Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

School of Computer Science and Statistics

Comparing Internet Censorship Between Ireland & Iraq

Griffin Steinman

Dr. Stephen Farrell

March 5, 2025

Submitted in partial fulfilment of the requirements for the degree of

B.A.I. Computer Engineering

Declaration

I hereby declare that this Thesis is entirely my own work and that it has not been submitted as an exercise for a degree at this or any other university.

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at `http://www.tcd.ie/calendar`.

I have also completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write', located at `http://tcd-ie.libguides.com/plagiarism/ready-steady-write`.

Signed: ______________________ Date: ______________________

Abstract

A short summary of the problem investigated, the approach taken and the key findings. This should not be more that around 400 words.

The must be on a separate page.

what's the title for our title abstract one page five paragraphs area and digital twin project research questions two paragraphs how to solve them paragraph to implement and evaluate main findings one paragraphs expanding the abstract

introduction literature review design implementation evaluation conclusion

Acknowledgements

Thanks Mum!

You should acknowledge any help that you have received (for example from technical staff), or input provided by, for example, a company.

Contents

1 | Introduction

1.1 Internet Censorship and Privacy

The primary aim of this work is to identify and compare internet censorship methods between Ireland and Iraq.

1.1.1 Overt vs. Covert Censorship

Censorship can be implemented in many different ways, but there are two main categories: Overt and Covert Censorship. Overt censorship is openly implemented by governments, ISP's, or legal courts to block or restrict access to certain types of content, or specific websites. When the content a user is trying to access is blocked using overt censorship, it is made very clear to the user that it is blocked. An example of this is the 'Golden Shield Project', which is China's internet censorship project. This project blocks access to websites such as google and facebook, and the citizens of China are often aware that they websites have been blocked by the government (1).

Covert censorship is more often harder to detect. Search engine manipulation, throttling or slowness, and shadow banning are some of the primary methods of covert censorship. The goal of this type is to make censorship more difficult to detect by users, and is often disguised as technical issues.

1.1.2 Privacy

User Privacy across the internet is directly tied to censorship efforts from different regimes. Censorship often involves the state or corporate monitoring of internet users, and governments that impose censorship frequently justify it using security concerns while often violating privacy rights in the process. In countries where censorship is highly enforced, using anonymity tools to circumvent censorship can protect the right to free expression and access to information. For instance, the *Human Rights Watch* advises people in China to make use of the Tor Browser to avoid abuses by the state (2).

Based on a meta-analysis of studies related to internet privacy concerns, privacy literacy, and the adoption of privacy-protective measures, it was found that there is no strong correlation between national privacy laws and protective behaviors (3). This suggests that individuals do not rely on legal protections in their country, and more often take privacy into their own hands. It was also found that culture did not impact the use of privacy-protective behaviors in different countries.

While it may be easy to think censorship is only prevalent in non-western countries, such as China or Russia, it can also happen in democratic states. Weak privacy protections can lead to surveillance capitalism, where companies act as de facto censors by shaping information flows based on user data (4). For example, during the COVID-19 pandemic in the United States, it was recently revealed that Meta (formerly Facebook) was asked to censor certain information regarding COVID-19 (5). The United States Government and Meta actively engaged in the censorship of the people's right to free speech and expression, as humor and satire was also removed from the platform.

1.1.3 Background

This section will talk about internet censorship across the world and give a brief intro into the differences by general region

1.1.4 Global Censorship

1.2 Project Goals

The aim of this project is to ...

2 | State of the Art

2.1 Censorship Mechanisms

2.1.1 IP and DNS Blocking

Internet Protocol (IP) blocking is one of the most straightforward censorship techniques. Each device connected to the internet is assigned a unique numeric label called an IP Address, which serves as an identifier that allows data to travel across the internet to the correct destination. When a government or ISP wants to censor a specific website it can be implemented in either incoming or outgoing traffic. ISP controlled firewalls can be configured so that any outgoing or incoming requests to a selected IP address are dropped. ISPs can also adjust routing tables in their network to remove an IP address, making it unreachable for the user.

IP blocking can either be implemented at a centralized level or at an ISP level. In Ireland, IP blocking is done at an ISP level to block certain illegal websites. In Iraq, the government has complete control of all internet traffic entering the country, which allows them to implement IP blocking at a central level.

DNS blocking refers to the altering of responses from the DNS to block or filter access to certain content. This is usually done by either blocking the response, replying with an error message, or responding with an incorrect address. *DNS Mangling* is a network-level technique of on-path interceptioon where an incorrect IP address is returned in response to a DNS query to a censored destination.

DNS Cache Poisoning is an off-path technique in which a censor intercepts and replaces the legitimate response from an authoritative DNS name server with a spoofed IP address. Instead of allowing the real IP address of a site to reach the user, the censor replies faster than the real server, and that spoofed IP gets cached (perhaps by numerous recursive resolvers). Subsequent requests will then be redirected to an incorrect IP, normally leading to a warning page or an meaningless domain. In other cases, such as in Iran, the censor can merely block the response of the upstream resolver, so the accurate IP address is never transmitted.

DNS Lying is the most authoritative approach, where a censor mandates that the DNS responses provided are to be different that what would actually be returned by the DNS server (6).

2.1.2 Deep Packet Inspection (DPI)

Deep Packet Inspection consists of any kind of packet analysis beyond IP address and port number. DPI reassembles network flows to examine the application data section, and is often implemented using Middleboxes. DPI is often used for keyword identification, but this method can also determine packet size and flow timings to detect other forms of content, such as the difference between text or video packets. Despite DPI having trouble against encrypted data and being the most expensive form of censorship to implement, it is still the most powerful identification method and is widely used in practice (6).

2.1.3 Transport Layer Security (TLS)

Transport Layer Security (TLS) may be censored by mechanisms similar to those against plain HTTP, particularly through the Server Name Indication (SNI) field. In the case of TLS over TCP, the SNI value is seen in the non-encrypted ClientHello message so that censors can inspect the field and exclude connections to those domains they disapprove of. While QUIC encrypts ClientHello, the initial encryption keys are visible to network observers, and therefore it is possible, though more complex, to decrypt and observe the SNI. Governments in most nations use SNI-based filtering, occasionally leading to over-blocking when important domains or second-level domains are inadvertently ensnared.

Attempts to encrypt SNI have resulted in Encrypted SNI (ESNI), which embeds the SNI field in encrypted traffic but can induce blanket blocking by censors who blindly terminate all ESNI connections. Even more comprehensive security improvements, such as Encrypted Client Hello (ECH) for TLS 1.3, aim to encrypt the whole ClientHello rather than merely the SNI, though these enhancements are still under way in standardization and deployment.

Another way is to not include the SNI at all. However, non-SNI connections can be blocked as well, since censors can deploy policies that will drop any TLS traffic that does not have an SNI. This can again lead to overblocking, since clients that are able to handle older SSL-only configurations, or are deliberately configured not to have an SNI, can get blocked even when they are going to otherwise acceptable sites.

Censors also have the option to examine the server certificate field within the TLS handshake, which contains information on the requested domain. In TLS 1.3, however, certificates are encrypted by default, and thus such censorship is not possible. Certificate-inspecting censors must therefore employ more computation-intensive deep packet inspection techniques and can even be forced to track connections deeper into the handshake process, especially when SNI-based approaches fail or bypassed (6).

2.2 Ireland

2.2.1 Censorship in the Past

According to a report from the United States Department of State in 2011, it was found that there were no government restrictions on access to the internet or that the government actively monitored email or internet chatrooms (7).

The Irish government engages in censoring or blocking the distribution of pirated copryrighted material. In 2009, the Irish Telecom Company, EIRCOM, blocked its customers from accessing the website *The Pirate Bay*. The Pirate Bay is a Swedish website which provides links to copyrighted material. The website was hit with a lawsuit from major record labels and many ISPs around the world agreed to block access to the website as part of the settlement. However, not all Irish ISPs complied. The cable TV operator UPC announced that it would not comply (8).

In alignment with international agreements, the Irish Government blocks access to websites that contain illegal content, such as Child Sexual Abuse Material (CSAM). The government has setup a hotline that allows citizens to anonymously report websites that they suspect contain illegal content, called hotline.ie (9).

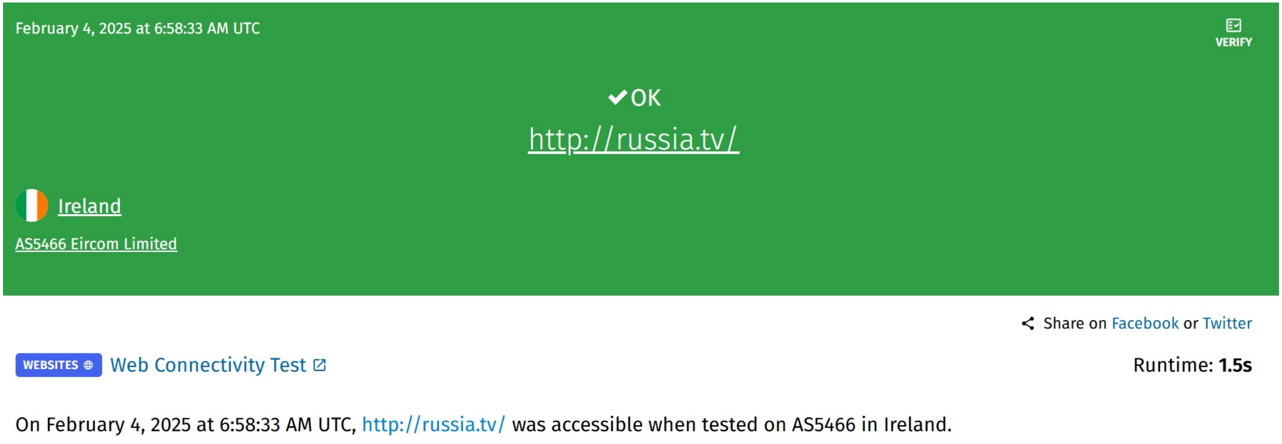
In contrast to other EU countries, Ireland does not have a broad government-mandated filtering system. They instead have the power through the Irish courts to mandate Irish ISPs to block certain websites. In addition, Irish ISPs may voluntarily enforce content filtering and website blocking in alignment with Irish content law.

Up until 2014, Ireland and other EU countries followed data retention laws, which required ISPs to store metadata for law enforcement purposes. In 2014, the European Court of Justice struck down the directive, which led to a change in this law in Ireland (10). After this change, Ireland enacted the *Communications (Retention of Data)(Amendment) Act 2022* (11). This legislation allows for the general and indiscriminate retention of communications traffic and location data on the grounds of national security, where approved by a judge.

2.2.2 Current Censorship

As a whole, Ireland's censorship efforts are limited and specific. The government and ISPs target mainly illegal and pirated content. Some specific websites that have been blocked include 1337x, Eztv, BMovies, GoMovies, Putlocker, Rarbg, WatchFree, and Yts (12). However, piracy websites are still widely accessible in Ireland.

It seems that Ireland has also rolled back blocks on some websites, such as Russian News outlets. Previously, the domain russia.tv, was blocked in Ireland. But as of 2025, it is able to be partially accessed. Based on data from the OONI project, there is evidence of TCP/IP blocking of this domain in Ireland. Based on the findings from OONI, this domain is able to be accessed when EIRCOM's root DNS server (AS5466, IP: 86.47.80.38) is used, but is blocked when accessed through Cloudflare's DNS server (AS14593, IP: 172.69.193.80).



February 4, 2025 at 6:58:33 AM UTC

✔ OK

http://russia.tv/

Ireland

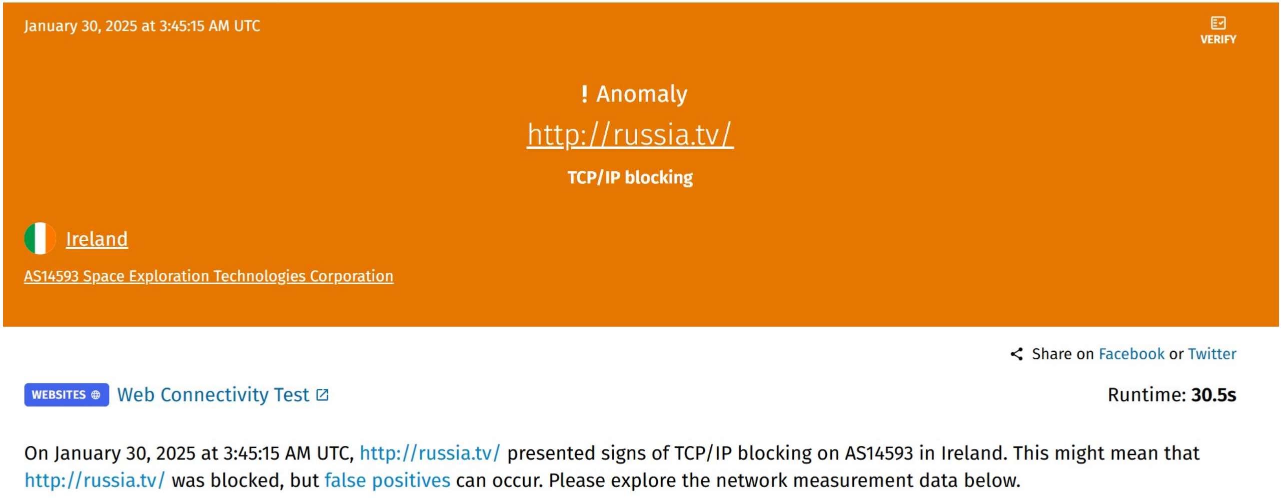
AS5466 Eircom Limited

Web Connectivity Test

Runtime: **1.5s**

On February 4, 2025 at 6:58:33 AM UTC, http://russia.tv/ was accessible when tested on AS5466 in Ireland.

Figure 1.1, EIRCOM DNS test for Russia.tv on OONI probe



January 30, 2025 at 3:45:15 AM UTC

! Anomaly

http://russia.tv/

TCP/IP blocking

Ireland

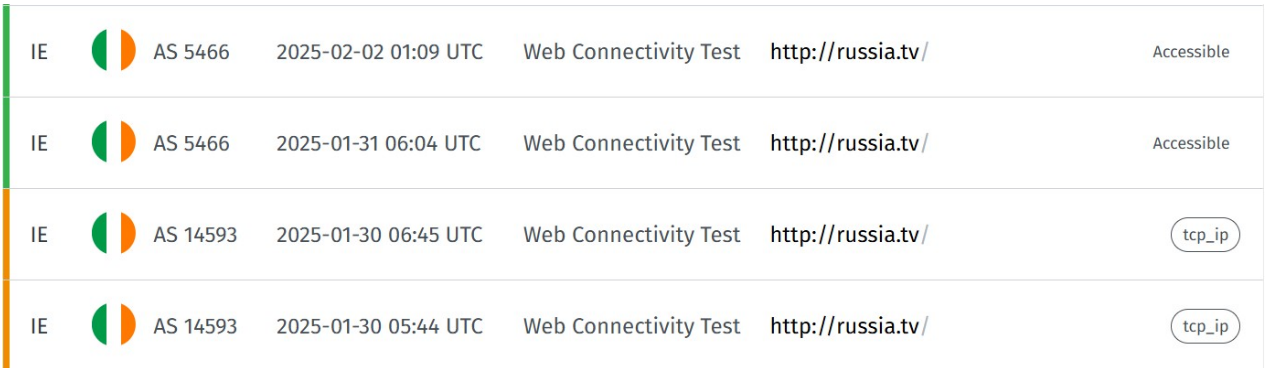
AS14593 Space Exploration Technologies Corporation

Web Connectivity Test

Runtime: **30.5s**

On January 30, 2025 at 3:45:15 AM UTC, http://russia.tv/ presented signs of TCP/IP blocking on AS14593 in Ireland. This might mean that http://russia.tv/ was blocked, but false positives can occur. Please explore the network measurement data below.

Figure 1.2, CloudFlare DNS test for Russia.tv on OONI probe



IE	🇮🇪	AS 5466	2025-02-02 01:09 UTC	Web Connectivity Test	http://russia.tv/	Accessible
IE	🇮🇪	AS 5466	2025-01-31 06:04 UTC	Web Connectivity Test	http://russia.tv/	Accessible
IE	🇮🇪	AS 14593	2025-01-30 06:45 UTC	Web Connectivity Test	http://russia.tv/	tcp_ip
IE	🇮🇪	AS 14593	2025-01-30 05:44 UTC	Web Connectivity Test	http://russia.tv/	tcp_ip

Figure 1.3, Russia.tv domain search on OONI

2.3 Iraq

2.3.1 Censorship in the Past

Iraqi internet censorship has been radically reshaped over the years. Under Saddam Hussein's regime, only a very few Iraqis had access to the internet, leading to the state controlling all parts of the internet within the country. Post-2003, with more people accessing the internet and the country struggling with internal conflict and the threat of radicalization, censorship was decentralized and usually carried out with little transparency and regionally differentiated. While the constitution and laws of Iraq recognize free expression, actual enforcement is usually slow whenever security is at stake. As the internet began to take a greater role, both as a platform for political discourse and a bulletin for extremist messaging, the censorship and intrusions of the government increased correspondingly. Generally speaking, the policy of controlling the internet in Iraq has mirrored the broader political and security situation, tightening whenever Iraq is unstable (13).

2.3.2 Current Censorship

In a 2023 report from the United States Department of State, it was found that the government of Iraq restricted or disrupted access to the internet and censored online content, in conjunction with monitoring private online communications without appropriate legal authority (14). The Iraqi government and the Kurdistan Regional Government (KRG) consistently engage in implementing internet outages during protests or times of unrest (13). In 2023, Iraqi officials implemented 66 internet outages, more than any other country in the world. Most, if not all, internet infrastructure is controlled and managed by the government.

After the fall off Saddam Hussein's Regime in 2003, the internet became much more accessible and the information landscape was opened. However, the current-day Iraqi government occasionally blocks websites, and more often social media websites in order to maintain stability and control during times of unrest (13). During anti-government protests in 2019, the Iraqi government blocked access to Facebook, X (Formerly Twitter), WhatsApp, and Instagram. In protests in 2018, some users in Iraq found that they were unable to use VPNs to circumvent website blocking. The government routinely engages in the censoring and blocking of Pornography and Gambling websites on the guise of protecting their citizens from harmful content.

2.4 Censorship Circumvention Tools

2.4.1 The Tor Browser

The Tor Project Background

The Tor Browser is built on a concept called *Onion Routing*, which was developed in the 1990s by researchers at the United States Naval Research Laboratory. The goal of the project was to create a communication method where data is wrapped in multiple layers of encryption so that no point in the network could reveal the sender and receiver (15). Originally, the United States Government used the Tor network to access potentially illegal websites anonymously, and transmit data. But because only the US Government was using it at the time, it was easy to tell who the single anonymous user was, when viewing the site logs. It would also have made Tor a target for bad actors, as they could be sure that all data being sent over the network was related to the United States Government/Military.

To stop this from happening, the US Government released Tor to the public in the early 2000s, and later it became the Tor Project, a non-profit organization funded by the United States that develops and maintains the Tor software.

Technical & Circumvention Information

Internet traffic sent over the Tor network is encapsulated in multiple layers of encryption. Think of your data as a letter that is placed inside several envelopes. Each node in the network removes one envelope, revealing only the information necessary to pass the message along to the next node. To do this, the Tor browsers sends your data through at least three nodes, and the pathway of these nodes are randomly constructed and reconstructed during your session (16).

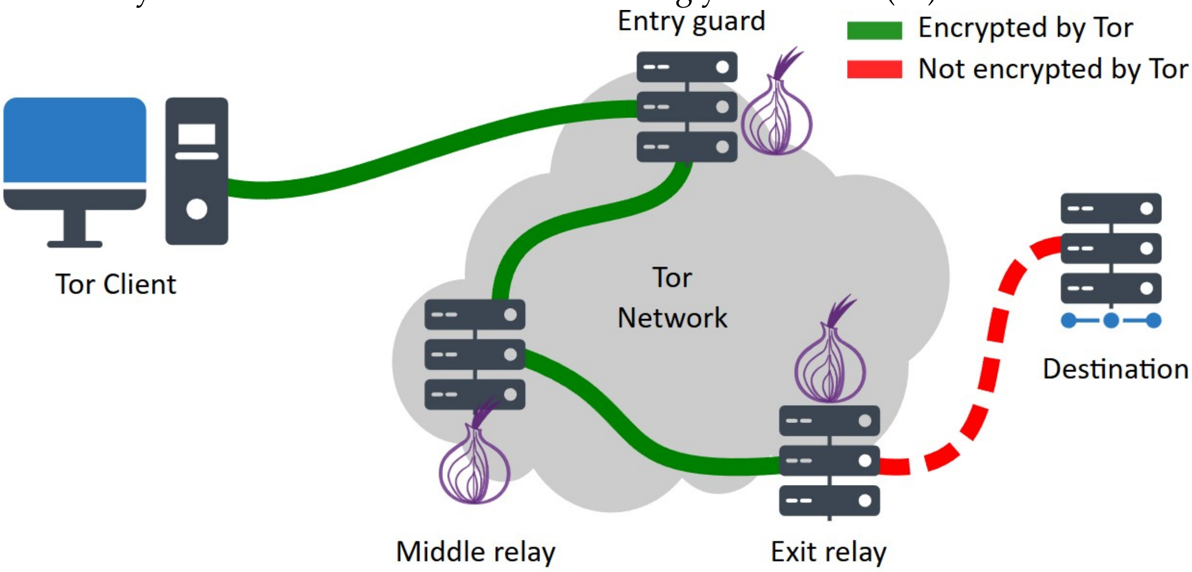


Figure 1.4, How the Tor Network Works

Tor is a great tool to combat censorship. Tor's distributed architecture of nodes makes it resilient against localized censorship efforts. In countries where the Tor network is blocked, users are able to use "Bridges", which are Tor nodes that are not listed publicly. Using a bridge address allows for the user to connect to the network covertly (17). Users can also avail of "Pluggable transports", which transforms Tor traffic to look like regular network traffic. This method can help circumvent censorship in regions that use *Deep Packet Inspection* (DPI) and other forms of advanced internet censorship (18).

2.4.2 VPNs

Virtual Private Networks (VPNs) broadly speaking provide an end-to-end encrypted connection between your device and a VPN server. This method hides your IP address and grants the user anonymity while browsing over the network. This allows users to bypass censorship by connecting to servers outside of their location while masking your IP address (19).

3 | Methodology

3.1 Introduction

3.2 The OONI Probe

3.2.1 Background of OONI

The Open Observatory of Network Interference (OONI) project was started in 2012 as a non-profit open-source software project aimed at identifying and documenting internet censorship around the world (20). The OONI organization openly publishes measurements and provides a public archive on network interference from across the world.

3.2.2 Data-Collection

Web Connectivity Test

The Web Connectivity test determines if, and how, access to a specific website may be blocked. To do this, OONI Probe performs several checks from the network where the test is run and compares the results with measurements collected from a control network where censorship is not expected. If the measurements differ significantly, censorship techniques are likely used on the local network. This test is designed to perform the four different actions: Resolver Identification, DNS Lookup, TCP Connect, HTTP GET Request.

The Web Connectivity test begins by identifying the DNS resolver in use on the network. It achieves this by sending DNS queries to special domains, which disclose the resolver's IP address. Once the resolver is identified, the test performs DNS lookups to determine which IP addresses (and potentially other host names) are mapped to the tested domain. After collecting that information, the test attempts to establish a TCP session on port 80 or port 443, depending on whether the URL uses HTTP or HTTPS. Finally, once the TCP connection is successful, the test sends an HTTP GET request to the server hosting the website; under normal circumstances, the server will respond with the requested webpage content (21).

Circumvention Test

The circumvention test is used to check weather Psiphon, Tor, or RiseupVPN are blocked on a given network. These are tools used to circumvent censorship by utilizing VPN, SSH, and HTTP proxy technologies.

The Psiphon VPN serves as a tunnel that enables you to circumvent censorship by connected you to an uncensored portion of the internet (22). The Psiphon test first uses Psiphon's own code to establish a Psiphon tunnel. After the tunnel is created, the test attempts to load a webpage to see if Psiphon actually works for accessing the internet. If the tunnel is successfully set up and the webpage loads, Psiphon is functioning on the tested network and can bypass censorship. If the tunnel is established but the webpage does not load, Psiphon is blocked in some way, preventing access to online resources. Finally, if the test cannot even create the Psiphon tunnel, it indicates that Psiphon is completely blocked on that network (23).

The Tor Test (24) automatically checks whether Tor is accessible in a given network by examining the reachability of core components such as Tor directory authorities, OR ports, and obfs4 bridges. It first attempts to retrieve the Tor consensus from directory authorities, then tries to connect to OR ports (including those of directory authorities) via a TLS handshake, and finally tests obfs4 bridges through an obfuscated handshake. If all of these steps succeed, Tor is likely usable in the tested network (unless it is blocked in ways not covered by the test). If any step fails, Tor may be blocked and therefore unavailable on that network (25).

The RiseUpVPN test evaluates if the bootstrap servers used during the self-configuration of the VPN clients can be reached. The test also checks if RiseupVPN's gateways can be reached on different ports and transports (26). This test was contributed by the LEAP collective (27).

Instant Messaging Test

The Instant Messaging test is used to check weather WhatsApp, Facebook Messenger, Telegram, and Signal are blocked on a given network.

The Whatsapp test attempts to determine is there is any interference or blockage of it's App or Web Interface. To to this, the OONI probe attempts to perform an HTTP GET request TCP Connection, and DNS lookup to WhatsApp's enpoints. These include the endpoints used by the WhatsApp mobile app, the registration service, and the web interface (28). To conduct these tests, the OONI probe attempts to open TCP sockets towards WhatsApp endpoints on Ports 443 and 5222. If these connections fail or are rejected, it is seen as an indicator of blockage at the TCP level. The probe then verifies if the DNS resolution returned a valid IP address that is registered to WhatsApp. If the resolved IP address does not belong to WhatsApp, it can indicate DNS level blocking or tampering. And to check if the WhatsApp registration service is working correctly, an HTTP GET request is sent to the URL `https://v.whatsapp.net/v2/register`. The request is considered successful if there is no DNS, TCP connect, TLS (Transport Layer Security), or I/O error (29).

The Facebook Messenger Test is used to examine the reachability of the service within a tested network. The OONI probe begins by attempting to perform a TCP connect and DNS lookup to facebook's endpoints (30). The test verifies if Facebook Messenger endpoints resolve to consistently known IPs and if it's possible to establish TCP connections to them on port 443. For each endpoint tested, an A lookup for the domain name is performed and it is considered consistent if the IP is inside of a netblock linked to the *Facebook Authonomous System Number* (AS32934) (31).

The Telegram Test is used to examine the reachability of Telegram's app and web version within a tested network. The telegram access points (DCs) are those used by the desktop client, and they have six unique IP addresses. The test establishes a TCP connection to all of the access point IP addresses and attempts to send a POST HTTP request to each of them. If all TCP connections on ports 80 and 443 fail, Telegram is considered to be blocked at the TCP level. Otherwise, Telegram is considered to be working as intended (32).

The Signal Test is used to measure the reachability of the Signal messaging app within a tested network. The test checks if it is possible to establish a TLS connection and send an HTTP GET request to the Signal server endpoints (33). A DNS query to `uptime.signal.org` is also performed to check if the backend servers are down (34).

Middlebox Test

A Middlebox is a computer networking device that transforms, filters, and manipulates traffic for purposes other than packet forwarding. These include network address translators, load balancers, and deep packet inspection (DPI) devices. The presence of Middleboxes can lead to evidence of censorship and/or traffic manipulation, but it can also be indicative of a less malicious intent, such as network caching.

The OONI Middlebox test consists of two main operations: HTTP Header Field Manipulation and HTTP Invalid Request Line. The HTTP header field manipulation test emulates an HTTP request towards a server, but sends HTTP headers that have variations in capitalization. These requests are sent to a backend control server which send back any data it receives, and if these requests return exactly as we sent them, it is assumed there is no middlebox present. If the alterations of the headers come back normalized, it can be assumed that there was packet manipulation of some kind, leading to the confirmation of presence of Middleboxes It is worthy to note that false negatives can happen in this test, as some ISPs use highly sophisticated software that can disguise the presence of Middleboxes (35).

The HTTP Invalid request line test sends an invalid HTTP request to an echo service listening on the standard HTTP port, rather than a valid one. If the request is returned to the user exactly as it was sent, it can be concluded that there is no evidence of the presence of a Middlebox. However, it is possible that this invalid request can be intercepted by a Middlebox that triggers an error that is sent back to the probe. This is evidence that there is a Middlebox present in the network. It is worthy to note that false negatives are possible as some ISPs use highly sophisticated software that is designed not to trigger such errors (36).

3.3 Challenges & Limitations

4 | Results and Discussion

5 | Security Privacy

6 | Conclusions

Bibliography

[1] &xBB; The Great Firewall of China: Background Torfox — cs.stanford.edu. https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html, . [Accessed 18-02-2025].

[2] Eric Jardine. Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. https://journals.sagepub.com/doi/full/10.1177/1461444817733134, 2017. [Accessed 29-01-2025].

[3] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1): 26–53, 2017.

[4] Paul M Schwartz. Internet privacy and the state. *Conn. L. Rev.*, 32:815, 1999.

[5] Zuckerberg says the White House pressured Facebook to 'censor' some COVID-19 content during the pandemic — pbs.org. https://www.pbs.org/newshour/politics/zuckerberg-says-the-white-house-pressured-facebook-to-censor-some-covid-19-conte
[Accessed 01-02-2025].

[6] Mallory Knodel. RFC 9505: A Survey of Worldwide Censorship Techniques — rfc-editor.org. https:

//www.rfc-editor.org/rfc/rfc9505.html#name-technical-identification. [Accessed 04-03-2025].

[7] Technical Difficulties — 2009-2017.state.gov. https://2009-2017.state.gov/j/drl/rls/hrrpt/2011humanrightsreport/index.htm?dlid=186364#wrapper,. [Accessed 04-02-2025].

[8] Eircom to block internet access to Pirate Bay as other firms refuse — irishtimes.com. https://www.irishtimes.com/news/eircom-to-block-internet-access-to-pirate-bay-as-other-firms-refuse-1.722015,. [Accessed 04-02-2025].

[9] About &x2013; Hotline — hotline.ie. https://hotline.ie/about/. [Accessed 04-02-2025].

[10] Practical Law IPIT. ECJ declares Data Retention Directive invalid. https://uk.practicallaw.thomsonreuters.com/5-564-2768?contextData=(sc.Default)&transitionType=Default&firstPage=true#:~:text=The%20ECJ%20has%20ruled%20that%20the%20Data%20Retention,%281%29%20of%20the%20EU%20Charter%20of%20Fundamental%20Rights. [Accessed 04-02-2025].

[11] Data retention law to be brought into effect — irishlegal.com. https://www.irishlegal.com/articles/data-retention-law-to-be-brought-into-effect,. [Accessed 04-02-2025].

[12] John Kennedy. Movie industry victory as eight piracy sites blocked in Ireland — siliconrepublic.com. https://www.siliconrepublic.com/enterprise/movie-piracy-ireland-legal-action-isps. [Accessed 04-02-2025].

[13] Iraq: Freedom on the Net 2024 Country Report | Freedom House — freedomhouse.org. https://freedomhouse.org/country/iraq/freedom-net/2024#footnote1_

d8PVkoU73PsQqsV4AnRY-VMTJWntGAP2vv547rIRUA_vIch24iLQyPS. [Accessed 08-02-2025].

[14] Technical Difficulties — state.gov. https://www.state.gov/wp-content/uploads/2024/03/528267_IRAQ-2023-HUMAN-RIGHTS-REPORT.pdf. [Accessed 08-02-2025].

[15] The Tor Project | Privacy & Freedom Online — torproject.org. https://www.torproject.org/about/history/,. [Accessed 07-02-2025].

[16] Roger Dingledine, Nick Mathewson, Paul F Syverson, et al. Tor: The second-generation onion router. In *USENIX security symposium*, volume 4, pages 303–320, 2004.

[17] BRIDGES | Tor Project | Tor Browser Manual — torproject.github.io. https://torproject.github.io/manual/bridges/,. [Accessed 07-02-2025].

[18] CIRCUMVENTION | Tor Project | Tor Browser Manual — torproject.github.io. https://torproject.github.io/manual/circumvention/,. [Accessed 07-02-2025].

[19] How does a VPN work? — tomsguide.com. https://www.tomsguide.com/features/how-does-a-vpn-work. [Accessed 05-03-2025].

[20] About — ooni.org. https://ooni.org/about/,. [Accessed 25-01-2025].

[21] Web Connectivity — ooni.org. https://ooni.org/nettest/web-connectivity/,. [Accessed 02-03-2025].

[22] Psiphon — ooni.org. https://ooni.org/nettest/psiphon/,. [Accessed 02-03-2025].

[23] spec/nettests/ts-015-psiphon.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-015-psiphon.md. [Accessed 02-03-2025].

[24] Tor — ooni.org. https://ooni.org/nettest/tor/, . [Accessed 02-03-2025].

[25] spec/nettests/ts-023-tor.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-023-tor.md, . [Accessed 02-03-2025].

[26] spec/nettests/ts-026-riseupvpn.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-026-riseupvpn.md. [Accessed 02-03-2025].

[27] LEAP Encryption Access Project — leap.se. https://leap.se/. [Accessed 02-03-2025].

[28] WhatsApp test — ooni.org. https://ooni.org/nettest/whatsapp/, . [Accessed 02-03-2025].

[29] spec/nettests/ts-018-whatsapp.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-018-whatsapp.md. [Accessed 02-03-2025].

[30] Facebook Messenger test — ooni.org. https://ooni.org/nettest/facebook-messenger/, . [Accessed 02-03-2025].

[31] spec/nettests/ts-019-facebook-messenger.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-019-facebook-messenger.md. [Accessed 02-03-2025].

[32] spec/nettests/ts-020-telegram.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-020-telegram.md. [Accessed 02-03-2025].

[33] Signal test — ooni.org. https://ooni.org/nettest/signal, . [Accessed 02-03-2025].

[34] spec/nettests/ts-029-signal.md at master · ooni/spec — github.com. `https://github.com/ooni/spec/blob/master/nettests/ts-029-signal.md`. [Accessed 02-03-2025].

[35] HTTP Header Field Manipulation — ooni.org. `https://ooni.org/nettest/http-header-field-manipulation/`, . [Accessed 02-03-2025].

[36] HTTP Invalid Request Line — ooni.org. `https://ooni.org/nettest/http-invalid-request-line/`, . [Accessed 02-03-2025].

A1 | Appendix

You may use appendices to include relevant background information, such as calibration certificates, derivations of key equations or presentation of a particular data reduction method. You should not use the appendices to dump large amounts of additional results or data which are not properly discussed. If these results are really relevant, then they should appear in the main body of the report.

A1.1 Appendix numbering

Appendices are numbered sequentially, A1, A2, A3... The sections, figures and tables within appendices are numbered in the same way as in the main text. For example, the first figure in Appendix A1 would be Figure A1.1. Equations continue the numbering from the main text.