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

SCHOOL OF COMPUTER SCIENCE AND STATISTICS

COMPARING INTERNET CENSORSHIP IN IRELAND VS. ISRAEL

CHRIS CASEY

DR. STEPHEN FARRELL

MARCH 6, 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 Research Motivation

Since its inception, the Internet has served a vast user base that wishes to communicate with one another and spread information. By design, the Internet is a platform that should provide unfiltered content to users. In many cases this content may otherwise be inaccessible by traditional media outlets such as radio or TV. Originally designed to aid government researchers share information, its open and transparent foundation has since changed. Across the globe, governments and other entities are censoring the internet by network manipulation, legislative pressure or otherwise. This is a global threat to fundamental internet user rights and should be treated as such. It is for these reasons that this area ought to be investigated more thoroughly.

Although censorship of certain content (CSAM, pirated entertainment) is widely considered appropriate, normalising this has far reaching consequences on user privacy and free speech. The importance of establishing a quantitative approach to measuring internet censorship cannot be overstated as users are unaware of invisible content in most cases. As a result, the state has a large influence over what ideas can propagate within its borders. Various open-source and community led projects aimed at addressing this issue. Notable examples include the Tor project, OONI, Tails OS and others. However, it is coming to light that this technology is becoming deprecated. In 2022, German police were able to make an arrest after de anonymising

Tor traffic using timing analysis. [1]. This highlights the large dichotomy between what users believe governments are capable of and reality.

For the above reasons, the increasingly pervasive censorship done by governments and corporations around the world is concerning.

1.1.1 Practical Implications

1.1.2 Awareness & Transparency

1.1.3 Problem Statement

1.2 Background

1.2.1 Global Internet Censorship

Experts suggest that censorship on the internet is increasing at an alarming rate. “The majority of countries that censor content do so across all four themes, although the depth of the filtering varies. The study confirms that 40 percent of these 2,046 websites can only be reached by an encrypted connection (denoted by the "HTTPS" prefix on a web page, a voluntary upgrade from "HTTP").” [4] It is also clear that more and more countries are viewing this as a necessary solution to the unique problems they have. Whether this is appropriate or not, it is happening, and users should be aware of this.

Governments have a vested interest in maintaining control over telecommunications industries and public internet use. Whether protecting state secrets, preventing cyber crime piracy or acts of terrorism, insulating from perceived negative influence, aiding in the creation of propaganda or otherwise; a large majority of governments choose to exercise inordinate control over the information available to its public.

As more governments and entities began to engage in this, it became increasingly important to hold them accountable. As a result, the ‘Enemies of the Internet’ list was

devised. It contains the governments and entities that actively engage in the repression of online freedoms, in the form of censorship and surveillance. As of 2014, there were 19 governments that fit this criterion but by now this number has likely increased. [5] Traditionally, censorship involved monitoring a handful of media and cutting undesirable content, potentially replacing this with a message more in line with the agenda and norms of the locale. However, with the advent of the internet, this distribution of information became decentralised and thus allowed for more expression and freedom in the content consumed by a user. As a result, censorship has become more difficult to conduct, but potentially easier to get away with. Nowadays, governments leverage points of control, network-level filtering and many other techniques to block undesirable content.

1.2.2 User Privacy

1.2.3 Censorship vs. Surveillance

1.2.4 Legislation

Governments can enforce censorship directly through ISPs, tech companies and social media platforms by creating new legislation or simply mandating content be removed. This is used to deplatform individuals and movements during periods of unrest. This is also done in app stores, shutting down entire platforms that are deemed problematic.

1.3 Project Scope

1.3.1 Project Objectives

Below is an outline of the objectives completed during the duration of the project:

- To conduct a literature review to identify and evaluate existing censorship

measurement tools with a focus on OONI.

- To understand how and why censorship is conducted in these countries and how it can be measured.

- To collect data using OONI and other sources for both countries. Use historical datasets as well as rerunning tools for up to date data.

- To conduct a comparative analysis between the two countries' datasets.

- To consider ethical implications of the research early so as to ensure compliance.

- To set up VMs in Israel in order to establish ground truth.

- To present high-level findings about the two countries approach to censoring the experience of their internet users, make conclusions about the attitudes and values present in each locale based on the data collected.

- To understand more about the unique situations of both Ireland and Israel, and how censorship is used by the state considering this.

1.3.2 Core Research Questions

1.3.3 Data Collection & Analysis Tools

1.4 Ethical Considerations

1.4.1 GDPR and Data Privacy

1.4.2 Potential Risks

2 Literature Review

2.1 Introduction

Write an introduction outlining the reasons for lit review... Briefly elude to some high level differences between Ireland and Israel.

The purpose of this literature review is to survey and consider published work regarding internet censorship globally, with a particular focus on that of Ireland and Israel. Legislation, important events and other notable areas will be discussed and compared in order to gain a greater understanding the differences between internet censorship experienced in Israel and Ireland. Internet censorship is constantly evolving as it competes with privacy based tools in an 'Arms race' of sorts. This makes researching and understanding how censors achieve their purpose of particular importance. To properly understand the current situations faced by both Israeli and Irish citizens using the internet, a broad analysis of existing literature and ongoing research had to be considered. This section lays the groundwork for the thesis, detailing how both countries approach to internet censorship has evolved over the years.

Internet usage is rising year on year globally as more users are free to surf the web. Our World in Data, an independent organisation that tracks internet usage statistics suggests that as of 2023, 67.4% of the world was connected to the internet. This is a staggering number of individuals that is only set to increase. With more people relying on the internet for their livelihood, communication or otherwise, internet

censorship is becoming a more pressing matter. It has also been noted previously that, based on OONI data, censorship is rising globally. This growth highlights the need for transparency and regulation surrounding user rights and privacy.

As previously mentioned, a common misconception about the internet is that it's content is not manipulated. Another misconception held by many is that internet censorship occurs in few countries. This is also false, with censors increasing their restrictions continuously. According to Bischoff in his online article mapping internet censorship and geographies "This year we saw nearly 60 countries increase their internet censorship in some way, compared to 50 from last year's study."(1) This is a troubling reality as internet content is increasingly being censored not just in authoritarian countries but by democratic states.

2.2 Literature Review Methodology

In conducting this literature review, sources from a variety of mediums were used. Research was conducted primarily using the internet, focusing on academic papers and peer reviewed literature. Other sources like Trinity College Library, online articles and journals were also considered and sources were cross checked with relevant authorities. Information regarding country-specific legislation was taken from the official state-run website of those countries. Sources deemed potentially unreliable were placed under a higher level of scrutiny. It is worth mentioning that researching this area can be difficult as state level censorship is typically clandestine and overt.

2.3 Findings of the Literature Review

2.3.1 Ireland Historically (Griff)

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 (6). 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 (7). 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 (8). 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 (9). After this change, Ireland enacted the Communications (Retention of Data)(Amendment) Act 2022 (10). 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.

2.3.2 Ireland Today (Griff)

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 (11). 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).

2.3.3 Israel Historically

Since the early 2000s internet access has become increasingly more available in Israel. Things have changed since then. Israeli internet censorship has developed over the years to cover a variety of security and political concerns. Israel entrusts its internet censorship operation to the Israeli Military Censor. This group is primarily responsible for the protection of Israeli security interests, and headed by Israel's minister of defense, currently Israel Katz.

According to the Internet Monitor, a data analysis and collection tool used to monitor internet access and online content controls states about Israel's freedom of press: "Modern censorship of information operates through voluntary agreements between the military and the Israeli Committee of Daily Newspaper Editors. Even though these agreements lack full consent from media in the country, all media organizations operating in Israel must abide by the censor's decisions." (2)

2.3.4 Israel Today

Reporters Without Borders, responsible for the World Press Freedom Index have ranked Israel as 101st in the world as of 2024. This ranking is based on the level of freedom enjoyed by journalists and media. "Press freedom is defined as the ability of journalists as individuals and collectives to select, produce, and disseminate news in the public interest independent of political, economic, legal, and social interference

and in the absence of threats to their physical and mental safety." (3)

"In June 2017, after a few years of no blocking, the Palestinian Authority ordered ISPs to block 12 news websites affiliated with the rival Islamist group Hamas which controls the Gaza Strip, websites affiliated with dismissed Fatah leader Mohammed Dahlan, and 10 news websites that provide news and views on Palestinian politics."(4)

2.4 Analysis: Ireland vs Israel

2.4.1 Similarities

2.4.2 Differences

2.5 Conclusions

3 State of the Art

3.1 Introduction

In order to quantify internet censorship conducted across the globe it is important to understand the different methods used by censors to achieve their aims. Censors engage in a range of steps at various layers of the OSI model in order to either stop the publication of information or make it more difficult for the user to attain. Ultimately, a censors choice of how they detect and interrupt the flow of undesirable information is based on a number of factors such as cost, scalability, and whether the censor wishes to be transparent.

3.1.1 Overt vs. Covert Censorship

ICLab, a censorship measurement tool very similar to OONI, released a paper in 2020 describing the need for their contribution. In this paper, the author highlights an important distinction between covert and overt censorship: 'In overt censorship, the censor sends the user a 'block page' instead of the material that was censored. In covert censorship, the censor causes a network error that could have occurred for other reasons, and thus avoids informing the user that the material was censored." (5) This is a concerning capability as it alludes to the potential for censorship to go unchecked.

3.2 Censorship Techniques and Mechanisms

3.2.1 Points of Control

Key control points are nodes in the Internet's architecture that connect a large user base to the wider network, making them attractive targets for censorship enforcement. Governments and institutions use leverage these points in order to restrict user access. Some points of control include ISPs, IXPs, VPNs, national gateways and local networks. Institutions will typically use a combination of legislative pressure, technological and economic means to snuff out content. ISPs and VPNs face significant and constant pressure from legal arms to expose user data and manipulate the content available to a user.

These locations in the internet infrastructure are invaluable to those wishing to conduct internet censorship. Though security considerations such as HTTPS and TLS can protect users from MITM attacks, points of control are a physical reality to be contended with. At some point, user packets will route through state owned infrastructure and thus could be subject to inspection. In this way, points of control are a key consideration for all internet users.

3.3 Network-Level Filtering

3.3.1 IP and DNS Blocking (GRIFF)

Communicating on the internet typically looks something like that seen in the figure below. A publisher's website is associated with a domain, e.g www.example.com. A user who wishes to navigate to this site must first send a DNS request to the DNS server to resolve the IP address of the web server. Upon receiving the IP address, the user can then send a HTML get request in order to access the page. How the Domain Name System and Internet Protocol work together to navigate users through a vast infrastructure can thus be simplified into these two transactions. If the censor has

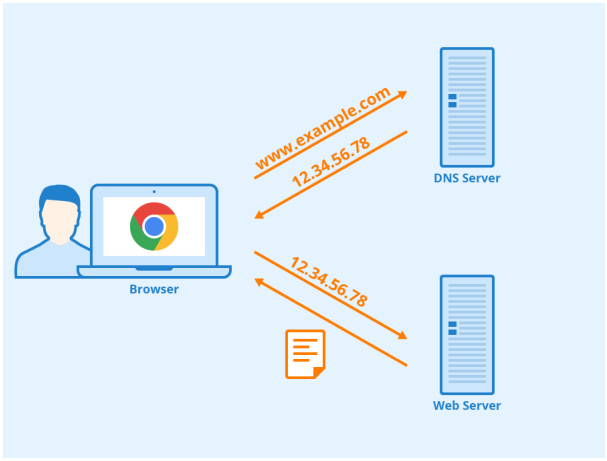

Figure 3.1: DNS Requests and IP

access to this DNS server, these flows can be manipulated in a number of ways to disrupt communication.

Originally implemented to stop email spam, 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. The primary motivation for the Irish government in doing this is to crack down on piracy.

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. Broadly, DNS manipulation involves redirecting users by returning incorrect IP addresses. This is used to route users to controlled versions of websites or block access entirely and thus is covert in nature.

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 (**?**).

3.3.2 Transport Layer Security (TLS) (Griff)

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 (**?**).

3.3.3 MITM Attacks

A man-in-the-middle attack involves intercepting encrypted packets (potentially at a point of control), to potentially alter or block internet traffic. Governments have been seen to pressure VPNs into routing traffic through designated MITM servers. Inevitably this allows for selective content manipulation, deep packet inspection and surveillance. MITM attacks are particularly concerning due to their covert and intrusive nature.

3.4 Application Layer Filtering

Beyond IP and DNS manipulation, censors can examine the contents within packets to make decisions regarding their accessibility. This refers to the concept of

application layer filtering or blocking; monitoring a communication channel and detecting offensive keywords. This is seen in more cultivated censorship models. Upon detecting a sensitive keyword, the communication will be disrupted, perhaps by sending TCP reset packets to both sides.

3.4.1 Keyword Filtering

Keyword filtering involves

3.4.2 Deep Packet Inspection

This is at the application layer, right? Deep packet inspection involves looking into payloads and data within packets, beyond its header. It is a sophisticated technique usually performed as part of a firewall defense and involves making real time decisions about the nature of each packet. DPI functions at the application level and can be used to identify both the sender and recipient of the packet by examining its payload. Compared to regular packet inspection which is only concerned with basic header information, it is considerably more costly.

Deep packet inspection is used in specific cases where a higher level of audit is required. This includes packets carrying malware, content that has been blocked and intrusion efforts. DPI is usually performed by network middle boxes, devices that lie between end points. One of the these middle boxes is BlindBox, a system that accommodates DPI while preserving privacy and encryption. The creators of this system highlight the potential risks to user privacy with other black boxes. "To enable middlebox processing, some currently deployed middlebox systems support HTTPS in an insecure way: they mount a man-in-the-middle attack on SSL and decrypt the traffic at the middlebox." (6)

Though its deployment is limited, DPI represents a significant risk to user privacy. Not all middle box providers offer the protections and guarantees that BlindBox offer. Forecasts for the market show a troubling trend, with no guarantees of user

privacy. "Global deep packet inspection (DPI) market size was anticipated to be worth USD 10.63 billion in 2024 and is expected to reach USD 79.26 billion by 2033 at a CAGR of 25% during the forecast period." (7)

3.5 Legislative and Economic Pressure

Governments can enforce censorship directly through ISPs, tech companies and social media platforms by creating new legislation or simply mandating content be removed. This is used to de-platform individuals and movements during periods of unrest. This is also done in app stores, shutting down entire platforms that are deemed problematic.

3.5.1 Search Engine Manipulation

Altering the ranking of websites or totally removing them from search results. This is done by companies like Google to incentivise paying for exposure, to censor content for compliance reasons, improve user experience and more.

3.6 Surveillance and Deanonymisation

In discussing internet user rights and how censorship occurs, it is important to mention anonymity and user privacy. DRI, a non-profit that challenges the Irish government on data retention issues is an independent, non-profit organization. They state on their website, that users have "a right to digital privacy [&] data security." (8) Individuals' freedom to access information and be anonymous are inherently linked, however very separate issues. Though censors may actively engage in deanonymisation efforts, potentially using methods described below, this research is focused on internet censorship. Hence, deanonymisation and surveillance will only be touched on briefly.

Efforts to identify users based on their traffic range from trivial to extremely complex

based upon the protections employed by the user. Operational security, the collection of measures taken by an individual to protect their online anonymity, is often overlooked by casual internet users. Projects like Tor, Tails OS (an amnesiac Linux distribution), and Briar (secure off-grid communication) as well as VPNs aim to protect users' identity. However, these methods are not fool proof.

VPN providers are subject to the scrutiny of the jurisdiction within which it operates. NordVPN, a very popular VPN provider based in Amserdam has said on record "We will comply with lawful requests as long as they are delivered according to all the laws and regulations." This reflects the reality of VPN services as provided by corporations. VPNs in this sense can be described as a double edged sword. In most cases they are very helpful in protecting user anonymity and circumventing censorship. However, if legislative pressure is applied, corporations will have no choice but to comply with the demands of the government. This may be trivial and to be expected by most consumers of VPN services, however, security issues in open source and previously trusted projects like TOR represent a more grave concern.

3.6.1 Side Channel Attacks

Previously, it was touched on that German authorities managed to de anonymise Tor users by deploying timing attacks. This was a concerning development in 2022 as basic internet privacy was called into question. Users assume taking measures like using Tor would provide robust privacy guarantees; however, as of late this has been undermined by several tactics used by adversaries around the globe. Side-channel attacks, for example, are are used and are quite costly. One example of this is timing attacks. This involves correlating the time taken for a computer to perform a task or perhaps how much energy was used, with what that task might be. These attacks are based on physical phenomena experienced by electronic parts such as power consumption in CMOS devices. These attacks are typically used to crack keys, voiding unprotected implementations of cryptographic primitives such as DES (Data

Encryption Standard).

Standaert, when discussing side channel attacks mentions two ways of looking at a cryptographic primitive. One could view it as a black box, some mathematical functions that translates inputs to outputs. However, another approach could be to consider how this black box will "have to be implemented in a program that will run on a given processor, in a given environment, and will therefore present specific characteristic." (9)

3.6.2 Machine Learning

It has been shown that deep learning models can be used to analyse network fingerprints to infer user identities.

INSERT SHORT SECTION

4 | Circumvention Tools

Users who care about privacy and anonymity have options to increase their operational security. Some of these tools are outlined below.

4.1 Virtual Private Networks

INSERT general paragraph explaining commercial VPNs, logs policies, etc.

Virtual Private Networks (VPNs) are one of the most commonly used circumvention tools. VPNs work by establishing a private tunnel in the public network through which users traffic is encrypted and routed. This allows users to mask their IP address and change their apparent geo location. This grants both privacy and circumvention potential; VPNs can be used to avoid geo - restrictions by routing traffic through more lenient countries.

VPNs also protect users from cybercrime through their use of encryption and secure protocols...

The role of VPNs in personal privacy and censorship circumvention cannot be overstated due to how commonplace the technology has become. INSERT A STAT ABOUT VPN USAGE

4.2 TOR & Proxy Solutions

The Onion Router, originally developed by the US government, is an open-source network overlay that routes internet traffic through volunteer-operated relays. According to the founders "Onion Routing is a distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell, and instant messaging."(10)

Requests travel through a relay passing three separate nodes. As a result, it is significantly more difficult to interpret the request's origin and destination. Tor is also commonly used as a censorship circumvention method. Tor was believed to be secure for a long time but recent developments would suggest otherwise. (11)

4.2.1 TOR Bridges

4.2.2 Mesh Networks

4.2.3 SSH Tunneling

4.3 Privacy & Communication

4.3.1 Encrypted Communication

4.3.2 Email & Browsing

4.3.3 Tails OS

5 Methodology

5.1 Introduction

5.2 The OONI Probe

5.2.1 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 (12). The OONI organization openly publishes measurements and provides a public archive on network interference from across the world.

5.2.2 Gathering Ground Truth: Virtual Machine in Israel

Below is a list of tests that will be ran on the virtual machine in Israel in order to accumulate ground truth. This data will be compared to that of OONI and a detailed analysis will be conducted.

5.2.3 Web Connectivity Tests

Gather potentially sensitive URLs here. Resources like https://github.com/citizenlab/test-lists are useful.

5.2.4 Web Messaging Tests

WhatsApp Facebook messenger Instagram TikTok Telegram Discord

Briar

5.2.5 Circumvention Tool Testing

Tor Particular Tor pages Psiphon

5.2.6 Performance Testing

5.2.7 Data-Collection

5.3 Challenges & Limitations

6 Results

7 | Conclusions

Bibliography

[1] Paul Bischoff. Internet censorship: A map of restrictions by country. *Comparitech*, 2025. URL `https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/`.

[2] Internet Monitor. Israel country profile. *Berkman Klein Center Research Publication*, (2012-1):1–5, 2012. URL `https://thenetmonitor.org/country-profiles/isr`.

[3] Reporters Without Borders. Israel. *Reporters Without Borders Country Profile*, 2023. URL `https://rsf.org/en/country/israel`.

[4] Jonathan L Zittrain, Robert Faris, Helmi Noman, Justin Clark, Casey Tilton, and Ryan Morrison-Westphal. The shifting landscape of global internet censorship. *Berkman Klein Center Research Publication*, (2017-4):17–38, 2017.

[5] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. Iclab: A global, longitudinal internet censorship measurement platform. pages 135–151, 2020. doi: 10.1109/SP40000.2020.00014.

[6] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. Blindbox: Deep packet inspection over encrypted traffic. In *Proceedings of the 2015 ACM conference on special interest group on data communication*, pages 213–226, 2015.

[7] Deep packet inspection (dpi) market size. *Business Research Insights*.

[8] Digital Rights Ireland. Digital rights ireland. https://www.digitalrights.ie/. Accessed: 2025-03-06.

[9] François-Xavier Standaert. Introduction to side-channel attacks, 2005. URL https://perso.uclouvain.be/fstandae/PUBLIS/42.pdf.

[10] 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.

[11] Paganini. Tor responds to deanonimisation. *Security Affairs*, 2024. URL https://securityaffairs.com/168667/security/tor-project-commented-on-deanonymizing-technique.html. Accessed: 2025-03-05.

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

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.