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 25, 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.

INSERT ABOUT USER PRIVACY

For the above reasons, the increasingly pervasive censorship done by governments and corporations around the world is concerning. The sheer number of individuals affected by internet censorship and the lack of transparency are strong motives for more extensive research.

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").” (2) 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. (3) 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.

1.3 Project Scope

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.

1.4 Privacy & Security Concerns

The following section contains information regarding the privacy and security concerns associated with the completion of the dissertation. This was completed in conjuncture with an assignment given in the CSU44302 Security and Privacy module. In writing a dissertation, it is crucial to consider the potential impacts of the research. This document discusses the security and privacy concerns associated with researching internet censorship. Initially, theoretical vulnerabilities will be explored. Specific cases such as Israel and Ireland will then be analyzed. Finally, a practical perspective will examine realistic security and privacy concerns, along with relevant case studies. The Open Observatory for Network Interference (OONI) will be used to gather data on internet censorship. OONI provides a comprehensive set of tests that can be run globally, offering insights into censorship situations. Since 2012, OONI has gathered over 2.5 billion measurements across 242 countries.

A virtual machine will be used to establish ground truth in Israel, running OONI CLI locally. The provider chosen, *interhost.co.il*, has a strong track record regarding data integrity and security; however, further scrutiny is necessary. Below is an audit of the software used during research.

1.4.1 OONI & OONI Probe

OONI, the Open Observatory for Network Interference, is a non-profit free software project that aims to empower decentralized efforts in documenting internet censorship worldwide (4). Released under the TOR project in 2012, it has maintained a strong reputation for data integrity and reliability.

Their positive track record is emphasized by the claim: *"To our knowledge, no OONI Probe user has ever faced consequences as a result of using our software."* (5). The success of

OONI is critically dependent on users conducting tests without repercussions. However, OONI outlines several scenarios in which running their probe may be unwise. This includes users residing in countries with a history of prosecuting similar activities, surveillance concerns, or legal restrictions on accessing content. Users who fall into one or more of these categories should be wary of the potential risks. In this context, operating in Ireland with no reason to believe I am under surveillance, I am considered a low-risk user.

Released in 2017, the OONI Probe is a mobile app and software designed to test internet censorship. Users can install and run this software, contributing to the growing dataset in the OONI database. OONI's mission is to *"ensure a free and open internet by increasing transparency of internet censorship worldwide."* While no user appears to have faced repercussions from using the OONI probe, this may lead to a false sense of security or incorrect assumptions about anonymity. As emphasized in OONI's onboarding quiz, probe tests can be visible on the network.

1.4.2 SSH & Virtual Machine (Interhost.co.il)

A virtual machine (VM) emulates a computer system. It is a file (.img) that contains instructions to create a virtual environment, leveraging physical PC resources. The provider was chosen based on location availability, with Interhost offering a machine in Tel Aviv. The shared nature of resources introduces vulnerabilities. The number of users sharing the same hardware is unknown, so file-sharing precautions were taken. Storing sensitive information on this VM may be unwise for these reasons.

SSH is a cryptographic protocol that allows users to securely and remotely control a machine over an unsecured network. It employs a client-server model with public-private key pairs for encryption and password authentication. In this project, SSH was used to remotely control the VM in Tel Aviv. Upon generating key pairs, authentication was established, and the VM became accessible. Provided secure settings are maintained and the private key is never shared, SSH is a reliable and trustworthy protocol (6).

1.4.3 Other Security and Privacy Considerations

Personal safety risks in researching internet censorship must be addressed. My supervisor highlighted that selecting a comparison country required more than just finding a contrast. Publishing documents that critique government censorship has historically been risky (7, 8). However, this research is relatively low-risk. Particularly compared to cases like Assange or Snowden. MIFTAH, an organization advocating open dialogue on the Israel-Palestine conflict, reported 310 press freedom violations from 2000-2003 (9). Although Israel has a history of reprisals, these incidents were tied to conflict zones such as Gaza. This research is not of a whistleblowing nature, reducing potential risks.

Researching Israeli state-sponsored internet censorship inevitably intersects with ongoing conflicts. The thesis remains unbiased and non-political. Historical events are included only to provide accurate context for internet censorship analysis. While Israel's military has strong ties to information control (10), it is crucial that internet censorship is examined from an empirical lense.

The security and privacy considerations for this project required assessing all tools used. OONI's privacy and security protocols appear robust. Its strong track record reinforces this confidence. SSH, as a long-established protocol, remains secure when best practices are followed. Potential consequences of researching this area are more extensive than initially anticipated. However, given my threat model, adverse effects are unlikely. Best practices will continue to be followed to ensure nonpartisan, data-driven research.

1.5 Ethical Considerations

2 | Literature Review

2.1 Introduction

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. (11) 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."(12) 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

In researching the early days of internet adoption in Ireland, a fascinating story emerges. As will be discussed, academia paved the way for the internet infrastructure Irish users enjoy today. To research the early days of internet technologies in Ireland, a variety of sources were used. One that was particularly helpful but admittedly casual resource was internethistory.ie. (13) Niall Richard Murphy documents a detailed account of Irish Internet history here. In order to verify this account and investigate specific cases, techarchives (14) was used. Other media and press sources such as RTE, The Irish Times and BBC were used in a similar fashion.

2.3.2 Ireland Today

2.3.3 EU Compliance

2.3.4 Israel Historically

Since the early 2000s, internet access has become increasingly available in Israel. In a paper discussing internet usage in Israel, Fisher speaks of "an increase of 152% in the number of Israeli households connected to the Internet during the period 2000–2005." (15)

An important aspect of this literature review was understanding how the Israel - Palestine conflict has shaped censorship of the press and the internet over the last few decades. To better appreciate the impact of this war, the Council of Foreign Relations (CFR) provides a brief overview of notable events. (16) MIFTAH, an organisation promoting open dialogue on the Israel - Palestine conflict, released a summary of freedom of press violations for the years 2000-2003. They tabulated 310 separate incidents of press freedom violations during this time, with reporters and journalists consistently being victimised. (17) It is clear from these documents that it is dangerous to report on this conflict. It is also clear that wars such as this one inevitably affect the information available to users online.

In an archived document produced by the IDF in 2016, the details for mandatory conscription of Israeli citizens is described. (18) This military draft has been ongoing since 1948 when Israel declared its independence. Men are required to serve 32 months while women serve 24. This policy, in combination with Israel's renowned intelligence operation has produced highly qualified cybersecurity professionals.

Regarding Israel's freedom of press in the 2000s, the Internet Monitor, a data analysis and collection tool states: "Modern censorship of [press] 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." (19) Though this pertains to press rather than the internet, it shows a tendency by the state to block political content. This trend would go on to continue in the 2010s and 2020s. The Colomubia Journalism Review wrote an article in 2025 discussing the potential bias of Channel 14, a prominent right-wing media outlet in Israel. Channel 14 lends itself to nationalist and patriotic rhetoric and has been subject to criticism as a result. "Netanyahu's relationship with Channel 14 goes back years, to the time when it was Channel 20, called the Heritage Channel." (20) This serves as evidence to suggest the Israeli government has a strong grasp over its media.

2.3.5 Israel Today

Today, a large majority of Israeli citizens have access to the internet. DataReportal, a website responsible for collecting and publishing global digital reports states "there were 8.51 million internet users in Israel at the start of 2024, when internet penetration stood at 92.1 percent." (21) It is also pertinent to mention Israel's booming cybersecurity industry. According to YL Ventures' recent report "In 2024, the Israeli cybersecurity industry demonstrated exceptional growth," receiving $4B in funding, double that of 2023. The roots of this industry come as a direct product of the nation's fixation with intelligence and national security.

Reporters Without Borders (RSF), responsible for the World Press Freedom Index, provide detailed reports pertaining to media censorship globally. They have ranked Israel as 101st in the world as of 2024 in this regard. 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." (22)

In a 2024 paper discussing digital diplomacy in the Israel - Gaza war, Othman asserts "Governments and non-state actors leveraged social media to influence international public opinion, while misinformation campaigns complicated the narrative, undermining trust in diplomatic channels." (23) The relationship between war and social media in the modern age is a concerning issue. To understand internet censorship in Israel today, it is important to identify what individuals and institutions are behind this activity. Israel entrusts this operation to the Israeli Military Censor, a department of the Israeli Defense Forces (IDF). This group is responsible for state-sponsored censorship online and is headed by the minister of defense, currently Israel Katz.(24) Historically, the IDF have had to answer for media censorship through their Spokesperson Unit (ISU). "the ISU is continually fluctuating between openness and opaqueness because its activities are affected by so many internal and external factors" (25)

Though internet censorship can prove inflammatory, the internet can also be used to ease tensions. Digital diplomacy can be described as how a government uses the internet and related technologies to manage international relations. "Findings reveal an unmatched proactive approach by Israel's digital diplomacy compared to other states, rooted in a humanitarian grounds concern despite limited peace efforts, and significant obstacles from prevalent anti-Israel online sentiment, changing social media perceptions, and platform executive decisions hindered by personal political inclinations." (23)

According to Zittrain in his 2017 paper discussing internet censorship, Israel has not always been proactive in blocking political content. "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." (26) Zittrain described this trend of blocking undesirable websites in 2017. In 2023, Israel passed what was described as "draconian" legislation by the RSF, that punishes the "consumption of terrorist materials." (27) This law targeted sites such as Aljazeera, a media outlet focusing on covering the Gaza crisis funded by the Qatari government. (28) This example shows the litigious nature of the Israeli state in censoring content online.

Having considered the unique national security threats faced by Israel, it is clear that citizens are not overly concerned with the State abusing its power. The tumultuous history faced by the state means that "the IDF is highly trusted by a society that deeply values the defense system, it is very difficult to criticize its deficiencies." (25) A troubling result of the Gaza crisis has been the utilisation of social media during war. On 14 November 2012, a tweet from the official IDF Twitter account stated "The IDF has begun a widespread campaign on terror sites & operatives in the Gaza Strip, chief among them Hamas & Islamic Jihad targets." (29) This marked the beginning of what Kretschmer described as a war that is "tweeted live." In her research, she describes a concerning account of both sides "constantly informing on rocket attacks." (30) Propaganda and misinformation has been influential in shaping global opinions on this war, and the internet has accommodated this.

2.4 Analysis: Ireland vs Israel

It is clear from the research conducted that Ireland and Israel's internet censorship situations share commonalities. Specifically, both countries are active in censoring pirated media and otherwise illegal content. However this is not the only similarity shared.

Both Israel and Ireland were early adopters of internet technologies as illustrated above. Though the two governments participated in this development to varying extents, it resulted in the successful deployment of the internet in both cases.

The motives for internet censorship vary from country to country, however there is a distinct overlap seen here. Both Ireland and Israel take a strong stance against pirated media, CSAM, or otherwise illegal material and use a combination of DNS tampering and IP/TCP blocking to combat sources of such content.

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.

Finding comprehensive and credible resources on censorship mechanisms proved challenging due to the depth of the research area. One resource that proved particularly useful in this way were Requests for Comments (RFCs). These documents highlight internet standards placed by the Internet Engineering Task Force and thus provide the accurate technical specifications needed. RFC 9505 proved invaluable in highlighting the majority of censorship methods used today. It was last updated by the Internet Research Task Force in late 2023 and provides the technical basis for this section of the thesis. The document "describes technical mechanisms employed in network censorship that regimes around the world use for blocking or impairing Internet traffic."(31) In combination with relevant academic papers, other RFCs like 2818 (HTTPS) (32) and 8446 (TLS 1.3) (33) were examined.

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." (34) 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. RFC 9505 explains points of control in great detail. It states "internet censorship takes place in all parts of the network topology," however, "There are various logical and physical points of control that censors may use for interception mechanism."(31). Below are some notable points of control explained.

Some points of control include ISPs, IXPs, VPNs, national gateways and local networks. These are noteworthy locations where censors likely operate. Internet Service Providers (ISPs)

Internet Exchange Points (IXPs)

National Gateways

Services

Institutions and Content Sites

Governments and institutions leverage these nodes in the network's topology to restrict user access to undesirable content. 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.

In his research paper from 2003, Zittrain gives a solid overview of points of control. He discusses varying reasons to be concerned about points of control and how they are used. One argument he makes is the violation of the end-to-end principle. Simply, this refers to keeping the middle of the network simple and pushing complexity out towards the edge of the network to hosts.

"The technical aspect of the end-to-end argument suggests a warning against blocking data transmissions at any point [other than endpoints]." (35)

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. Zittrain concludes his research with a word of warning regarding points of control and their potential for abuse. He highlights the need for "a comprehensive framework where sovereigns' actions to block material are thoroughly documented and open to challenge." (35) Unfortunately, we are yet to see this in action since 2003.

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

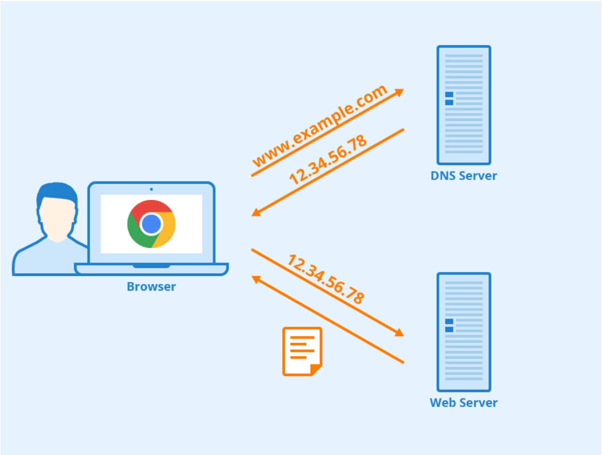

Figure 3.1: DNS Requests and IP

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 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 (31).

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 (31).

3.3.3 MITM Attacks

Kampourakis, Kambourakis, Chatzoglou, and Zaroliagis wrote an academic paper in 2022 arguing the effectiveness of MITM attacks against HTTPS in certain circumstance. They describe a MITM attack as follows. "A man-in-the-middle (MitM) attack enables threat actors to position themselves in a conversation between two parties. It can be used to eavesdrop on, or impersonate, either of the parties and may enable the perpetrator to steal personal information, including login credentials, payment card data and account details."(36)

A man-in-the-middle attack involves intercepting encrypted packets (potentially at a point of control), to 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.

RFC 2818, released in 2000, describes "how to use TLS to secure HTTP connections over the Internet," (32)known as HTTPS. This was designed to mitigate the effects of MITM attacks. Recent research suggests deployments of HTTPS in most browsers is insecure, at least in certain circumstance. Kampourakis and his colleagues went on to say "some insidious variants of MitM against HTTPS remain quite realistic across all popular Internet browser types irrespective of the underlying platform." (36) They mention how "both of the attack variations were successful against all the browser types and versions..." except the latest versions of Firefox that they tested.

3.4 Content Manipulation

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

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." (37)

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." (38)

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." (39) 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." (40)

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."(41)

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. (42)

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 (**?**). 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] Security Affairs. Tor project commented on deanonymizing technique, 2025. URL `https://securityaffairs.com/168667/security/tor-project-commented-on-deanonymizing-technique.html`. Accessed: 2025-03-22.

[2] J. Zittrain, R. Faris, H. Noman, J. Clark, C. Tilton, and R. Morrison-Westphal. The shifting landscape of global internet censorship. Technical report, Harvard Law School, 2017. URL `https://doi.org/10.2139/ssrn.2993485`. Accessed: 2025-03-22.

[3] Reporters Without Borders (RSF). 2014 report: Enemies of the internet, 2014. URL `https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf`. Accessed: 2025-03-22.

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

[5] Open Observatory of Network Interference (OONI). Risks of using ooni, 2025. URL `https://ooni.org/about/risks/`. Accessed: 2025-03-22.

[6] OpenSSH Project. Openssh manual, 2025. URL `https://www.openssh.com/manual.html`. Accessed: 2025-03-22.

[7] Encyclopædia Britannica. Julian assange biography, 2025. URL `https://www.britannica.com/biography/Julian-Assange`. Accessed: 2025-03-22.

[8] Encyclopædia Britannica. Edward snowden biography, 2025. URL https://www.britannica.com/biography/Edward-Snowden. Accessed: 2025-03-22.

[9] MIFTAH. Freedom of press violations 2000-2003, 2003. URL https://miftah.org/Display.cfm?DocId=4450&CategoryId=8. Accessed: 2025-03-22.

[10] Unknown. Israel war and censorship. *ScienceDirect*, 2025. URL https://www.sciencedirect.com/science/article/pii/S0363811117300231. Accessed: 2025-03-22.

[11] Hannah Ritchie, Edouard Mathieu, Max Roser, and Esteban Ortiz-Ospina. Internet. *Our World in Data*, 2023. https://ourworldindata.org/internet.

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

[13] Internet History of Ireland. Internet history of ireland, 2025. URL http://www.internethistory.ie/. Accessed: 2025-03-22.

[14] Tech Archives Ireland. Tech archives ireland. URL https://techarchives.irish/. Accessed: 2025-03-22.

[15] Yael Fisher and Orit Bendas-Jacob. Measuring internet usage: The israeli case. *International Journal of Human-Computer Studies*, 64(10):984–997, 2006. ISSN 1071-5819. doi: https://doi.org/10.1016/j.ijhcs.2006.05.003. URL https://www.sciencedirect.com/science/article/pii/S1071581906000814.

[16] Council on Foreign Relations (CFR). Israeli-palestinian conflict timeline, 2024. URL https://education.cfr.org/learn/timeline/israeli-palestinian-conflict-timeline. Accessed: 2025-03-09.

[17] Miftah: The Palestinian Initiative for the Promotion of Global Dialogue and Democracy. Analysis of internet censorship and freedom of expression in palestine, 2003. URL https://miftah.org/Display.cfm?DocId=4450&CategoryId=8. Accessed: 2025-03-09.

[18] Ministry of Immigrant Absorption, Israel. The israel defense forces (idf), 2016. URL https://web.archive.org/web/20190722211213/http://archive.moia.gov.il/Publications/idf_en.pdf. Accessed: 2025-03-09.

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

[20] Columbia Journalism Review (CJR). Israel's channel 14 and the battle over human rights reporting, 2024. URL https://www.cjr.org/world/israel-channel-14-human-rights.php. Accessed: 2025-03-09.

[21] DataReportal. Digital 2024: Israel, 2024. URL https://datareportal.com/reports/digital-2024-israel. Accessed: 2025-03-09.

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

[23] Rose Othman. The challenges facing digital diplomacy in the israel-gaza war (2023-2025). *SSRN Electronic Journal*, February 12 2025. doi: 10.2139/ssrn.5134274. URL https://ssrn.com/abstract=5134274. Accessed: 2025-03-09.

[24] Ministry of Defense, Israel. Minister of defense, 2025. URL https://english.mod.gov.il/Minister_of_Defense/Pages/Minister-of-Defense.aspx. Accessed: 2025-03-09.

[25] Clila Magen and Ephraim Lapid. Israel's military public diplomacy evolution: Historical and conceptual dimensions. *Public Relations Review*, 44(2):287–298, 2018. ISSN 0363-8111. doi: https://doi.org/10.1016/j.pubrev.2017.11.003. URL https://www.sciencedirect.com/science/article/pii/S0363811117300231.

[26] 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.

[27] Reporters Without Borders (RSF). Pressure, intimidation, and censorship: Israeli journalists have faced growing repression in the past year, 2024. URL https://rsf.org/en/pressure-intimidation-and-censorship-israeli-journalists-have-faced-growing-repr Accessed: 2025-03-09.

[28] Al Jazeera. Knesset introduces 'consumption of terrorist publication' as offense, November 8 2023. URL https://www.aljazeera.com/news/2023/11/8/knesset-introduces-consumption-of-terrorist-publication-as-offense. Accessed: 2025-03-09.

[29] Israel Defense Forces (IDF). Official idf statement on x (formerly twitter), 2024.

[30] Lisa-Maria Kretschmer. Imagine there is war and it is tweeted live – an analysis of digital diplomacy in the israeli-palestinian conflict. *Global Media Journal - German Edition*, 7(1), Jul. 2017. URL https://globalmediajournal.de/index.php/gmj/article/view/37.

[31] Joseph Lorenzo Hall, Michael D. Aaron, Amelia Andersdotter, Ben Jones, Nick Feamster, and Mallory Knodel. A Survey of Worldwide Censorship Techniques. RFC 9505, November 2023. URL https://www.rfc-editor.org/info/rfc9505.

[32] Eric Rescorla. HTTP Over TLS. RFC 2818, May 2000. URL https://www.rfc-editor.org/info/rfc2818.

[33] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018. URL `https://www.rfc-editor.org/info/rfc8446`.

[34] 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.

[35] Jonathan Zittrain. Internet points of control. 2003.

[36] Vyron Kampourakis, Georgios Kambourakis, Efstratios Chatzoglou, and Christos Zaroliagis. Revisiting man-in-the-middle attacks against https. *Network Security*, 2022, 03 2022. doi: 10.12968/S1353-4858(22)70028-1.

[37] 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.

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

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

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

[41] 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.

[42] 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.

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.