to protect their privacy.

For example VPNs often have known IP addresses, so users should take care when attempting to use them, especially when VPN usage is not just blocked but forbidden and prosecuted. Some VPNs also actively cooperate with data requests or have bad security practices which can lead to potentially leaking sensitive data of it's users.

Websites can partake in fingerprinting which identifies users based on their browser's unique characteristics, such as installed plugins and fonts. This can be used to deanonymize a user and track their activities across multiple websites.

4.3.5 The Uncensored Library

The Uncensored Library is an alternative method of bypassing censorship in countries with limited free press. It was created by Created by the organization Reporters without Borders and the Minecraft design collective BlockWorks[35]. It's a virtual library built entirely within the video game Minecraft where it can be accessed through joining the Minecraft server or downloading it and running it locally.

The library hosts articles by journalists from countries such as Saudi Arabia, Russia, Vietnam, Mexico and Egypt[1]. Each country has it's own wing dedicated to it containing banned articles.

4.4 Internet censorship in Saudi Arabia

In Saudi Arabia, internet censorship is enforced through a combination of technical and regulatory measures designed to limit access to information and other undesirable content. The government enforces it's control via the Communications, Space and Technology Commission (CST), which is responsible for the nationwide firewall used for censoring content. This blocking is focuses at the sociopolitical and historical contexts, which are a combination of the conservative religion, authoritative government and security concerns over extremist groups.

The CST is in charge of regulating and enforcing the censorship rules of Saudi Arabia. It may request any data, information or documents that CST deems necessary to enforce the provisions of the Law, Regulations or regulatory decisions. It also mandates rules for ISPs on how they should manage data, specifically the protecting, processing, sharing, developing, classifying or preserving such data and information, and monitoring compliance with their provisions[12].

The CST maintains a blacklist of websites containing political dissent, pornography, LGBT content, and criticism of the government. This list is enforced through the use of a national level firewall. HTTPS has somewhat mitigated this censorship. For example in the case of Wikipedia specific pages such as those relating the theory of evolution were blocked, however with the adoption of HTTPS Wikipedia appears to be fully accessible[9].

Saudi Arabia censors a wide variety of political, religious, social content and any other that they perceive as a threat to their security. As a part of this it also enacts geopolotical internet filtering such as from Iran or Syria, especially in the case of Iran censoring the majority of Iranian websites. During the Gulf crisis in 2017 it also partook in censoring content affiliated with Qatar. This included websites such as that of the state news agency Qatar News Agency, the websites of al-Jazeera and several other media outlets[29].

There are several groups that it actively censors: [29]

- Muslim Brotherhood - it designates it as a terrorist organization and accuse Qatar of sponsoring the organization.
- Hezbollah - organization backed by Iran, also designated as a terrorist organization.
- Houthis - Yemen political and military movement, Saudi Arabia blocks multiple of their websites.

The internet is also monitored in Saudi Arabia, especially when it comes to social media. One such example is a man being sentenced to prison and lashes for posts on Twitter promoting atheistic views, which are designated as terrorist in Saudi Arabia[40]. Many of the laws for punishing cybercrime and counterterrorism are also very vague such as „defaming the state" or "calling for atheist thought", making targeting anyone deemed a threat easily targetable[19].

Apart from using standard methods of internet censorship and monitoring, Saudi Arabia makes use of sophisticated tracking and monitoring software. This was the case in the very publicized murder of journalist Jamal Khashoggi, whom they tracked using the Pegasus software supplied by the Israeli company NSO Group[23, 36].

4.5 Censorship in the United Arab Emirates

Being neighbors geographically, politically and culturally another similarity that Saudi Arabia and the United Arab Emirates (UAE) share is the content that those two countries censor on the internet. Like Saudi Arabia, the UAE also censors pornographic sites, LGBT content as well as anti-Islamic and anti-government material.

Like Saudi Arabia it has also been working on building a positive image of itself, portraying itself as an open, modern country. Meanwhile it still maintains very strict rules of morality and adherence to religion, regularly arresting their own citizens for criticism and controlling what media can be accessed[22]. This includes human rights activists, journalists and other people deemed uncomfortable, such as the case of Ahmed Mansoor, a journalist and human rights activist, who was jailed for ten years[21].

The regulations are managed by the Telecommunications and Digital Government Regulatory Authority (TDRA) which issues guidelines with emphasis on morality and public order[37]. These are in nineteen categories and include pornography, phishing, drugs and offences against the UAE and public order. In Q4 of 2023 the TDRA claims to have blocked 4212 websites, with 6.7% related to drugs, 49.1% impersonation fraud and phishing, 26.9% intellectual property infringements and 14.9% related to pornography and nudity[37]. The TDRA also maintains a list of allowed VoIP applications.

To achieve the level of control deemed necessary, the government closely regulates the internet as well as use mass surveillance programs. It keeps a majority stake in both of the countries largest ISPs Etisalat and Du, this allows it to mandate any rules and enforce their fulfilment. Unlike China, which enforces a national level firewall, blocking and filtering of content is done by the ISPs which follow and enforce the bans on websites listed by the TDRA. This includes requirements about the monitoring of communication, accessibility of services and which content is allowed. Some of these rules have gotten less strict, such as the UAE lifting some of it's blocks to VoIP services such as Microsoft Teams and Skype, however services such as WhattsApp voice calls and FaceTime remain blocked[14].

Another major aspect of censorship is that related to LGBT. The UAE blocks numerous LGBT related websites, [30] as well as restricting access to content that might be related to such topics. An example of this is requesting the streaming service Netflix to censor or remove "culturally sensitive content aimed at children„[13]. The use of tools for circumventing censorship, such as VPNs, is punishable by law when used for illegal purposes, in this case accessing forbidden content[38].

Similarly to Saudi Arabia it blocked Qatari websites during the 2017 Gulf crisis, blocks websites related to the Muslim Brotherhood and Hezbollah. It also blocks Iranian websites, but to a lesser degree than Saudi Arabia[29].

Over all the UAE focus in a large part on content filtering and moderation, blocking websites it views as undesirable and issuing takedown requests or for content to be modified to suit their requirements. They also use monitoring and subsequent punishments for transgressions justified by religion and strict societal morals to encourage self-censorship of any dissenters. To maintain the maximum level of control for their monitoring the use of circumvention tools is banned, for example the use of VPNs for illegal purposes like accessing banned websites. Another restricted service is VoIP, where a large amount of applications is blocked.

Chapter 5

Censorship analysis tool

One of the goals of this thesis is to design and implement an application to test and practically verify, the use of censorship means. The implementation will be in the form of a Python3 script, that if the requirements are satisfied should be able to run on any operating system. Python3 was chosen because of it's support for network communication and ease of use and addition of modules. It will be executed from the terminal, taking input from specified input files and outputting to text files.

5.1 Inputs

The inputs for the script will be as follows:

- A directory containing categories of websites to test connections to. These can be URLs with specified and IP addresses with optionally specified ports or HTTP/HTTPS connection. If none are specified the script defaults to testing HTTPS.
- A file of google queries to be searched on the target.
- A file containing a list of URLs to test for http tampering
- An additional file containing URLs and IP addresses, for testing various ports and services.

5.1.1 Implementation

The inputs directory contains input files, primarily containing files of IP addresses and URLs, which the test loads and tests. The following files are within the inputs:

- `google_queries.txt` - file containing search queries to Google, each search phrase is on it's own line.
- `urls.txt` - uncategorized IP addresses and URLs which will be tested.
- `cleaned_inputs` directory - directory containing `.txt` files with categories of URLs / IP addresses

A large part of the dataset used for testing if from the citizenlabs project test-lists [25]. A large part of the websites listed within the test list do not exist, so first they were cleaned of entries that had no result from the Google DNS resolver 8.8.8.8. The entries were then separated into separate test files based on their category.

5.2 Website censorship analysis

The script will go through the directory containing the files of grouped URLs and IP addresses. It will create separate directories based on the name of the file for categorization, where it will store the results of the following tests. In the case of URLs it will attempt a DNS resolution. The result is saved to a file, including the IP address in the case of a success. In the case of a success it continues with attempting a TCP connection. IP addresses in the file will immediately go to test for a TCP connection. The result of the TCP connection is saved. In the case of a successful HTTP/HTTPS TCP connection a HTTP GET request is sent either to the path if specified in the URL or IP address and to the root directory if path is not set.

The script will create a directory for every input file of websites. This directory will contain a file with the individual results of the DNS resolution attempts:

- Success : {domain name} {resolved IP address}
- Fail : {domain name}
- Exception : unexpected error {domain name} {error message}

TCP connection attempts:

- Success : {ip address} {port}
- Blocked/FAILED : {ip address} {port}
- Timeout : {ip address} {port}
- Exception : {ip address} {port} {error message}

GET requests:

- {status code} {url}
- Timeout : {url}
- Exception : {url} {error message}

All of the output files will be later grouped into results as well as saved for the possibility of examining them individually.

5.2.1 Implementation

The function `websites` is handed a file containing the URLs or IP addresses to test. It will first create a directory in `output/websites_test/{filename}` where it will save all the grouped results for the given file. It will then parse through the file one entry at a time with the following logic:

It will parse the entry using the `urlparse()` function from urllib.parse. It will then check if a port has been specified for the entry and save that for later functions. A port will also be set if the entry contains http:// or https://. If no port is specified by the above stated logic it will default to the HTTPS port 443. It will then check if the entry is an IP address. If the entry is not an IP address it will then attempt DNS resolution, if it is it goes straight to establishing a TCP connection. DNS resolution is attempted using the socket

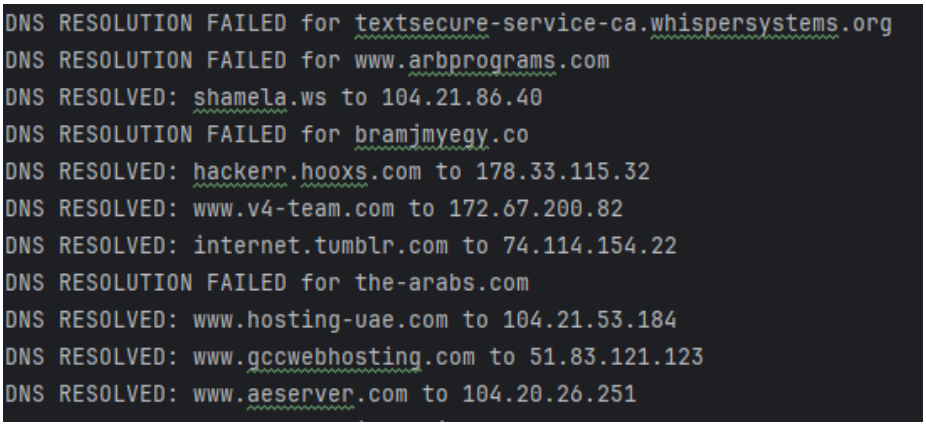

Figure 5.1: Example of saved DNS logs

library and it's result is saved to the dns_resolution.txt file within the output directory for the tested file. Where it logs the result of the resolution, for which entry it was attempted and in the case of a success the IP address it was resolved to.

IP address entries and successfully resolved entries are then tested for establishing a TCP connection. A socket at the IP address and port of the entry is attempted to be opened. If the connection is successful and the entry has a port specified as 80 or 443 a HTTP GET request is attempted from the URL. The response code and the entry are saved to the http_get.txt file for the relevant file. As well as that, a function is called to parse the response of GET request. This includes searching for the title within the HTML of the reply as well as the length of the response to be able to check if in the tested country a successful connection was established with a reply claiming OK, but no content was actually delivered.

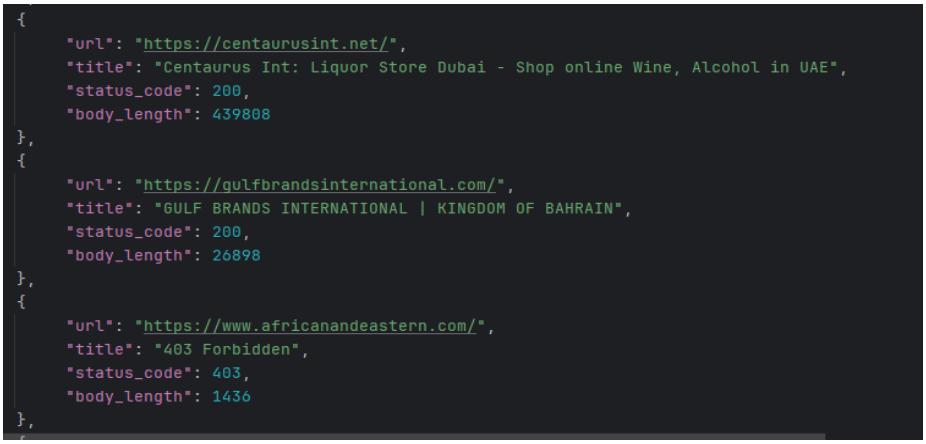

Figure 5.2: Example of saved HTTP GET responses

5.3 Google results

The script will get a result of set Google search results for manual comparison from an input file. The format of the file will be individual search phrases delimited by a new line. The script will make use of the google-this repository on GitHub [27]. Since it is a JavaScript project, the main Python script will create a subprocess to call from this library. The results will be saved in the format provided by google-this in a directory for the Google results.

5.3.1 Implementation

A subprocess is created within the main script, which calls the JavaScript script containing the `googlethis.search()` function used to get the search results from Google. It loads it's search strings from the `google_queries.txt` file within the inputs directory and outputs the results to the `google_results` directory within the output directory.

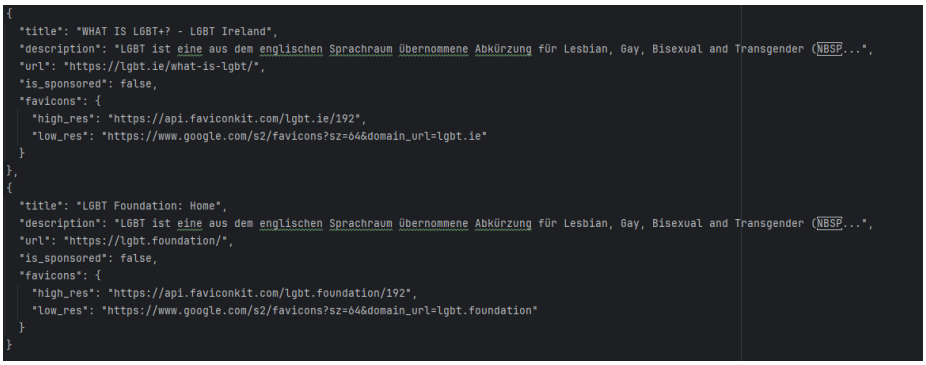

Figure 5.3: Example of returned Google search results

The project was cloned from GitHub [27]. The contents of it have been slightly modified to restore functionality as the project has not been maintained recently and the search results had an issue with return functionality. As such it is recommended to use the provided version instead of installing it through npm or cloning it and adding it manually.

The issue mentioned is described in the Issue #66[1]. The solution was modifying the /lib/utils/constant.js file with the following changes to SELECTORS:

- TITLE: 'a[role="presentation„][ping][data-ved] div[aria-level="3„][role="heading„]
- DESCRIPTION: 'div[data-sncf="1„] div',
- URL: 'a[role="presentation„][ping][data-ved]',

[1] https://github.com/LuanRT/google-this/issues/66

5.4 Telegram test

This script will test the reach ability of Telegram. It will attempt to connect to Telegram access points, then get a response from my bot API and finally attempt to reach the web version of telegram if it's responding. The access points will be acquired by creating a simple Telegram application and requesting them via the Telegram API.

The results of the Telegram test will be saved in the individual directory grouped with the Tor test. They will log the results for accessing the access points, response from the bot API and HTTPS response from the web version of Telegram.

5.4.1 Implementation

First the access points of telegram were gained by registering an application with Telegram to get an api_id and api_hash then calling to the API with the `help.GetConfig()` function which as a part of it's answer lists Telegram access points. The access points are saved in a list within the telegram test script. A bot was also registered with Telegram to be able to make use of the bot API and get a reply to a HTTP POST request.

The test first attempts to send a POST request to the bot API for telegram. It then attempts to establish connections to the access points at both ports 80 and 443. Finally it attempts a GET request to the web version of Telegram web.telegram.org.

5.5 Tor test

This script will attempt to get a rudimentary overview if the Tor network is accessible without the use of Snowflake or bridges. It will check if the Tor directory authorities are reachable. It will then attempt to retrieve a consensus from a directory authority.

The results will show which directory authorities were reachable and which weren't as well as if a consensus request succeeded.

5.5.1 Implementation

The list of Tor directory authorities can be found on the projects GitLab page[2]. This test will first attempt to connect to the directory authorities and then try to get consensus data from them by sending a GET request to the HTTP port for the URL /tor/status-vote/current/consensus.z.

5.6 Testing environment

To test the conditions and make them as realistic as possible the tests must be run within the network of a tested country. In countries like Saudi Arabia, Qatar and the UAE there may be difficulties with this step. For example some companies advertise as providing VPS services in Qatar, but their physical data center is in Lithuania. The use of a VPS was chosen as a viable option, due to it's relative price accessibility and access to the internet within UAE.

[2]https://gitlab.com/torproject/tor/-/blob/main/src/app/config/auth_dirs.inc

5.7 Requirements

The functionality of the test is multi-platform. It was developed on a Windows 10 machine and the testing was done on Ubuntu 20.04. These are the requirements for proper functionality:

- python3
- nodejs - version 14.0.0 or greater
- bs4 - python module used for parsing the HTML for the tampering test
- dnspython - python module used if using DoH instead of regular DNS
- requests - python module used for sending requests

5.8 Results

The results of the preformed tests will be within the output directory. It will contain:

- `google_results` directory - files with results of Google searches
- `individual` directory - Telegram and Tor test output files
- `websites_test` directory - Will contain directories for files of website testing
- `results.txt` - The main script `censortest.py` will parse the results after the tests have concluded.

Each of the subsets will contain detailed information about their individual tests. The `results.txt` will be created by the main process `censortest.py` after the conclusion of the tests. It will provide a brief overview of the results of the test. Such as individual tested website category results with their DNS and TCP success rates as well as the amount of times HTTP responses were recorded for GET requests. It will provide an overview of the totals of DNS resolution, TCP connections and HTTP responses. It will also contain a brief overview of the results of the Telegram and Tor tests.

Chapter 6

Experiments

Execution of the test tool is done by running `python3 censortest.py`

6.1 Test data

The input test data for the Tor test remains the same and can be used universally, unless some of the directory authorities are changed. The Telegram test can also be used without changes as long as the bot API remains active and the access points do not change. For the Google search results a list of ten search phrases was used. The websites test dataset consisted of 8 primary categories those being:

- Alcohol and gambling - websites related to alcohol, drugs and gambling
- Anon, search and host - websites related to staying anonymous on the internet, alternative search engines and hosting providers
- Companies - websites of companies both international and regional
- Criticism - websites related to criticism of governments, Islam and environmental issues
- Culture and religion - websites related to talking about culture or hobbies and sites related to various religions
- Military and government - military, militant and government websites of various countries and groups
- News - websites of news outlets
- Sex - websites related to pornography, LGBT content, sexual health and dating

There is also CTRLS containing control websites and the file urls.txt which contains additional URLs and IP addresses I wanted to check.

6.2 Control test

The first test was done connected to a VPN in Germany Frankfurt with the same datasets, that would be used for testing within the UAE. Due to using a VPN a lot of the websites

using DDOS protection from services like CloudFlare refused the HTTP GET request with the code 403.

The test results show a low amount of censorship with the Telegram and Tor tests returning consistent results with a manual test done on my home PC. All of the Tor directory authorities were successfully connected to and returned consensus data. All Telegram access points were reached, the bot API successfully replies to the POST request and the web version of Telegram was also successfully reached. The Google results are also in-line with them containing the same type of content, the main differences in the results are due to localisation, despite running the search with the 'en' parameter for English results.

The results of the experiment are displayed using pie charts representing individual categories as well as a pie chart showing the overview of the whole test.

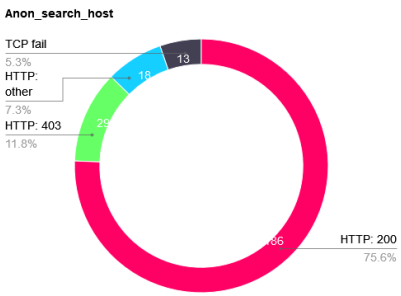

Figure 6.1: Anon, search and host category result of control test

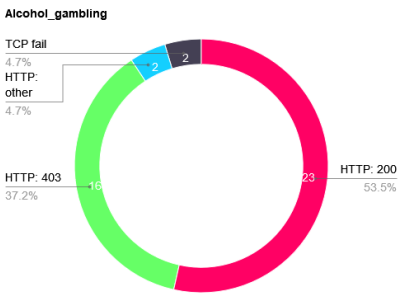

Figure 6.2: Alcohol and gambling category result of control test

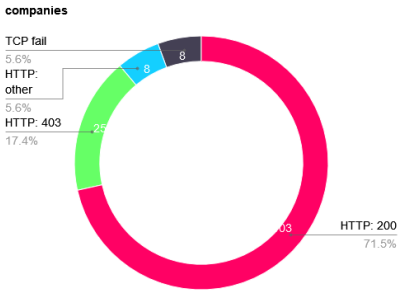

Figure 6.3: Companies category result of control test

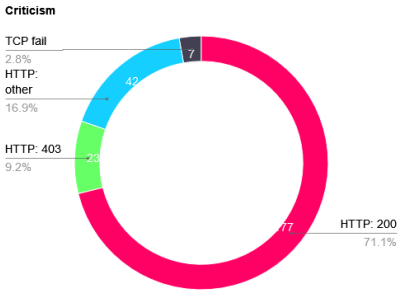

Figure 6.4: Criticism category result of control test

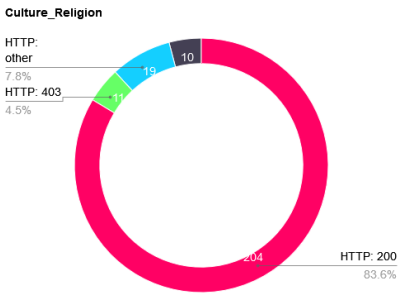

Figure 6.5: Culture and religion category result of control test

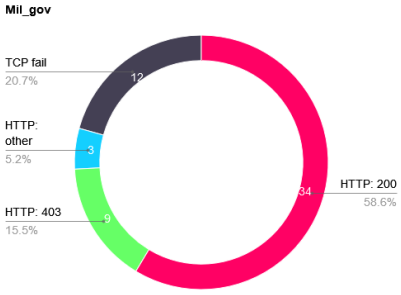

Figure 6.6: Military, militant and government category result of control test

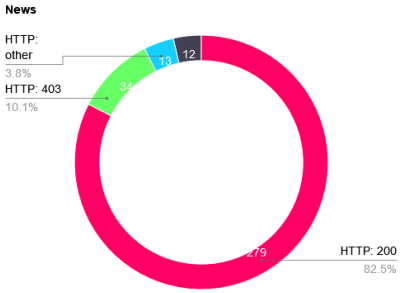

Figure 6.7: News category result of control test

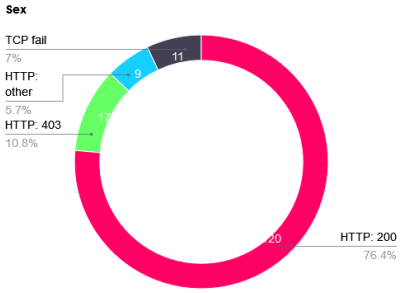

Figure 6.8: Sex category result of control test

6.3 Testing on AHost VPS

The first VPS used for the experiment was from the provider AHost.eu[1]. Despite the VPS being in a data center within the UAE the results of the test were very similar to that of the one being ran from the VPN and manual testing testing. There were only a few notable examples like `www.heineken.com` which check the IP of the accessing client and tailor their response, in this exact case by replying with a blocked page.

The conclusion that I was able to reach was that due to censorship being enforced by the ISPs, using a non user grade internet connection bypasses these restrictions. To test this theory I also bought access another VPS, from a different provider `serverwala.cloud`[2], and a VPN with a server within the UAE and got the same results, being able to access any website, including pornography, the Tor network and the contents of Google results being the same as in my other testing, including links to otherwise blocked sites. The comparison of running the tests on a uncensored VPN and a VPS located in the UAE is shown below.

[1] ahost.eu
[2] serverwala.cloud

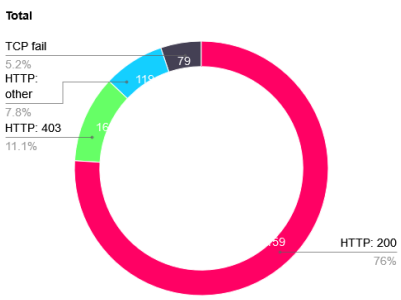

Figure 6.9: Result totals from the control test

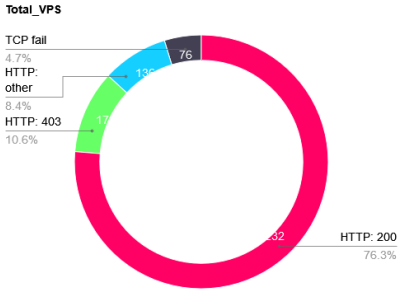

Figure 6.10: Result total of running the test on a VPS

Chapter 7

Conclusion

The goal of this thesis was to examine the situation of internet censorship in the UAE. First the methods of censoring the internet were studied. The different methods were examined in depth, looking at how they are categorized as well as what technologies they rely upon. The investigation to the means of censorship was followed by a look at methods for internet censorship circumvention. These looked at the popular methods of circumventing censorship today as well as the way they interact with censorship methods.

This was then followed up by focusing on censorship of the internet in the UAE. This examined what parts of the internet are censored, the purposes for this censorship as well as their implementation. It also focused on the topic of monitoring within the country and that it is a risk for individuals of interest, like journalists.

The censorship analysis tool was then designed to test various methods of censorship. This primarily consisted of testing websites if they are censored, as well as saving the information for further examination and possible review if the resulting replies had been tampered with. It also contains tests for the accessibility of the Tor network, if the messaging service Telegram is accessible and the possibility of getting Google search results for topics of interest to compare them with results from an uncensored location.

The tool can be used to test censorship in other countries as well, as the tests are not region-specific. Using it in another country will require the changing of the input, namely the files containing the lists of the websites to be tested, to adapt the tests to the tested country.

I was unable to prove the presence of censorship using my tool within the UAE. I believe this isn't due to the tool being inherently faulty, as it's data collection works and the methods used for obtaining it are correct. Censorship within the UAE is also definitely present and prevalent, with reports about it coming regularly as it being one of the most censor heavy countries in the world. My censorship analysis tool wasn't able to prove that. To try proving the presence of censorship I tried manually testing websites both through the VPS I used as well as purchasing VPN access within the UAE and testing for censorship both using the tool and manually. In none of these scenarios was I able to obtain proof of censorship being present.

Since the censorship of the internet is carried out by the ISPs in the UAE, I believe, that if I was able to get a user grade connection, travelling to the UAE however was not financially viable for me. An alternative could have been requesting a person physically in the UAE to allow me access to their device and test for censorship that way, however that might put the person at risk as attempting to access illegal content could face them with repercussions.

A conclusion to this however is, that it is possible to bypass most censorship methods within the UAE by connecting to a VPS or VPN. This does not take into account possible monitoring that might be happening at this level, but it makes connection to forbidden websites and services possible.

The core functionality of the tool works well as far as my testing allowed. It could be expanded with more tests and automation. For example the Tor test could be expanded to check for the blocking of Tor bridges or if Tor Snowflake is being blocked. Additional services like Signal could also be added to the tests to provide a greater breadth of information. For the checking of the websites the addition of using DNSSEC and the impact it would have on the results could be an interesting point. To the automation aspect, the tool could be expanded upon to check it's results against a trusted server, that would provide known uncensored results and allow for a more automatic comparison of censorship.

Bibliography

[1] *The Uncensored Library*. Accessed on April 15, 2024. Available at: https://uncensoredlibrary.com/en.

[2] 19, A. *Tightening the Net: Iran's National Internet Project*. Article 19, 29. Mar 2017. Accessed: 2024-01-05. Available at: https://www.article19.org/resources/tightening-the-net-irans-national-internet-project/.

[3] Barmé, G. R. and Ye, S. *The Great Firewall of China*. 1. June 1997. Accessed: 2024-01-05. Available at: https://www.wired.com/1997/06/china-3/.

[4] Blog, X. *What is the Great Firewall of China and why you should care*. Accessed: 2024-01-05. Available at: https://blog.xeovo.com/what-is-the-great-firewall-of-china-and-why-you-should-care/.

[5] Burgess, M. How Tor Is Fighting—and Beating—Russian Censorship. *Wired*. July 2022, [cit. Accessed: 2024-04-02]. Available at: https://www.wired.com/story/tor-browser-russia-blocks/.

[6] Cherry, S. Edholm's law of bandwidth. *IEEE Spectrum*. 2004, vol. 41, no. 7, p. 58–60. DOI: 10.1109/MSPEC.2004.1309810.

[7] Cheswick, W. R., Bellovin, S. and Rubin, A. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, 2003. Addison-Wesley professional computing series. ISBN 9780201634662.

[8] Chris, B. *China Tightens Limits for Young Online Gamers and Bans School Night Play*. 30. August 2021. Accessed: 2024-01-05. Available at: https://www.nytimes.com/2021/08/30/business/media/china-online-games.html.

[9] Clark, J., Faris, R., Morrison Westphal, R., Noman, H., Tilton, C. et al. *The Shifting Landscape of Global Internet Censorship*. Berkman Klein Center for Internet & Society, 2017. Accessed on May 2, 2024. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425.

[10] Commons, W. *Schematic diagram of a firewall*. 2007. Available at: https://commons.wikimedia.org/wiki/File:Firewall.png.

[11] Commons, W. *Diagram of the initialisation (handshake) of a TCP connection*. 2010. Available at: https://commons.wikimedia.org/wiki/File:Tcp-handshake.svg.

[12] Communications, Space & Technology Commission. *Implementing Regulations of the Telecommunications and Information Technology Law* [online]. November 2022.

Available at: https://www.cst.gov.sa/en/RulesandSystems/bylaws/Documents/LA_005_E_Telecom_Act_Bylaws.pdf.

[13] Esquire Middle East. *UAE, Saudi Arabia ask Netflix to censor culturally sensitive content aimed at children*. 2022. Accessed: 2024-05-03. Available at: https://www.esquireme.com/culture/film-and-tv/uae-saudi-arabia-ask-netflix-to-censor-culturally-sensitive-content-aimed-at-children.

[14] Freedom House. *United Arab Emirates: Freedom on the Net 2023*. 2023. Accessed: 01-05-2024. Available at: https://freedomhouse.org/country/united-arab-emirates/freedom-net/2023.

[15] GeeksforGeeks. *TCP/IP Model*. 21. july 2023. Available at: https://www.geeksforgeeks.org/tcp-ip-model/.

[16] Giles, C. *Myanmar coup: How the military disrupted the internet*. BBC, 4. Feb 2021. Accessed: 2024-01-05. Available at: https://www.bbc.com/news/world-asia-55859665.

[17] Goldschlag, D., Reed, M. and Syverson, P. *Onion Routing for Anonymous and Private Internet Connections* [online]. January 1999. Accessed: 2024-03-10. Available at: https://www.onion-router.net/Publications/CACM-1999.pdf.

[18] Hafner, K. and Lyon, M. *Where Wizards Stay up Late: The Origins of the Internet*. 1stth ed. USA: Simon & Schuster, Inc., 1996. ISBN 0684812010.

[19] Hassine, W. B. *The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online*. Electronic Frontier Foundation, april 2016. Accessed on April 13, 2024. Available at: https://www.eff.org/files/2016/04/28/crime-of-speech.pdf.

[20] Hoang, N. P., Niaki, A. A., Dalek, J., Knockel, J., Lin, P. et al. *How Great is the Great Firewall? Measuring China's DNS Censorship*. 2021.

[21] Human Rights Watch. *UAE: Award-Winning Activist Jailed 10 Years*. 01. June 2018. Accessed: 01-05-2024. Available at: https://www.hrw.org/news/2018/06/01/uae-award-winning-activist-jailed-10-years.

[22] Human Rights Watch. *UAE: Tolerance Narrative a Sham*. 01. October 2021. Accessed: 01-05-2024. Available at: https://www.hrw.org/news/2021/10/01/uae-tolerance-narrative-sham-0.

[23] Kirchgaessner, S. Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests. *The Guardian* [online]. july 2021. Accessed on April 25, 2024. Available at: https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus.

[24] Kurose, J. F. and Ross, K. W. *Computer Networking: A Top-Down Approach*. 8th ed. Pearson, 2021.

[25] Lab, C. and Others. *URL testing lists intended for discovering website censorship*. 2014. https://github.com/citizenlab/test-lists. Available at: https://github.com/citizenlab/test-lists.

[26] Lanfranco, E. *The China Yahoo! welcome: You've got Jail!* UPI, 9. Sept 2005. Accessed: 2024-01-05. Available at: https://www.upi.com/The-China-Yahoo-welcome-Youve-got-Jail/40351126286824/.

[27] LuanRT. *Google-this* [https://github.com/LuanRT/google-this]. 2023. Accessed: 2024-04-22.

[28] Lunden, I. *Russia's game of Telegram whack-a-mole grows to 19M blocked IPs, hitting Twitch, Spotify and more.* TechCrunch, 19. Apr 2018. Accessed: 2024-01-05. Available at: https://techcrunch.com/2018/04/19/russias-game-of-telegram-whack-a-mole-grows-to-19m-blocked-ips-hitting-twitch-spotify-and-more/.

[29] Noman, H. *Internet Censorship and the Intraregional Geopolitical Conflicts in the Middle East and North Africa.* Internet Monitor, january 2019. Accessed on May 5, 2024. Available at: https://thenetmonitor.org/bulletins/internet-censorship-and-the-intraregional-geopolitical-conflicts-in-the-middle-east-and-north-africa.

[30] Open Observatory of Network Interference. *2021 LGBTIQ Website Censorship Report.* 2021. Accessed: 2024-05-03. Available at: https://ooni.org/documents/2021-lgbtiq-website-censorship-report/2021-lgbtiq-website-censorship-report-v2.pdf.

[31] Preneel, B. and Vercauteren, F. *Applied Cryptography and Network Security: 16th International Conference, ACNS 2018, Leuven, Belgium, July 2–4, 2018, Proceedings.* 1st ed. Cham: Springer Cham, june 2018. Lecture Notes in Computer Science. ISBN 978-3-319-93387-0.

[32] Quintin, C. *Snowflake Makes It Easy For Anyone to Fight Censorship* [online]. Electronic Frontier Foundation, October 2022. Accessed: 2024-03-10. Available at: https://www.eff.org/deeplinks/2022/10/snowflake-makes-it-easy-anyone-fight-censorship.

[33] Roberts, H., Zuckerman, E., York, J., Faris, R. and Palfrey, J. *2010 Circumvention Tool Usage Report* [online]. The Berkman Center for Internet & Society, october 2010. Available at: https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

[34] Shadowsocks. *What is Shadowsocks?* [online]. Accessed: 2024-03-10. Available at: https://shadowsocks.org/doc/what-is-shadowsocks.html.

[35] Staff, M. The Uncensored Library. [online]. february 2023. Accessed on April 15, 2024. Available at: https://www.minecraft.net/en-us/article/uncensored-library.

[36] Tahrir Institute for Middle East Policy. TIMEP Brief: Use of Surveillance Technology in MENA. [online]. october 2019. Accessed on April 17, 2024. Available at: https://timep.org/2019/10/23/timep-brief-use-of-surveillance-technology-in-mena/.

[37] Telecommunications and Digital Government Regulatory Authority. *Internet Guidelines.* 2023. Accessed: [03-05-2024]. Available at: https://tdra.gov.ae/en/About/tdra-sectors/information-and-digital-government/policy-and-programs-department/internet-guidelines.

[38] The National News. *Use of VPN still confusing despite recent law change*. 2016. Accessed: 2024-05-03. Available at: https://www.thenationalnews.com/uae/government/use-of-vpn-still-confusing-despite-recent-law-change-1.145308/.

[39] The Tor Project. *Censorship* [online]. 2023 [cit. 2024-05-02]. Available at: https://support.torproject.org/censorship/.

[40] VICE News. Saudi Arabia Sentenced a Man to 10 Years in Prison and 2,000 Lashes for Atheist Tweets. [online]. february 2016, [cit. 2024-05-03]. Available at: https://www.vice.com/en/article/xw3mpk/saudi-arabia-sentenced-man-to-10-years-in-prison-and-2000-lashes-for-atheist-tweets.

[41] Xynou, M., Filastò, A., International, A. and Walabuma, G. *Ethiopia: Evidence of social media blocking and internet censorship*. OONI, 14. Dec 2016. Accessed: 2024-01-05. Available at: https://ooni.org/post/ethiopia-report/.

[42] Zetter, K. Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise. *Wired* [online]. Septemper 2007, [cit. 2024-03-10]. Available at: https://www.wired.com/2007/09/rogue-nodes-turn-tor-anonymizer-into-eavesdroppers-paradise/.

Appendix A

Content of the DVD

Attached DVD has the following structure:

xposto03.pdf Thesis text

tex/ Source files for the thesis pdf

src/ Source files of the test tool