



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

APRIL 14, 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 than 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

Abstract	ii
1 Introduction	1
1.1 Research Motivation	1
1.1.1 User Rights & Privacy	2
1.2 Background	2
1.2.1 Global Internet Censorship	2
1.3 Project Scope	3
2 Literature Review	5
2.1 Introduction	5
2.2 Literature Review Methodology	6
2.3 Ireland Historically	6
2.4 EU Compliance	8
2.4.1 EU Law: Case Studies	9
2.5 Ireland Today	10
2.5.1 Irish Legislation	11
2.5.2 Irish Law: Case Studies	12
2.5.3 Israel Historically	13
2.5.4 Israel Today	14
2.5.5 Israeli Law: Case Studies	15
3 State of the Art	17

3.1	Introduction	17
3.1.1	Overt vs. Covert Censorship	18
3.2	Censorship Techniques and Mechanisms	18
3.2.1	Points of Control	18
3.2.2	Legislative Pressure	20
3.2.3	MITM Attacks	21
3.3	Network-Level Filtering	22
3.3.1	IP Blocking	22
3.3.2	DNS Interference	22
3.3.3	Network Blackouts	24
3.4	Keyword Filtering & Deep Packet Inspection	24
4	Circumvention Tools	27
4.1	Circumvention Tools	27
5	Methodology	32
5.1	Collecting Data: OONI	32
5.1.1	Background	32
5.1.2	OONI Probe	32
5.1.3	Virtual Machine	33
5.2	Ground Truth: Ireland & Israel	33
5.2.1	Description of OONI Tests	35
5.2.2	Data Collection and Transparency	39
5.3	Privacy & Security Concerns	39
5.3.1	OONI Probe	39
5.3.2	SSH & Virtual Machine	40
5.3.3	Other Security and Privacy Considerations	40
6	Results	42
6.1	Overview	42
6.1.1	Network Environment Context: Ireland	43

6.1.2	Network Environment Context: Israel	43
6.2	Website Connectivity Tests	43
6.2.1	Ground Truth via SSH	43
6.2.2	Native Website Connectivity Tests	43
6.2.3	my-websites.txt	44
6.2.4	Investigating Aljazeera.com	45
6.2.5	Public OONI Database	46
6.3	Instant Messaging Tests	48
6.3.1	Public OONI Database: Ireland	48
6.3.2	Public OONI Database: Israel	50
6.3.3	Ground Truth via SSH	51
6.4	Circumvention Tests	51
6.4.1	Public OONI Database: Ireland	51
6.4.2	Public OONI Database: Israel	52
6.4.3	Ground Truth via SSH	53
6.5	Middlebox Tests	54
6.5.1	Public OONI Database: Ireland	54
6.5.2	Public OONI Database: Israel	55
6.5.3	Ground Truth via SSH	56
6.6	Comparative Analysis: Ireland vs. Israel	57
6.6.1	Summary: Irish Internet Censorship	57
6.6.2	Summary: Israeli Internet Censorship	57
6.6.3	57
6.7	Guide to Replicating Results	57
6.7.1	Investigating Aljazeera.com	57
6.7.2	Raspberry Pi Setup	57
7	Conclusions	59
7.1	Analysis: Ireland vs Israel	59

A1 Appendix	76
A1.1 Appendix numbering	76
A1.2 Website Connectivity Tests: my-websites.txt	76
A1.2.1 my-websites Results: Ireland	81
A1.2.2 my-websites Results: Israel	82
A1.3 sample_aljazeeraurls.txt	82

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.

1.1.1 User Rights & Privacy

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." (2) 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.

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")." (3) 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. (4) 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 goals for the thesis. The stretch goal is to contribute to the OONI project. A more attainable contribution is to merge resources in order to compile a better sensitive domain list that is specific to Ireland and Israel. This would improve the testing capability for the locations being considered.

Review existing literature	Examine notable events in each country
Assess internet censorship mechanisms	Use OONI data to cross-correlate events
Identify censoring parties	Use OONI data to note interference trends
Analyse motives and ethics	Gather ground truth with a virtual machine
Investigate justifications & transparency	Comparative analysis of Israel & Ireland
Note mechanisms used by both countries	Consider security and privacy issues
Investigate public response	Contribute to the OONI project

Figure 1.1: Goals of the research

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. (5) 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." (6) 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 covert. This sections aims at laying the foundation for discussing both countries' approach and sentiments towards internet technologies.

2.3 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. (7) Niall Richard Murphy documents a detailed account of Irish Internet history here. In order to verify this account and investigate specific cases, [techarchives](http://techarchives.org) (8) was used. Other media and press sources such as RTE, The Irish Times and BBC were used in a similar fashion.

The internet in Ireland has come a long way since The Irish Sugar Company took delivery of the first computer in the country. "The Sugar Company paid £33,000 for the system." (9) Conservatism hampered development early on, however, as the cost of hardware decreased in the 60s Irish universities began investing in computers. Tech Archives suggests of early adopters, "their financial backing was minimal. They relied on students and volunteers to keep running. Their day-to-day operations were largely improvised and sometimes anarchic." (10) This progress continued into the 80s and 90s as the potential became apparent. This progress was also driven by IT professionals who adopted Unix. EUnet was a collaborative effort that succeeded in becoming the "first public wide area network in Europe." (10) The gateway was later relocated and managed by Trinity College Dublin. This advancement set the stage for the foundation of Ireland's first ISP by Cormac Callanan and Michael Nowlan, IEUnet. In a low-key email, Nowlan announced the arrival of the internet in Ireland, aptly stating "No guarantees of reliable service are offered at present, it is quite likely that the line will go down at no notice. " (11)

Though the Irish government played a passive role in this development, they deserve credit for the legislation they passed in 2000. The E-Commerce Act legitimised electronic transactions by asserting "electronic communications are deemed equivalent to written or oral communications." (12) This seems trivial today, but it was a huge step in the right direction. Though Ireland was in many ways following EU trends, a strong emphasis was placed on privacy. The Irish Times released an article discussing how the legislation "appears to protect the privacy of communications far more than the laws of our neighbours." (13) This is contextually impressive considering other institutions, such as the FBI, harked "the widespread

use of robust non-recovery encryption will ultimately devastate our ability to fight crime and terrorism." (13)

Fast forward to 2002 and Eir has began rolling out broadband internet access to consumers. In 2005, Ireland surpassed 2 million internet users, denoting the successful adoption of the technology. At this point, the internet and its technologies had penetrated industry, academia and consumerism. This time marked a turning point in communications both in Ireland and globally.

2.4 EU Compliance

Aside from Irish legislation, there are EU directives that run in conjuncture such as the Digital Services Act, GDPR and more. These will be discussed in detail in this section. Let us first establish the primacy of EU law as echoed in the Irish Constitution. "As well as being superior to national law, some EU law has direct effect on its citizens." (14) The European Commission proposes laws that are sent to the European Commission and then the Council of the European Union to be approved by a qualified majority and passed, or rejected. (15) This procedure has lead to the passing of legislation that affects internet usage in Ireland.

General Data Protection Regulation (GDPR) The first law to be discussed is General Data Protection Regulation (GDPR). This legislation is designed to protect user privacy and bolster data integrity. It highlights the acceptable procedures for handling user data and is used to police organisations. Penalties come in the form of fines, up to 20 million euros. (16)

Digital Services Act (DSA) The second law worth mentioning is the Digital Services Act, which came into EU law in November of 2022, and was followed by the Irish law of the same name in 2024. (17) (18) This act addresses illegal content, disinformation and transparent advertising and thus, is of particular relevance to the research being conducted. The final example of EU legislation that has undoubtedly shaped internet censorship seen in Ireland is the Copyright Directive (2019). This

legislation solidifies intellectual copyright law within the EU, providing some edge cases of where free use applies. (19) These three important pieces of legislation guide Ireland's internet censorship.

2.4.1 EU Law: Case Studies

It has been mentioned that compliance is a strong motivation for the Irish government to censor and due to EU law primacy. Now, let us focus on some notable real world examples of legislation being used to censor content online or otherwise reprimand nonconforming organisations. Four high profile cases of non compliance will be discussed as well as the outcomes in each case.

1. Google and the "Right to be Forgotten" (2014) In 2014, the Court of Justice of the European Union (CJEU) ruled in *Google Spain SL v. Agencia Española de Protección de Datos*. This salient case granted individuals the right to request the removal of outdated personal data from search engine results. (20) This landmark ruling was based on the EU's data protection laws. The ruling had a profound impact on how search engines and online platforms handle personal data. Google, as the largest search engine, were forced to make stark changes in their browser's operation, reshaping online content management. The decision triggered similar discussions on privacy and free speech, creating a global precedent for data removal requests.

2. YouTube and the EU Copyright Directive (2019) Under the EU Copyright Directive, Article 17 requires platforms like YouTube to prevent the upload of copyrighted content without permission. (21) This change forced YouTube to implement automatic content filtering systems. This mandated more stringent controls over user-uploaded videos, significantly impacting how online platforms handle user-generated content. Though it aimed to protect copyright holders, it also raised concerns about excessive censorship. Automatic filters could lead to the removal of legitimate content, raising a significant challenge in balancing copyright protection and free speech.

3. Facebook and the GDPR Fines (2021-2024) In 2021, Meta (formerly Facebook) was fined €265 million by Ireland's Data Protection Commission (DPC) due to a data breach that exposed personal information of millions of users. (22) The breach was linked to the company's failure to adequately protect user data, violating GDPR standards. Meta has faced a litany of fines at the hands of the EU and other regulating bodies. Meta has received fines of over 2 billion euros in 2024 alone. (23) This exemplifies the European Union's stringent enforcement of GDPR which holds companies accountable for safeguarding personal data.

4. Twitter's Non-Compliance with the Digital Services Act (DSA) In 2023-2024, Twitter (now X) faced scrutiny under the EU Digital Services Act (DSA) for failing to implement required measures to combat illegal content and misinformation. (24) The platform was given deadlines to comply, including implementing more robust content moderation policies. This case highlighted the increasing regulatory pressure on tech firms to ensure their platforms are safe, free of illegal content, and accountable for user actions. Previously, X withdrew from a voluntary agreement to combat disinformation online. Despite this protest in the face of the Digital Services Act, legislators were quick to point out that X will still have to comply with EU standards. (25)

2.5 Ireland Today

As of 2024, the Irish digital sector exceeded a valuation of \$50 billion, (26) Bolstered by strong international relations and low corporate tax, Ireland is an attractive location for any tech company looking to infiltrate the EU market. A corporate tax of 12.5% (27) and a skilled and educated work force has proved tantalizing for tech giants. Ireland balances citizens privacy and safety with keeping tech giants satisfied. Over the years, this approach has proved very effective with the likes of Google, Facebook (Meta), Apple and Microsoft setting up EU bases in Ireland. It is clear that Ireland's tech industry is a booming financial success but it has faced criticism for its

tax system. Criticism recently came at the hands of financier Howard Lutnick who described Ireland as his favourite "tax scam." (28) He highlights concerns around the number of US pharmacological and tech companies operating in Ireland and the intellectual property acquired by Ireland as a result. Conjecture aside, it is clear that there are strong forces at play that influence the regulation of tech companies on Irish soil. This influence undoubtedly affects the internet censorship situation faced by Irish users and will be investigated in the context of case studies. Before this, let us briefly go over the legislation that affects this area.

2.5.1 Irish Legislation

The Defamation Act (2009) An early piece of legislation passed by the Irish government that addresses defamation both online and offline. This act describes defamation as "the publication, by any means, of a defamatory statement concerning a person to one or more than one person." (29) Simply, this document aims to uphold an individual's right to a good name.

Communication Act (2011) This act strengthened the regulation of electronic communication and focused primarily on issues like data retention, consumer rights and cybersecurity. This act articulates the legal framework for the monitoring and interception of certain online communications in the interest of law enforcement and national security. It mandates timelines for the safe retention and eventual destruction of sensitive consumer data. It also enables a senior Gardai to "request a service provider to disclose to that member data retained by the service provider." (30)

Online Safety and Media Regulation Act (2022) This law targets harmful digital content like hate speech and misinformation. This empowers a newly appointed Coimisiun na Meán to regulate content that fits these criteria, addressing issues such as cyber-bullying and extremism. At the head of this organisation is the Online Safety Commissioner who is "responsible for the implementation of a binding online

safety code." (31)

2.5.2 Irish Law: Case Studies

Now that we have some background on the legislation passed in Ireland relating to internet censorship, we can examine notable cases.

The Pirate Bay & More (2009, 2013) In 2009, major media labels began pressuring six ISPs to block access to the Pirate Bay website. This came to a head in 2013, when the ISPs were ordered to block access by the High Court. (32) This was a momentous event as it marked the first use of updated EU copyright legislation. The website was and still is one of the most popular torrent sites globally, with total monthly visits exceeding 20 million today, according to Similar Web. (33) Since the 2010s this trend of blocking piracy by judiciary process continued, with site like Eztv, Putlocker and GoMovies being blocked to this day.

Ban on Russian State Media (2022) Following the Russian invasion of Ukraine in February of 2022, the EU released a directive (34) to block access to Russian state media websites. European Commission President Ursula von der Leyen announced "The state-owned Russia Today and Sputnik, and their subsidiaries, will no longer be able to spread their lies to justify Putin's war." (35) Following this, the EU imposed heavy sanctions on those who were found to be hosting versions of these websites. In response, Russia blocked a number of EU based media outlets, particularly those critical and vocal about the invasion. This included the Irish state-owned RTE and the Irish Times. (36)

Social Media Under EU Law Under the aforementioned DSA and GDPR legislation, Ireland's Data Protection Committee has required platforms such as TikTok and X to remove non-compliant content. Platforms such as Meta, TikTok and X have faced legal trouble regarding misinformation and hate speech. A salient example is TikTok's refusal to submit a risk report prior to launching TikTok Lite in France, Spain and elsewhere. "Under the DSA, designated Very Large Online Platforms are

obliged to submit a risk assessment report." (37)

2.5.3 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." (38)

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. (39) 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. (40) 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. (41) 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." (42)

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 Colombia 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." (43) This serves as evidence to suggest the Israeli government has a strong grasp over its media.

2.5.4 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." (44) 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." (45)

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." (46) 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.(47) 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" (48)

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." (46)

2.5.5 Israeli Law: Case Studies

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." (49) 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." (50) This law targeted sites such as Aljazeera, a media outlet focusing on

covering the Gaza crisis funded by the Qatari government. (51) 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." (48) 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." (52) 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." (53) Propaganda and misinformation has been influential in shaping global opinions on this war, and the internet has accommodated this.

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. Requests for Comments (RFCs) proved useful in this regard. 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." (54) In combination with relevant academic papers, other RFCs like 2818 (HTTPS) (55) and 8446 (TLS 1.3) (56) 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.'" (57) 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." (54). Below are some notable points of control explained.

Internet Service Providers (ISPs) Entities that accommodate the accessing, using or participating in the internet. Bridging the gap between consumers and the global internet, ISPs are often required to act as "law enforcers and adjudicators." (58) Tosza discusses how ISPs and tech giants alike are self-regulating and implicit in internet censorship. Legislation like the Digital Services Act (EU) allows governments to effectively block content deemed harmful at the ISP level.

Internet Exchange Points (IXPs) A common definition for IXPs is a "network infrastructure with the purpose to facilitate the exchange of Internet traffic between

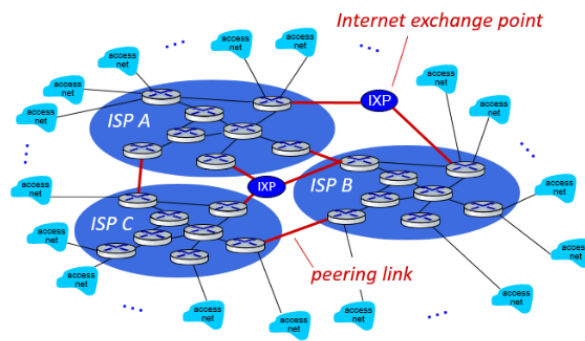


Figure 3.1: Caption

Autonomous Systems (ASes) and operating below layer 3." (59) Put more simply, they are physical locations where different ISPs and networks interconnect to exchange traffic. IEEE describes IXPs as "the facilitator of peering." (60)

National Gateways Refers to the centralised infrastructure through which a country's internet traffic is routed. In a 2009 paper discussing internet infrastructure as it relates to censorship, Karlin and Forrest argue that internet traffic is "increasingly affected by national policies." (61) They go on to illustrate how countries like the UK, Germany and the US are "central to international reachability, and their policies thus have huge potential impact." (61)

Institutions Businesses, universities and other organisations often have a responsibility to filter the content seen by their users on their network. This is often done to comply with legal obligations, apply ethical standards or to protect network security. This is achieved by a combination of firewalls, keyword-filtering and network level blocking. These techniques are highlighted in Zittrain's 'The Future of the Internet - And How to Stop It,' (62) and will be discussed further below.

Governments leverage these nodes in the network 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. One issue he raises 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 presence of middleboxes and other devices could be impacting performance of the network.

"The technical aspect of the end-to-end argument suggests a warning against blocking data transmissions at any point [other than endpoints]." (63)

Although security considerations such as HTTPS and TLS can help protect users from threat actors, points of control are a physical reality to be contended with. As user packets traverse the network they are 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." (63)

3.2.2 Legislative 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. More commonly, judiciary process is used in democratic states to block access to illegal sites. Blocking will then be implemented through DNS servers, ISPs, institutions, service providers or otherwise in accordance with court orders.

VPN providers are subject to the scrutiny of the jurisdiction within which they operate. NordVPN, a very popular VPN provider based in Amsterdam has said on record "We will comply with lawful requests as long as they are delivered according to all the laws and regulations." (64) 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.

3.2.3 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." (65) A MITM attack simply involves a threat actor, or in this case a censor, placing themselves in the middle of a conversation, potentially at a point of control. 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," (55) 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." (65) 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.

3.3 Network-Level Filtering

The following section is based primarily on information from the source *RFC 9505 A Survey of Worldwide Censorship Techniques* (54). Any other information sourced from elsewhere is identified as such.

3.3.1 IP Blocking

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. RFC 791 describes the function of the Internet Protocol, "to move datagrams through an interconnected set of networks." (66)

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. In a 2009 report, Callanan and co. describe how "the server that contains the website could be blocked at the level of its IP address, preventing anyone using the filter from accessing that address." (67) 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. A prime example discussed previously is the blocking of the Pirate Bay. (32)

3.3.2 DNS Interference

DNS interference 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,

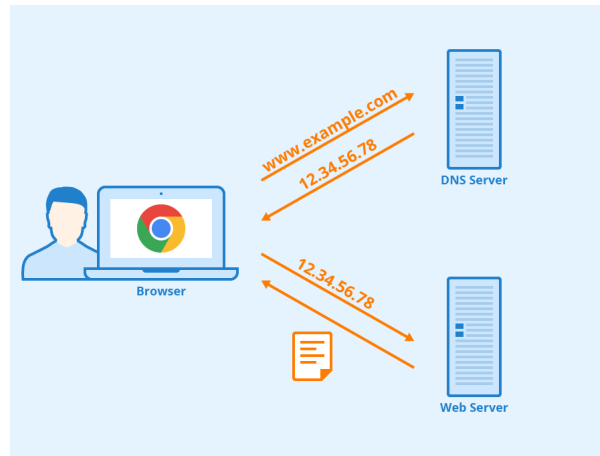


Figure 3.2: DNS Requests and IP

replying with an error message, or responding with an incorrect address. *DNS Mangling* is a network-level technique of on-path interception where an incorrect IP address is returned in response to a DNS query to a censored destination. *DNS Cache Poisoning & Lying* 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 a meaningless domain. DNS lying on the other hand involves the censor mandating that the DNS server provide a particular response. Of all of the methods to tamper with DNS resolution this is the most aggressive. (54).

The above DNS interference methods require the censor to traverse a controlled DNS hierarchy for this mechanism to be effective. This mechanism can be circumvented by using a different publicly known DNS resolver that is not controlled by the censor. This mechanism can also lead to unintentional blocking in area's not controlled by the censor. For example, sometimes a user outside of the censor's region will be directed through DNS servers controlled by the censor, causing the request to fail.

3.3.3 Network Blackouts

A very straightforward, holistic, and blunt form of censorship is network blackouts. This method involves a large governing body of an area or region completely shutting off Internet access for all content. This method is becoming more and more common across areas in the Middle East and Asia. According to a report from *Access Now*, there were a total of 296 different internet shutdowns across 54 countries. (68) This is a 35% increase from the previous high in 2022 (69). This form of censorship is very extreme and is often implemented in times of conflict, protest and democratic instability.

3.4 Keyword Filtering & Deep Packet Inspection

So far, methods of internet censorship have revolved around blocking a publishers address. However censors can examine the contents within packets to make decisions regarding their accessibility. This refers to the concept of application layer filtering; monitoring a communication channel and detecting offensive keywords. This is seen in more cultivated censorship models that strive to censor topic 'x'.

Keyword Filtering This approach involves scanning the contents of web requests for specific sensitive words or phrases. Upon encountering a request that contains a blacklisted keyword, the censor can disrupt the communication by, for example, sending TCP reset packets to both sides. This is a simple approach that is easily implemented. Pattil, in a 2014 paper, described this process saying "any packet that is passed across the network is scanned against a list of sensitive keywords and if present it forces the connection to terminate." (70) Circumventing keyword filtering is not particularly difficult. Coy publishers will employ deliberate misspelling or use of synonyms in place of sensitive keywords.

A notorious example of keyword filtering in the real world is China's censorship of the 1989 Tiananmen Square protests. The Chinese government has been dedicated to

removing this from the memory of its citizens, particularly the younger generation. (71) Louisa Lim, while researching this topic in 2014, polled Chinese students at four Beijing campuses and found that "out of 100 students, only 15 could identify the [Tank Man] picture." (72) In December of last year it surfaced that Tokyo University had embedded a keyword relating to the incident into one of its online applications. In an apparent attempt to prevent the page from loading in mainland China and stop Chinese students from applying, the university weaponised the Great Chinese Firewall. This is a prime example of the limitations of keyword filtering. (73)

Deep Packet Inspection DPI 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 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." (74)

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." (75)

4 | Circumvention Tools

4.1 Circumvention Tools

Users who care about privacy and anonymity have options to increase their operational security and avoid censorship. Some of the most noteworthy tools are briefly explained below. It is worth mentioning that accessing these tools can be difficult for certain individuals. ProtonVPN discusses some of the countries that have outlawed VPN usage. (76) Some notable examples include Cuba, China, Vietnam and Egypt. This is a common theme; an arms race between oppressive regimes interested in censorship and circumvention and privacy based tools.

Encryption Encryption is the fundamental security element driving communication over the internet. Bhanot describes encryption as "the process of converting normal data or plaintext to something incomprehensible or cipher-text by applying mathematical transformations or formulae." (77) The importance of cryptography in security cannot be overstated. "Today, end-to-end encryption is the standard by which almost if not all communication over the internet occur. Examples of messaging platforms that offer this as standard include Telegram, Whatsapp and Facebook Messenger. CloudFlare states that end-to-end encryption "gives people total control over who can read their messages, enabling them to keep their messages private." (78) Encryption is the backbone of privacy online which allows users to leverage math to provide anonymity, at least in the best of cases. Zeadally, Das and Sklavos state the following about encryption "These techniques provide several

security requirements, such as confidentiality, data integrity, entity authentication, message authentication, key management, non-repudiation, trustworthy data platforms, and digital signatures." (79) It is clear from the research conducted that encryption has been fundamental in protecting user rights.

Side Channel Attacks Side-channel attacks are a sophisticated technique used for deanonymisation and key cracking. 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." (80)

Transport Layer Security Transport Layer Security (TLS) is an example of encryption being used to secure data transfer online. TLS replaced the deprecated Secure Socket Layers (SSL), and TLS 1.3 is the standard by which data is transferred over the internet. According to the Internet Society, "TLS is normally implemented on top of TCP in order to encrypt Application Layer protocols such as HTTP, FTP, SMTP and IMAP." (81) TLS operation is described in detail in RFC 8446 (56) (82). Below is a figure that shows a TLS handshake.

However, cryptography has not always had this virtuous reputation. The FBI lead what can only be described as a smear campaign against the technology in the early 2000s. In 1999, the director of the FBI, Louis Freeh, stated "encryption ultimately will devastate our ability to fight crime and prevent terrorism." (83) Unsurprisingly, their stance has changed along with the growing necessity for encryption. Today, the FBI website states of encryption: "Law enforcement supports strong, responsibly

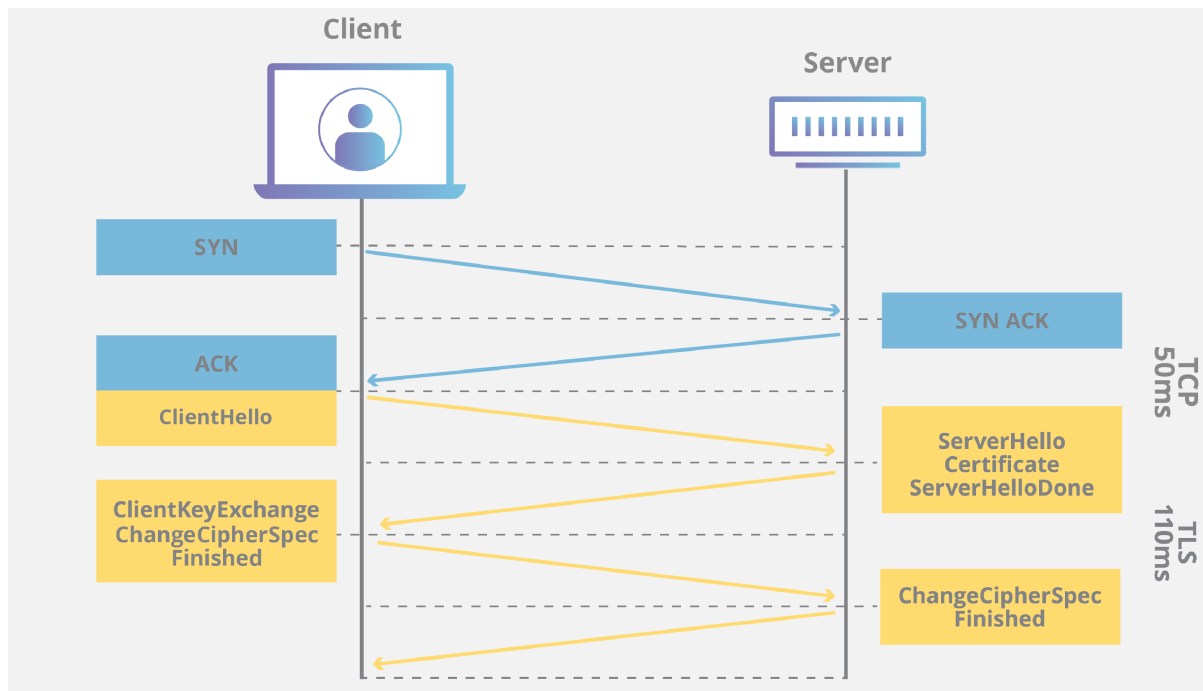


Figure 4.1: TLS Handshake, source cloudflare.com

managed encryption. This encryption should be designed to protect people's privacy and also managed so U.S. tech companies can provide readable content in response to a lawful court order." (84) The US government employs more methods than slander to defeat cryptography. The National Security Agency (85) has a colourful reputation regarding its contributions to cryptographic standards. Dual_EC_DRBG was a cryptographic standard released by the NSA in 2007 and ratified by the National Institute of Standards and Technology (NIST). It was later found that this was insecure, having back door potential. CloudFlare defines a back door as "an intentional flaw in a cryptographic algorithm or implementation that allows an individual to bypass the security mechanism." (86) The discovery of this vulnerability is credited to Dan Shumow and Niels Ferguson. (87)

Virtual Private Networks Virtual Private Networks (VPNs) are one of the most commonly used and important circumvention tools on the market. VPNs use tunnelling to encrypt packets at the lowest level, the OSI link layer. Microsoft developed Point-to-point Tunnelling Protocol (PPTP) which is now deprecated, having been shown to be insecure. (88) More relevant examples of VPN protocols

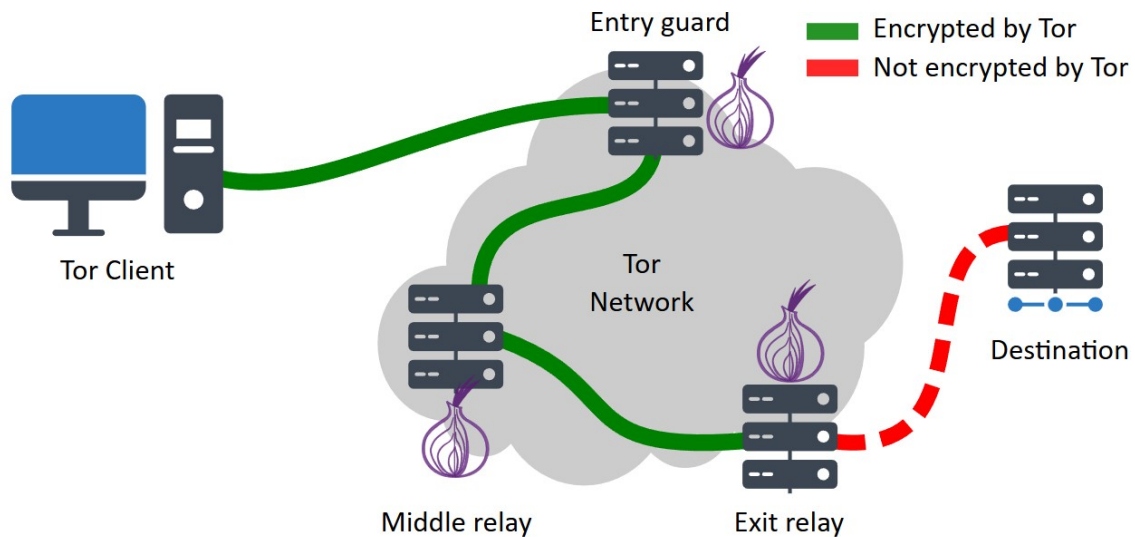


Figure 4.2: How TOR works

include IPsec (89) and WireGuard (90). These protocols work by encapsulating packets and encrypting all of the information within. This provides secure data transfer over an insecure network. (91)

VPNs also allows users to effectively 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. The role of VPNs in personal privacy and censorship circumvention cannot be overstated due to how commonplace the technology has become.

According to SurfShark, a prominent provider, "over 1.6 billion people use VPNs."

(92) Forbes states "Both the availability and usage of VPNs for personal use continue to rise," and this appears accurate. (93)

The Onion Router (TOR) 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." (94)

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. Aside

from granting privacy, 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. (95)

TOR Bridges Previously, we have mentioned TOR relays and how three of them make up a circuit. The first hop over a relay is an important one; TOR bridges act as the first relay in certain circumstance. "Bridges are onion routers in the Tor Network whose IP addresses are not public." (96) Bridges act as a hidden and flexible way to access the TOR network. This allows individuals, (particular in countries where TOR is heavily blocked), to bypass censorship, communicate securely and enhance privacy. For example, TOR bridges have been used to access TOR within China. (97) (98)

Psiphon Psiphon is a "free and open-source Internet censorship circumvention tool that uses a combination of secure communication and obfuscation technologies." (99) During the 2021 Cuban protests, the government shut down several social media sites. This lead to over 1 million protesters using Psiphon as a circumvention method. (100)

Typically, circumvention tools either divert web traffic so it avoids the machines that filter, or disguise the traffic as that that does not need to be filtered. Psiphon state on their website that "the Psiphon app has the ability to relay traffic through various communication protocols. It attempts to connect through different protocols until a connection is made." (99) As previously mentioned, this technology has proved its value in combating internet censorship.

5 | Methodology

5.1 Collecting Data: OONI

5.1.1 Background

Released under the TOR project in 2012, the Open Observatory of Network Interference (OONI) is a non-profit open-source software project whose goal is to empower decentralized efforts to document internet censorship worldwide (101). The OONI organization openly publishes measurements and provides a public archive of network interference across the globe. This has produced a database of more than 2.6 billion individual tests. (102)

OONI data has been used extensively by third parties both for research and advocacy. Examples include the Freedom on the Net 2024 (103) report, iMAP reports (104) by Sinar, and Access Now's annual #KeepItOn 2023 Report. (105) (106) Based on these high profile endorsements and the wealth of data available, OONI is a perfect tool to measure internet censorship.

5.1.2 OONI Probe

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.

5.1.3 Virtual Machine

In order to gather ground truth, a virtual machine in Israel is used to run OONI command line interface locally. This machine is accessed via SSH. These technologies will be discussed further below. The chosen provider, *interhost.co.il*, has a strong track record regarding data integrity and security; however, further scrutiny is necessary. (107)

These tools were audited for any security and privacy concerns and the results are below. Tools like CloudFlare's TCP reset dashboard (108) gave further insight on instances of throttling, blocking or otherwise. In order to expand the web connectivity tests included with OONI, resources like Citizen Lab's sensitive domain list were included. (109)

5.2 Ground Truth: Ireland & Israel

To gather ground truth in Ireland, the OONI probe Command Line Interface was installed and ran over a two week period. Since the CLI is not natively supported on Windows, a Unix-based operating system was flashed onto a Raspberry Pi 5, which served as a dedicated headless testing device. The device was accessed remotely via SSH, enabling the automation and management of tests.

A similar process was used to remotely control the Israeli VM. This allowed for side-by-side running of tests and comparison of results.



Figure 5.1: Headless Raspberry Pi 5

```

Raspberry Pi Imager v1.8.5
[engine] dnsllookup://www.gamku.com... ok
[engine] using control: [{Address:https://5.th.ooni
.org Type:https Front:} {Address:https://6.th.ooni
.org Type:https Front:} {Address:https://d33digs9kp
ic5.cloudfront.net Type:cloudfront Front:d33digs9kp
qic5.cloudfront.net}]
[engine] control for https://www.gamku.com/...
[engine] sessionresolver: lookup 6.th.ooni.org usin
g system://... started
[engine] sessionresolver: lookup 6.th.ooni.org usin
g system://... ok
[engine] httpsDialer: [#166] tactic '{"Address":"18
.157.235.1","InitialDelay":8,"Port":"443","SNI":"6
.th.ooni.org","VerifyHostname":"6.th.ooni.org"}' is
ready
[engine] httpsDialer: [#166] TCPConnect 18.157.235
.1:443... started
[engine] httpsDialer: [#166] TCPConnect 18.157.235
.1:443... ok
[engine] httpsDialer: [#166] TLSHandshake with 18.1
57.235.1:443 SNI=6.th.ooni.org ALPN=[h2 http/1.1]...
started
[engine] control for https://www.gamku.com/... ok
[engine] httpsDialer: [#166] TLSHandshake with 18.1
57.235.1:443 SNI=6.th.ooni.org ALPN=[h2 http/1.1]...
interrupted
[engine] DNS analysis result: inconsistent
[engine] TCP/TLS endpoints: 8/2 reachable
[engine] GET https://www.gamku.com/...

[engine] ooniprobe-engine/v3.23.0 7e9a978d541a891165
4e6389a0e3d2b916c6b19 dirty=false gol.21.11
[engine] iplookup: using cloudflare
[engine] sessionresolver: lookup www.cloudflare.com u
sing system://... started
[engine] sessionresolver: lookup api.ooni.io using ht
tp3://dns.google/dns-query... started
2025/04/06 12:27:48 connection doesn't allow setting
of send buffer size. Not a net.UDPConn? See https:/
/github.com/quic-go/quic-go/wiki/UDP-Buffer-Sizes for
details.
[engine] sessionresolver: lookup api.ooni.io using ht
tp3://dns.google/dns-query... ok
[engine] httpsDialer: [#2] tactic '{"Address":"162.55
.247.208","InitialDelay":8,"Port":"443","SNI":"api.oo
ni.io","VerifyHostname":"api.ooni.io"}' is ready
[engine] httpsDialer: [#2] TCPConnect 162.55.247.208:
443... started
[engine] httpsDialer: [#2] TCPConnect 162.55.247.208:
443... ok
[engine] httpsDialer: [#2] TLSHandshake with 162.55.2
47.208:443 SNI=api.ooni.io ALPN=[h2 http/1.1]... star
ted
[engine] httpsDialer: [#2] TLSHandshake with 162.55.2
47.208:443 SNI=api.ooni.io ALPN=[h2 http/1.1]... ok
[engine] httpsDialer: [#2] TLSVerifyCertificateChain
api.ooni.io... started
[engine] httpsDialer: [#2] TLSVerifyCertificateChain
api.ooni.io... ok
[engine] session: using probe services: {Address:http
s://api.ooni.io Type:https Front:}

```

Figure 5.2: Running OONI tests over SSH

5.2.1 Description of OONI Tests

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 (110).

Circumvention Test

The circumvention test is used to check whether 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 (111). 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 (112).

The Tor Test (113) 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 (114).

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 (115). This test was contributed by the LEAP collective (116).

Instant Messaging Test

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

The Whatsapp test attempts to determine if there is any interference or blockage of its App or Web Interface. To do this, the OONI probe attempts to perform an HTTP GET request TCP Connection, and DNS lookup to WhatsApp's endpoints. These include the endpoints used by the WhatsApp mobile app, the registration service, and the web interface (117). 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 (118).

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 (119). 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 Autonomous System Number* (AS32934) (120).

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 (121).

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 (122). A DNS query to `uptime.signal.org` is also performed to check if the backend servers are down (123).

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 (124).

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 (125).

5.2.2 Data Collection and Transparency

All results from OONI Probe tests are automatically sent to OONI's servers and published on the OONI explorer. This transparency ensures that anyone can explore the measurements for themselves. OONI aggregates measurements by country, time, and type of test. It highlights "confirmed" cases of blocking when there is strong enough certainty in the test result, but it also publishes anomalies that might be considered false positives.

The OONI team also work to release comparative analysis and real-time alerts for significant internet censorship related events. This would include events such as a sudden surge in social media blockage, or a complete drop off of internet traffic in certain areas. The OONI Measurement Aggregation Toolkit (MAT) can be used to visualize these events and potentially identify emerging trends.

5.3 Privacy & Security Concerns

The following section contains information on 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.

5.3.1 OONI Probe

OONI's 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."* (126). 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.

5.3.2 SSH & Virtual Machine

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 (127).

5.3.3 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 (128, 129). 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 (130). 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 (131), 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.

6 | Results

6.1 Overview

Tests were conducted over a two week period between 31/03/25 and 13/04/25. Seven days worth of tests were exported from both machines for comparison and analysis. The results are discussed below, with pertinent tables included in the Appendix section. In comparison, the OONI database that is publicly available was analysed for the dates 13/03/25 to 13/04/25.

It is important to recognize that, particularly in the case of Israel, different individuals may experience censorship of the Internet to varying degrees. The research focuses on replicating the experience of the average Israeli living in Tel Aviv. Having previously discussed the Gaza Strip, it is clear that the user experience varies greatly between the two areas. Further research may look at comparing Internet censorship experienced internally in Israel, but that is outside the scope of this work.

In the following section, the relevant context regarding the network conditions while gathering ground truth will be discussed. Having previously highlighted the varying levels at which internet censorship can be conducted, let us now define the specific network characteristics under which the OONI probe was run for both countries.

6.1.1 Network Environment Context: Ireland

As mentioned, the OONI CLI probe is running on a Raspberry Pi 5 connected to a home residential network over WiFi. The provider is Virgin Media (AS12388), registered under Liberty Global B.V. ISP (AS6830).

Details regarding the operating system flashed to the Raspberry Pi and packages required for this are illustrated below in the 'Guide to Replicating Results.'

6.1.2 Network Environment Context: Israel

Ground truth gathering in Israel was done using a virtual machine as described in the section on methodology. The virtual machine is operates within a data center hosted by O.M.C. COMPUTERS & COMMUNICATIONS LTD (AS44709), downstream of its owner Kamatera Inc. (AS36007). This differs from the residential network that is being tested in Ireland.

6.2 Website Connectivity Tests

6.2.1 Ground Truth via SSH

6.2.2 Native Website Connectivity Tests

This section details the results of the daily web connectivity tests performed using the command *ooniprobe run*.

Table 6.1: Summary of Tested vs. Blocked Websites by Country (Native to OONI)

Country	Tested	Blocked
Ireland	1695	25
Israel	1695	16

6.2.3 my-websites.txt

This file contains the additional 170 website connectivity tests I wished to conduct. The list was compiled with Griff Steinman, and additional tests relating to Israel were added. The contents can be found within the Appendix section. Below is a summary of the results from the daily running of this additional web connectivity test suite.

Table 6.2: Summary of Blocked vs. Unblocked Websites by Country (my-websites)

Country	Unblocked	Blocked
Ireland	151	19
Israel	155	15

The following figure illustrates the blocking methods for the additional web connectivity tests. See Appendix section for a more detailed breakdown of positive results for each locale.

Table 6.3: Distribution of Blocking Methods Detected in Ireland & Israel

Blocking Method	Ireland	Israel
TCP/IP	15	13
DNS	1	1
HTTP	1	1
Error/Failure	3	0

Table 6.4: Blocked Websites by Category and Country

Category	Total Websites Tested	Ireland	Israel
Uncategorized	34	4	4
Piracy / Streaming / File Sharing	21	6	4
News / Media	34	1	0
Adult Content	21	0	0
Creative / Educational / Misc	15	1	1
General / National Services	19	1	1
Streaming / Social Media	9	0	0
Religious	5	2	2
VoIP / Communication	4	1	0
Gambling	2	1	1
Email/Privacy Tools	3	1	0
Adult / Alcohol	2	1	1
LGBTQ+	1	1	1
AI / Technology	1	0	0

6.2.4 Investigating Aljazeera.com

Upon initial testing of Aljazeera blocking in Israel, it was surprising to see no evidence of blocking. To investigate further it was decided that the content of the site should be examined and a variety of URLs belonging to it should be tested.

Particular attention was given to articles that were critical of Israel.

The file sample_aljazeeraurls.txt contains 100 URLs for articles hosted on <https://aljazeera.com>. Below are some helpful commands used to obtain the sitemap and extract URLs for testing. Wget was used to examine the contents of the web page, and the following was observed.

Despite preconceived notions, Aljazeera and its articles were not found to be blocked on AS44709. Reasons for this will be explored in the coming chapter.

```
    window.dispatchEvent(otready)
  }</script><script data-gtm-script>!function(e,t,a,n,r){e[n]=e[n]||[],e[n].push({"gtm.start":(>
<p>Rogue had apparently mistaken Sodhi for being an Arab.</p><div class="recommended recommended__loading"><d>
<p>Prosecutors argued Sodhi's murder on 15 September, 2001 was fuelled by racism and hate, and carried out by
<p>But defence attorneys said Rogue was mentally ill and pushed over the edge by the attacks.</p>
<p>The jury deliberated for six hours, in the case which attracted international attention.</p>
<p>An appeal to the decision is mandatory.</p>
<p><strong>Indian complaint</strong></p>
<table align="right" border="0"><tbody><tr><td align="middle"><p></p>
<p align="left"><strong>"The jury brought justice back to our family. They brought the truth in front of the
<p>Lakhwinder Singh Sodhi,<br/>victim's brother</p><p></p>
<p></p></td></tr></tbody></table>
<p>The shooting prompted India to call on the US government to take steps to prevent assaults on Sikhs living>
<p>Sodhi, 49, who came to the US in 1988 from a small village in Punjab. </p>
<p>He was one of several Sikhs attacked in America after 11 September 2001 after apparently being mistaken as>
<p>Rogue, who still faces sentencing on other charges stemming from two other shootings of people of Afghani>
<p>Lakhwinder Singh Sodhi said he was relieved that more than two years of waiting was over and that his brot>
<p>"The jury brought justice back to our family," he told Reuters. </p>
<p>"They brought the truth in front of the whole world and showed that we are all Americans."</p>
</div><div class="article-source">Source<!-- -->: <!-- -->Reuters</div></main><hr/><div class="loading-cards">
<script type="text/javascript">window.__APOLLO_STATE__="eyJN2>
<script type="text/javascript">window.__FEATURES__="eyJhcmFia>

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_/ Go To Line M-E Redo
```

Figure 6.1: wget showing aljazeera.com content

As seen above, I was able to see unblocked content from the site. Within Appendix, one can find a sample of articles being tested.

6.2.5 Public OONI Database

In this section, the OONI database will be explored. As mentioned previously the period to be considered is 13/03/25 to 13/04/25. Below are screenshots of all web connectivity tests conducted in Ireland and Israel for these dates.

Web Connectivity Test

Ireland

OK Confirmed Anomaly Failure

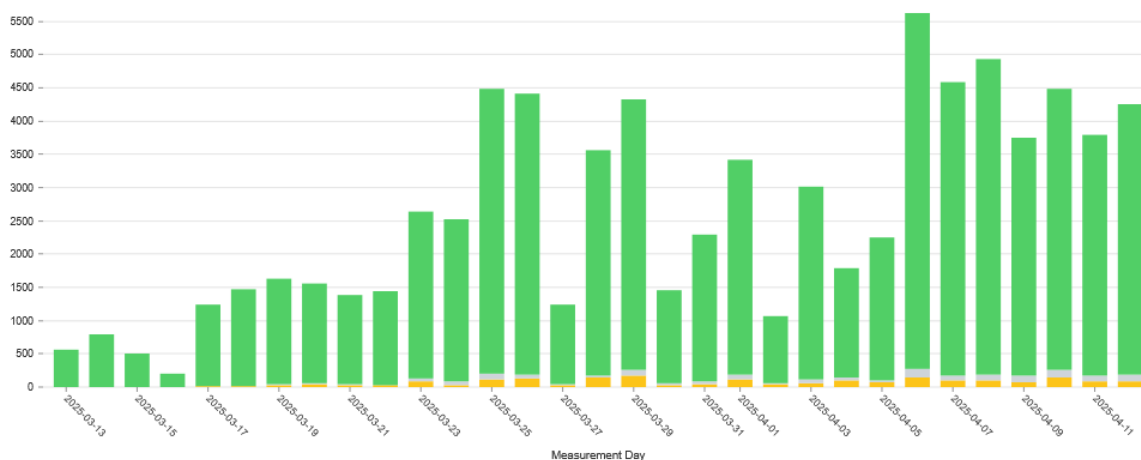


Figure 6.2: Irish OONI Database Web connectivity tests 13/03-13/04

Web Connectivity Test

Israel

OK Confirmed Anomaly Failure

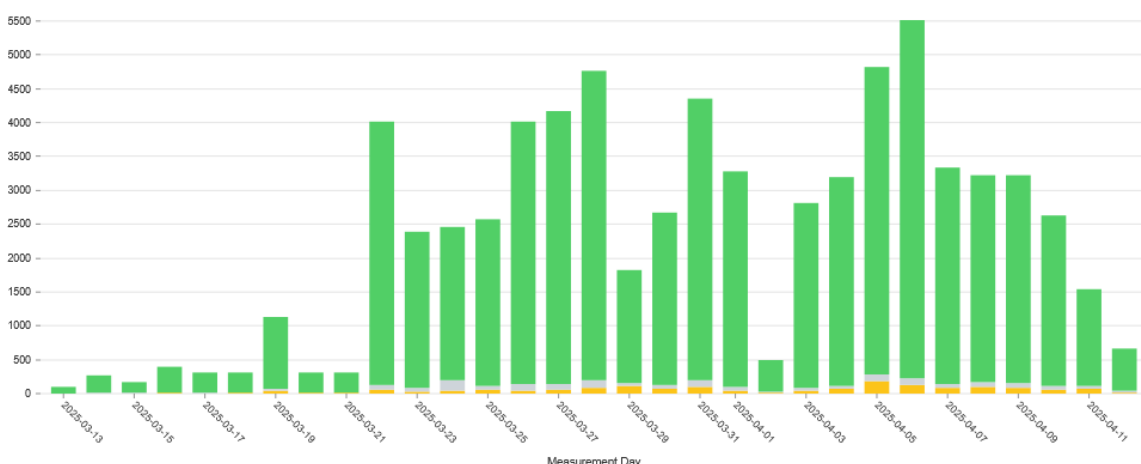


Figure 6.3: Israel OONI Database Web connectivity tests 13/03-13/04

Further insight into this data can be seen through the proceeding table that documents a daily averages.

Table 6.5: Website Blocking based on Public OONI Data

	Ireland	Israel
Number of Websites Tested	2603	2299
Number of Successful Connections	2491	2195
Number of Anomalies	67	53
Number of Failures	46	51

By examining the publicly available data on Aljazeera and filtering based on ASN, an interesting picture emerges. There is clear evidence of large scale DNS tampering on certain ASNs, while others go unblocked. Prior to my testing using the VM in Tel Aviv, it was unknown whether O.M.C. COMPUTERS & COMMUNICATIONS LTD (AS44709) was blocking this content.

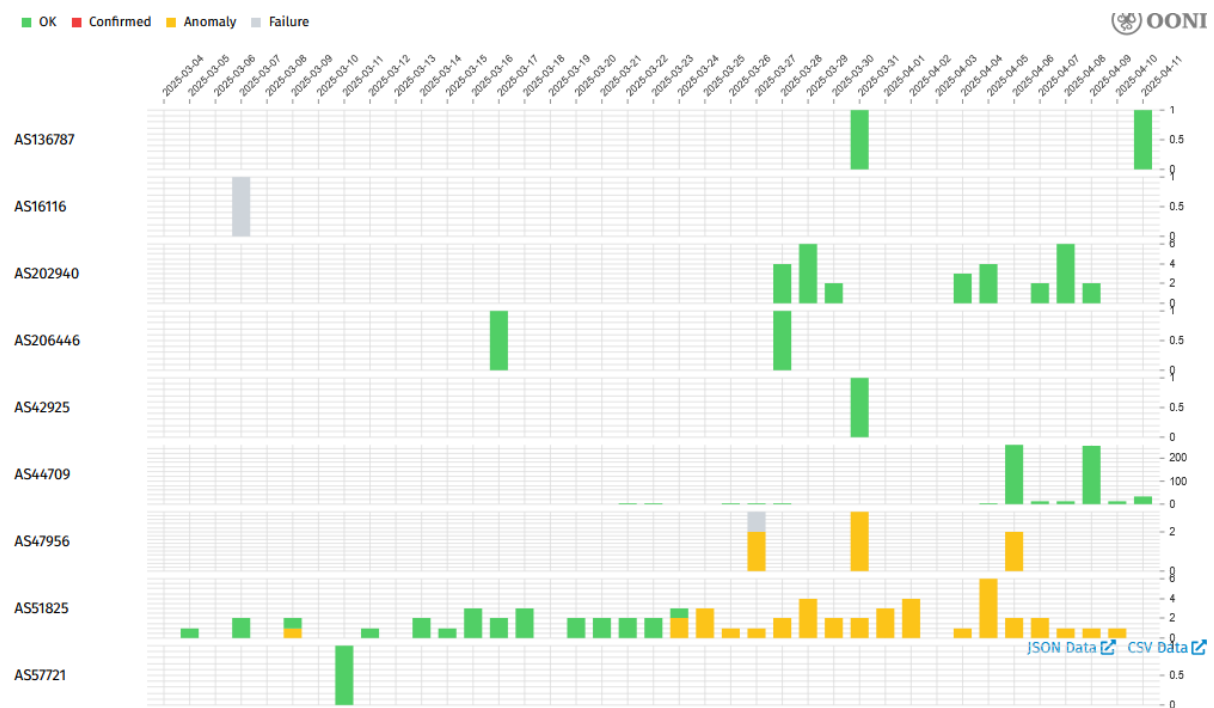


Figure 6.4: OONI data (04/03/2025 - 11/04/2025) showing blocking of Alazeera.com grouped by ASN

6.3 Instant Messaging Tests

By analysing the publicly available OONI data for both countries for the period of interest we can see little evidence of blocking of instant messaging platforms in either country.

6.3.1 Public OONI Database: Ireland

As seen in the below figures, there is little evidence to suggest network interference of instant messaging platforms in Ireland over the period considered.

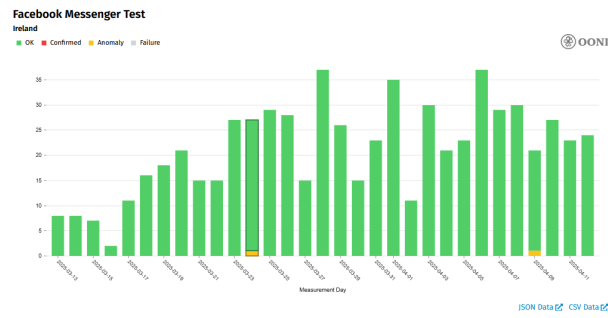


Figure 6.5: Facebook Messenger test results for Ireland 13/03-13/04

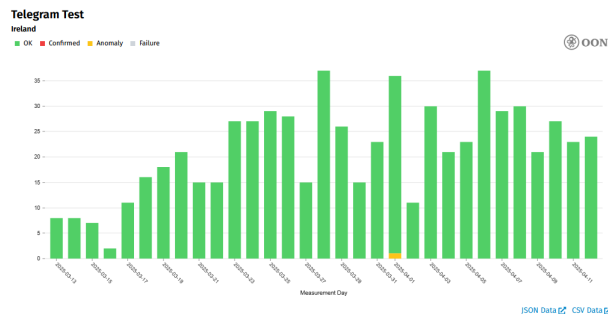


Figure 6.6: Telegram test results for Ireland 13/03-13/04

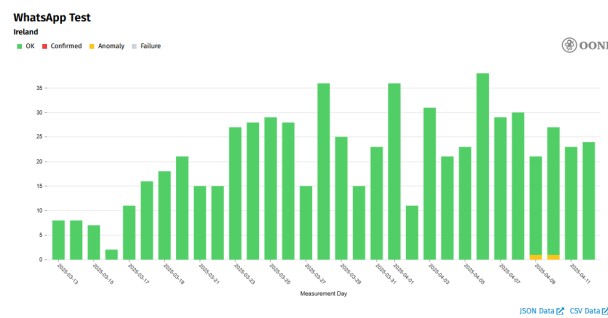


Figure 6.7: WhatsApp test results for Ireland 13/03-13/04

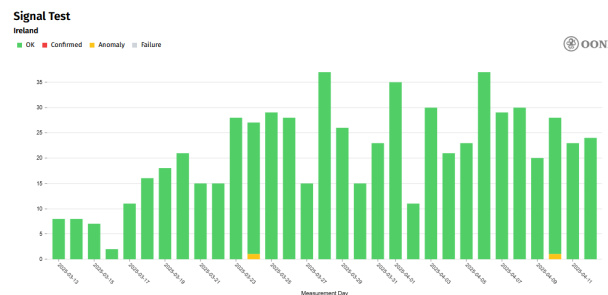


Figure 6.8: Signal test results for Ireland 13/03-13/04

6.3.2 Public OONI Database: Israel

As seen in the below figures, there is little evidence to suggest network interference of instant messaging platforms in Israel over the period considered.

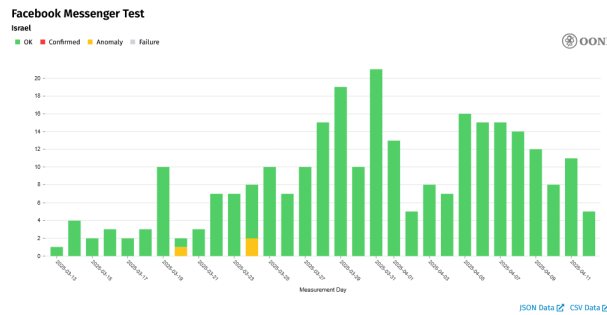


Figure 6.9: Facebook Messenger test results for Israel 13/03-13/04

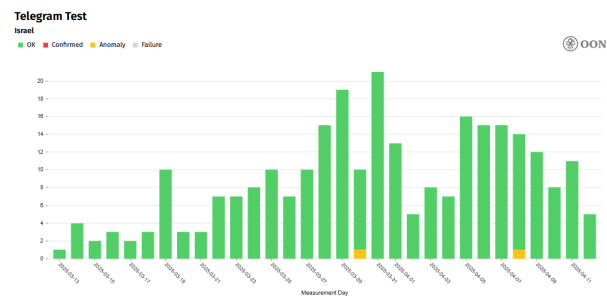


Figure 6.10: Telegram test results for Israel 13/03-13/04

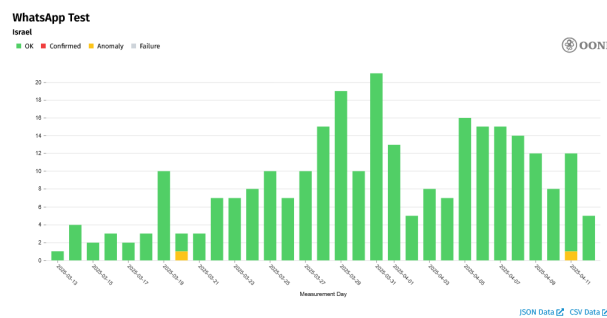


Figure 6.11: WhatsApp test results for Israel 13/03-13/04

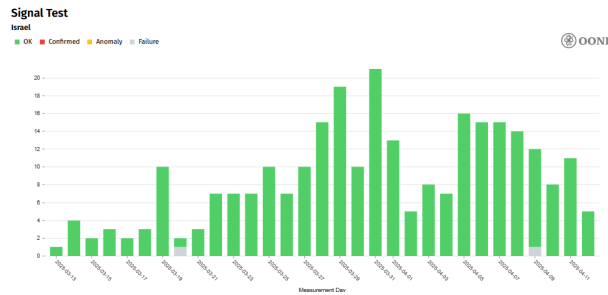


Figure 6.12: Signal test results for Israel 13/03-13/04

6.3.3 Ground Truth via SSH

While running tests locally, no evidence for the blocking of instant messaging platforms was found in either Ireland or Israel. As seen in the above figures, there is little evidence in the OONI database to suggest either country interferes with instant messaging platforms.

6.4 Circumvention Tests

6.4.1 Public OONI Database: Ireland

The majority of circumvention tests go unblocked in Ireland, however, certain ASNs show evidence of blocking. This can be see below.

Ireland Circumvention Test Anomalies Based on data seen in the OONI database, TOR is not blocked by the majority of ASNs in Ireland. However, consistent blocking is seen in some networks. Over the period considered, there were seven instances of TOR being blocked, all attributed to HEAnet (AS 1213).

Psiphon appears to be blocked somewhat consistently on certain ASNs. The results are seen tabulated below, with a focus on ASNs containing anomalies.

Table 6.6: Psiphon Circumvention Anomalies in Ireland

Metric / ASN	Blocked	OK	% Blocked
Total	82	575	12.48%
ASN 1213	57	6	90.48%
ASN 6830	18	271	6.23%
ASN 13280	5	13	27.78%
ASN 9009	1	6	14.29%
ASN 212238	1	0	100.00%
ASN 8075	1	0	100.00%
ASN 15751	1	8	11.11%

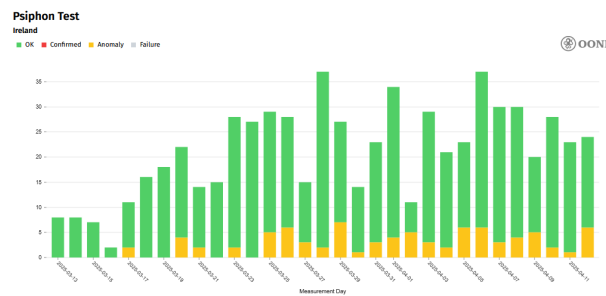


Figure 6.13: Psiphon test results for Ireland 13/03-13/04

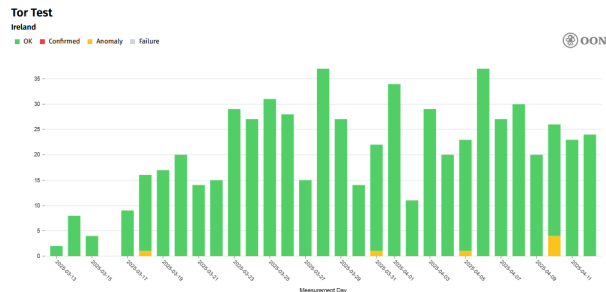


Figure 6.14: TOR test results for Ireland 13/03-13/04

6.4.2 Public OONI Database: Israel

Based on observations of the OONI database over the period of interest, TOR and Psiphon tests are not blocked in Israel. The only evidence of blocking comes from one autonomous system as described below.

Israel Circumvention Test Anomalies ITC NG ltd (AS 202940) was responsible for 25 instances of blocking TOR connections and one instance of blocking Psiphon

connections over the dates examined. This was the only ASN responsible for positive results. These anomalies are tabulated below.

Table 6.7: Circumvention Results in Israel (ASN 202940)

Tool	Blocked (Anomaly)	OK	% Blocked
Psiphon	1	27	3.57%
Tor	25	3	89.29%

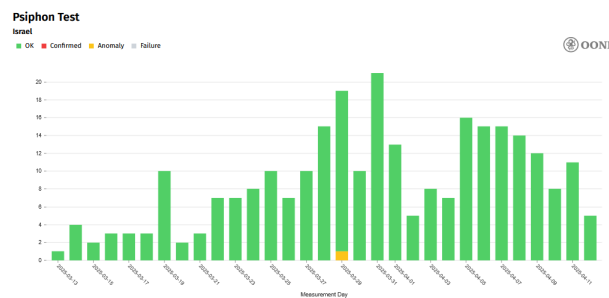


Figure 6.15: Psiphon test results for Israel 13/03-13/04

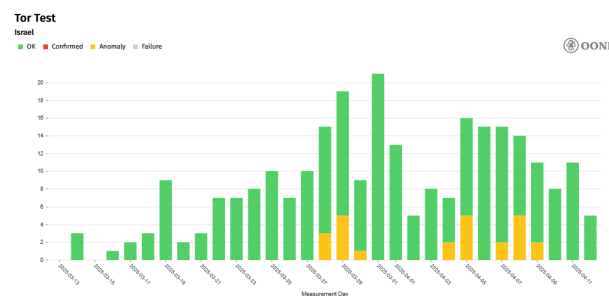


Figure 6.16: TOR test results for Israel 13/03-13/04

6.4.3 Ground Truth via SSH

No evidence for the blocking of TOR or Psiphon was found while running circumvention tests in either locale. This is consistent with the OONI database as in both countries, blocking appears inconsistent and AS specific.

6.5 Middlebox Tests

6.5.1 Public OONI Database: Ireland

In examining the OONI database for HTTP Invalid Request Line tests conducted in Ireland over the period of interest, only a handful of anomalies are observed. Out of the 660 HTTP Invalid Request Line tests conducted there were 5 anomalies. These instances belonged to M247 Europe SRL (AS9009), Vodafone Ireland Limited (AS15502) and Meteor Mobile Communications Limited (AS15751). A breakdown of the anomalies is seen below.

Table 6.8: HTTP Invalid Request Line Test Anomalies in Ireland

ASN	Anomalies	OK
Total	5	660
AS9009	3	4
AS15502	1	103
AS15751	1	9

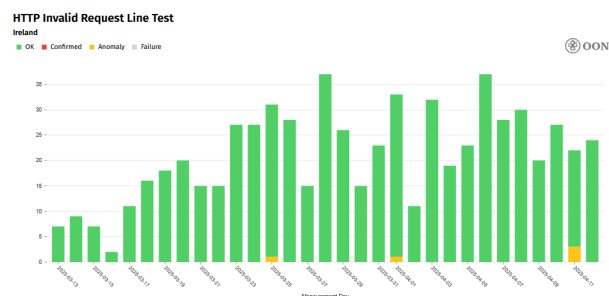


Figure 6.17: HTTP Invalid Request test results for Ireland 13/03-13/04

Irish tests for HTTP Header Field Manipulation were less intriguing with only 6 anomalies over the period of interest. These were attributed to M247 Europe SRL (AS9009) and HEAnet (AS 1213) respectively. A breakdown of these results is seen below.

Table 6.9: HTTP Header Field Manipulation Anomalies in Ireland

ASN	Anomalies	OK	Percentage Anomalous
Total	6	648	0.91%
AS9009	2	1	66.67%
AS1213	4	7	36.36%

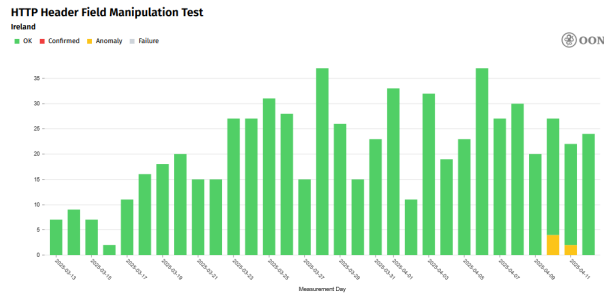


Figure 6.18: HTTP Header Field Manipulation test results for Ireland 13/03-13/04

6.5.2 Public OONI Database: Israel

Only one instance of HTTP a Invalid Request Line anomaly was seen in Israel over the period of interest and belonged to XFone 018 Ltd (AS47956).

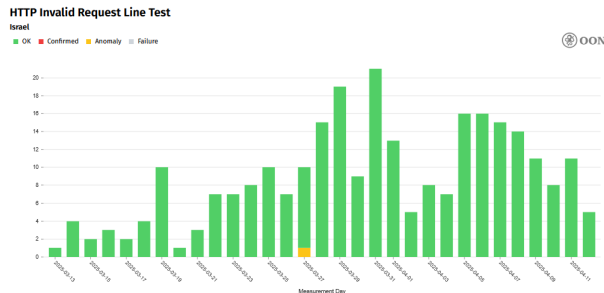


Figure 6.19: HTTP Invalid Request test results for Israel 13/03-13/04

On the other hand, HTTP Header Field Manipulation test results for Israel were quite interesting. Anomalies were attributed to three different ASNs: Cellcom Fixed Line Communication L.P (AS1680), ITC NG ltd (AS202940) and XFone 018 Ltd (AS47956). The breakdown of these results is tabulated below.

Table 6.10: HTTP Header Field Manipulation Anomalies in Israel

ASN	Anomalies	OK	Percentage Anomalous
Total	35	237	12.87%
AS202940	25	4	86.21%
AS1680	9	3	75.00%
AS47956	1	7	12.50%

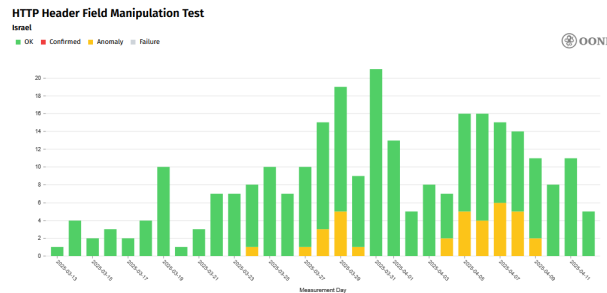


Figure 6.20: HTTP Header Field Manipulation test results for Israel 13/03-13/04

6.5.3 Ground Truth via SSH

Results of running middlebox tests locally in both countries were uninteresting and no evidence of their presense was noted. However, as seen above Cellcom Fixed Line Communication L.P (AS1680) and ITC NG ltd (AS202940) are responsible for a significant number of positive with a majority of measurements showing interference.

6.6 Comparative Analysis: Ireland vs. Israel

6.6.1 Summary: Irish Internet Censorship

6.6.2 Summary: Israeli Internet Censorship

6.6.3

6.7 Guide to Replicating Results

6.7.1 Investigating Aljazeera.com

Below are some commands I found helpful while investigating aljazeera.com.

```
curl https://www.aljazeera.com/ -o aljazeera_homepage.html  
grep -oP '(?<=<h2>).*?(?=</h2>)' aljazeera_homepage.html
```

Figure 6.21: Using curl and grep to scrape URLs for articles

```
sed -i 's#\([^/]\)$#\1/#' aljazeera_urls.txt
```

Figure 6.22: Inserting a dash after each URL, can now be ran with OONI

6.7.2 Raspberry Pi Setup

Operating System The operating system used was the latest available version of Raspberry Pi OS (64-bit) at the time of testing. It was flashed using the Raspberry Pi Imager application over USB.

Raspberry Pi OS (64-bit)

Release date: November 19th 2024

System: 64-bit

Kernel version: 6.6

Debian version: 12 (bookworm)

Packages Installed In order to install the OONI probe CLI, the guide 'Install OONI Probe CLI on Debian/Ubuntu Linux' (132) was followed. The process was similar to that of installing on the Israeli VM. One obstacle faced in both instances were OpenPGP errors. To solve, the permissions for OONI probe had to be updated to bypass PGP signature verification. To do this, `/etc/apt/sources.list.d/ooniprobe.list` was edited to include `'[trusted=yes]'`

A terminal window with a black background and white text. The text reads "gpg: no valid OpenPGP data found" followed by a vertical cursor bar. The word "gpg:" is highlighted in yellow.

```
gpg: no valid OpenPGP data found|
```

Figure 6.23: PGP Error installing CLI

7 | Conclusions

7.1 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. Both countries leverage judicial process to combat pirated media, copyright infringement and otherwise illegal content. Ireland benefits greatly from its membership in the European Union, however this means enforcing GDPR, DSA and more.

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] Digital Rights Ireland. Digital rights ireland.
<https://www.digitalrights.ie/>. Accessed: 2025-03-06.
- [3] 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.
- [4] 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.
- [5] Hannah Ritchie, Edouard Mathieu, Max Roser, and Esteban Ortiz-Ospina.
Internet. *Our World in Data*, 2023. <https://ourworldindata.org/internet>.
- [6] Paul Bischoff. Internet censorship: A map of restrictions by country.
Comparitech, 2025. URL <https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/>.
- [7] Internet History of Ireland. Internet history of ireland, 2025. URL <http://www.internethistory.ie/>. Accessed: 2025-03-22.

- [8] Tech Archives Ireland. Tech archives ireland. URL <https://techarchives.irish/>. Accessed: 2025-03-22.
- [9] TechArchives Irish. Ireland's first computers, 1956–69, 2025. URL <https://techarchives.irish/irelands-first-computers-1956-69/>. Accessed: 2025-03-26.
- [10] TechArchives Irish. How the internet came to ireland, 1987–97, 2025. URL <https://techarchives.irish/how-the-internet-came-to-ireland-1987-97/>. Accessed: 2025-03-26.
- [11] Trinity College Dublin, School of Computer Science and Statistics. Tcd-scss-t.20160323.001, 2016. URL <https://treasures.scss.tcd.ie/hardware/TCD-SCSS-T.20160323.001/TCD-SCSS-T.20160323.001.pdf>. Accessed: 2025-03-26.
- [12] Legal Guide Ireland. Electronic documents, 2025. URL <https://legalguide.ie/electronic-documents/>. Accessed: 2025-03-26.
- [13] The Irish Times. Legislation strong on privacy for internet users. 2001. URL <https://www.irishtimes.com/business/legislation-strong-on-privacy-for-internet-users-1.291390>. Accessed: 2025-03-26.
- [14] Citizens Information. How eu law works, 2025. URL <https://www.citizensinformation.ie/en/government-in-ireland/european-government/eu-law/how-eu-law-works/#4022f6>.
- [15] European Union. How eu policy is decided, 2025. URL https://european-union.europa.eu/institutions-law-budget/law/how-eu-policy-decided_en.

- [16] GDPR-Info. General data protection regulation (gdpr), 2025. URL <https://gdpr-info.eu/>.
- [17] Trade Department of Enterprise and Employment. Digital services act, 2025. URL <https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/eu-digital-single-market-aspects/digital-services-act/>.
- [18] Irish Statute Book. Act 2 of 2024 (enacted), 2024. URL <https://www.irishstatutebook.ie/eli/2024/act/2/enacted/en/html>.
- [19] Trade Department of Enterprise and Employment. Summary of articles of directive (eu) 2019/790, 2019. URL <https://enterprise.gov.ie/en/consultations/consultations-files/summary-articles-of-directive-eu-2019-790.pdf>. Accessed: 2025-03-28.
- [20] Court of Justice of the European Union. Google spain sl v. agencia española de protección de datos (2014), 2014. URL <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131>.
- [21] European Union. Directive (eu) 2019/790 on copyright in the digital single market, 2019. URL <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790>.
- [22] European Data Protection Board. €2.6 billion euro fine for facebook due to gdpr breach, 2023. URL https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.
- [23] Statista. Meta fines from eu and dpc, 2023. URL <https://www.statista.com/statistics/1192794/meta-fines-from-eu-and-dpc/>.
- [24] European Commission. Eu digital services act: Twitter under scrutiny, 2023. URL https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

- [25] Business Human Rights Resource Centre. Eu: Twitter could face legal consequences if it fails to comply with eu regulations, 2023. URL <https://www.business-humanrights.org/en/latest-news/eu-twitter-could-face-legal-consequences-if-it-fails-to-comply-with-eu-regulations>
- [26] International Trade Administration. Ireland - digital economy, 2025. URL <https://www.trade.gov/country-commercial-guides/ireland-digital-economy>.
- [27] Revenue Commissioners. Corporation tax - basis of charge, 2025. URL <https://www.revenue.ie/en/companies-and-charities/corporation-tax-for-companies/corporation-tax/basis-of-charge.aspx>.
- [28] Archyde. Us commerce secretary demands end to ireland's tax practices – insights from the irish times, 2025. URL <https://www.archyde.com/us-commerce-secretary-demands-end-to-irelands-tax-practices-insights-from-the-irish-times>
- [29] Government of Ireland. Defamation act 2009, 2009. URL <https://www.irishstatutebook.ie/eli/2009/act/31/enacted/en/print>.
- [30] Government of Ireland. Communications act 2011, 2011. URL <https://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/html>.
- [31] Government of Ireland. Online safety and media regulation act 2022, 2022. URL <https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/>.
- [32] The Journal. High court orders isps to block the pirate bay in ireland, 2013. URL <https://www.thejournal.ie/high-court-order-block-pirate-bay-948503-Jun2013/>.
- [33] SimilarWeb. The pirate bay - traffic overview and statistics, 2025. URL <https://www.similarweb.com/website/thepiratebay.org/#overview>.

- [34] European Commission. Faqs - eu sanctions on russian media, 2025. URL https://finance.ec.europa.eu/document/download/99b8682b-4f41-4d78-9756-7087d0a93965_en?filename=faqs-sanctions-russia-media_en.pdf. Accessed: 2025-03-28.
- [35] The Journal. Russian news channel rt banned in the eu and ireland, 2022. URL <https://www.thejournal.ie/russian-news-channel-rt-banned-eu-ireland-5698500-Mar2022/>.
- [36] Euronews. Russia blocks scores of european media outlets in latest retaliatory pushback, 2024. URL <https://www.euronews.com/my-europe/2024/06/25/russia-blocks-scores-of-european-media-outlets-in-latest-retaliatory-pushback>.
- [37] European Commission. Press release: Eu action on online content and media regulation, 2024. URL https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227.
- [38] 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>.
- [39] 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.
- [40] 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.
- [41] 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.
- [42] Internet Monitor. Israel country profile. *Berkman Klein Center Research Publication*, (2012-1):1–5, 2012. URL <https://thenetmonitor.org/country-profiles/isr>.
- [43] 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.
- [44] DataReportal. Digital 2024: Israel, 2024. URL <https://datareportal.com/reports/digital-2024-israel>. Accessed: 2025-03-09.
- [45] Reporters Without Borders. Israel. *Reporters Without Borders Country Profile*, 2023. URL <https://rsf.org/en/country/israel>.
- [46] 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.
- [47] 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.
- [48] 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>.

- [49] 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.
- [50] 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-rep> Accessed: 2025-03-09.
- [51] 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.
- [52] Israel Defense Forces (IDF). Official idf statement on x (formerly twitter), 2024.
- [53] 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>.
- [54] 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>.
- [55] Eric Rescorla. HTTP Over TLS. RFC 2818, May 2000. URL <https://www.rfc-editor.org/info/rfc2818>.
- [56] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018. URL <https://www.rfc-editor.org/info/rfc8446>.

- [57] 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.
- [58] Stanisław Tosza. Internet service providers as law enforcers and adjudicators. a public role of private actors. *Computer Law Security Review*, 43:105614, 2021. ISSN 2212-473X. doi: <https://doi.org/10.1016/j.clsr.2021.105614>. URL <https://www.sciencedirect.com/science/article/pii/S026736492100087X>.
- [59] Nikolaos Chatzis, Georgios Smaragdakis, and Anja Feldmann. On the importance of internet exchange points for today’s internet ecosystem. *CoRR*, abs/1307.5264, 2013. URL <http://arxiv.org/abs/1307.5264>.
- [60] Mohammad Zubair Ahmad and Ratan Guha. Internet exchange points and internet routing. In *2011 19th IEEE International Conference on Network Protocols*, pages 292–294, 2011. doi: 10.1109/ICNP.2011.6089065.
- [61] Josh Karlin, Stephanie Forrest, and Jennifer Rexford. Nation-state routing: Censorship, wiretapping, and BGP. *CoRR*, abs/0903.3218, 2009. URL <http://arxiv.org/abs/0903.3218>.
- [62] Zittrain. The future of the internet and how to stop it, 2013. URL <https://futureoftheinternet.org/wp-content/uploads/sites/12/2013/06/ZittrainTheFutureoftheInternet.pdf>. Accessed: 2025-03-31.
- [63] Jonathan Zittrain. Internet points of control. 2003.
- [64] NordVPN. How nordvpn protects the privacy of its customers, 2024. URL <https://nordvpn.com/blog/how-nordvpn-protects-the-privacy-of-its-customers/?msocid=3031a4f209f3667a1367b051088c67fe>. Accessed: 2025-04-07.

- [65] 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.
- [66] Jon Postel. Internet protocol. Request for Comments 791, RFC Editor, September 1981. URL <https://www.rfc-editor.org/rfc/rfc791>. Accessed: 2025-03-31.
- [67] Internet blocking and democracy, 2025. URL https://www.inthemis.fr/ressources/Internet_blocking_and_Democracy.pdf. Accessed: 2025-03-31.
- [68] Violence & internet shutdowns in 2023: the worst year on record - Access Now — accessnow.org. <https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2023/#:~:text=By%20almost%20every%20measure%2C%202023,rights%20of%20millions%20of%20people>. [Accessed 15-03-2025].
- [69] Carolyn Tackett Méabh Maguire Zach Rosson, Felicia Anthonio. Lives on hold: internet shutdowns in 2024 - Access Now — accessnow.org. <https://www.accessnow.org/internet-shutdowns-2024/>. [Accessed 15-03-2025].
- [70] Patil. A method to evade keyword based censorship, 2014. URL https://mavmatrix.uta.edu/context/cse_theses/article/1227/type/native/viewcontent.
- [71] National Security Archive. The tiananmen square, 1989: The declassified history, 2001. URL <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB16/>. Accessed: 2025-04-07.
- [72] Louisa Lim. *The People's Republic of Amnesia: Tiananmen Revisited*. Oxford University Press, New York, 2014.

- [73] Jay Allen. Report: Tokyo university used "tiananmen square" keyword to block chinese admissions, 2023. URL <https://unseenjapan.medium.com/report-tokyo-university-used-tiananmen-square-keyword-to-block-chinese-admissions>. Accessed: 2025-04-07.
- [74] 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.
- [75] Deep packet inspection (dpi) market size. *Business Research Insights*.
- [76] ProtonVPN. Are vpns illegal?, 2025. URL <https://protonvpn.com/blog/are-vpns-illegal/>.
- [77] Rajdeep Bhanot and Rahul Hans. A review and comparative analysis of various encryption algorithms. *International Journal of Security and Its Applications*, 9(4):289–306, 2015.
- [78] Cloudflare. What is end-to-end encryption?, 2025. URL <https://www.cloudflare.com/en-gb/learning/privacy/what-is-end-to-end-encryption/>.
- [79] Sherali Zeadally, Ashok Kumar Das, and Nicolas Sklavos. Cryptographic technologies and protocol standards for internet of things. *Internet of Things*, 14: 100075, 2021. ISSN 2542-6605. doi: <https://doi.org/10.1016/j.iot.2019.100075>. URL <https://www.sciencedirect.com/science/article/pii/S2542660519301799>.
- [80] François-Xavier Standaert. Introduction to side-channel attacks, 2005. URL <https://perso.uclouvain.be/fstandae/PUBLIS/42.pdf>.
- [81] Internet Society. Tls basics, 2025. URL <https://www.internetsociety.org/deploy360/tls/basics/>.

- [82] Cloudflare. What happens in a tls handshake?, 2025. URL <https://www.cloudflare.com/en-gb/learning/ssl/what-happens-in-a-tls-handshake/>.
- [83] BitsBook. Chapter 5 - network security, 2008. URL <https://www.bitsbook.com/wp-content/uploads/2008/12/chapter5.pdf>.
- [84] Federal Bureau of Investigation (FBI). Lawful access, 2025. URL <https://www.fbi.gov/about/mission/lawful-access>.
- [85] National Security Agency (NSA). National security agency official website, 2025. URL <https://www.nsa.gov/>.
- [86] Cloudflare. How the nsa may have put a backdoor in rsa’s cryptography: A technical primer, 2025. URL <https://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/>.
- [87] Bruce Schneier. The strange story of the nsa’s backdoor in the $\text{dual}_{\text{e}}\text{c}_{\text{d}}\text{r}\text{bg}$, 2007. URL.
- Microsoft. Point to point tunneling protocol (pptp) specification, 2025. URL https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-ptpt/32e8cf6d-2e0d-4843-8dc0-a4934e16e1f5.
- Yaron Sheffer, Paul Hoffman, and Adrian Farrel. Isec and ike document roadmap. Technical Report RFC 6071, RFC Editor, February 2011. URL <https://www.rfc-editor.org/rfc/rfc6071>.
- Pirate. Wireguard documentation, 2025. URL <https://github.com/pirate/wireguard-docs>.
- Jassim Hadi Alhassan et al. The vital role of vpn in making secure connection over internet world. *ResearchGate*, 2020. URL https://www.researchgate.net/publication/340336829_The_vital_role_of_VPN_in_making_secure_connection_over_internet_world.

Surfshark. Global vpn usage statistics: Over 1.6 billion users worldwide, 2025. URL [https://surfshark.com/blog/vpn-users#:~:](https://surfshark.com/blog/vpn-users#:~:text=We%20estimate%20that%20over%201.6%20billion%20people%20use,countries%20where%20VPN%20market%20penetration%20is%20above%2010%25.)

[text=We%20estimate%20that%20over%201.6%20billion%20people%20use,countries%20where%20VPN%20market%20penetration%20is%20above%2010%25.](https://surfshark.com/blog/vpn-users#:~:text=We%20estimate%20that%20over%201.6%20billion%20people%20use,countries%20where%20VPN%20market%20penetration%20is%20above%2010%25.)

Forbes Advisor. Vpn statistics: Usage, market trends, and security insights, 2025. URL <https://www.forbes.com/advisor/business/vpn-statistics/>.

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.

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

Srdjan Matic, Carmela Troncoso, Juan Caballero, et al. Dissecting tor bridges: a security evaluation of their private and public infrastructures. In *Network and Distributed System Security Symposium*, pages 1–15. The Internet Society, 2017.

Arun Dunna, Ciarán O’Brien, and Phillipa Gill. Analyzing china’s blocking of unpublished tor bridges. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, 2018.

Cyberly. What should i do if tor browser is blocked in my country?, 2025. URL <https://www.cyberly.org/en/what-should-i-do-if-tor-browser-is-blocked-in-my-country/index.html>.

Psiphon. Psiphon guide, 2025. URL <https://psiphon.ca/en/psiphon-guide.html>.

Bloomberg. Over 1 million cubans evade internet curbs with u.s.-backed tech, 2021. URL <https://www.bloomberg.com/news/articles/2021-07-16/>

over-1-million-cubans-evade-internet-curbs-with-u-s-backed-tech?srnd=premium&sref=yLCixKPR.

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

Open Observatory of Network Interference (OONI). Ooni explorer, 2025. URL <https://explorer.ooni.org/>. Accessed: 2025-03-22.

Freedom on the net 2024: The struggle for trust online, 2024. URL <https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online>.

Elizaveta Yachmeneva. imap 2024: State of internet censorship in 9 countries, 2024. URL <https://ooni.org/post/2024-imap-9-research-reports-southeast-asia/>.

Zach Rosson, Felicia Anthonio, and Carolyn Tackett. Shrinking democracy, growing violence: Internet shutdowns in 2023, 2024. URL <https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf>.

Maria Xynou. Year in review: Ooni in 2024, 2025. URL <https://ooni.org/post/2024-year-in-review/#research-reports>.

Interhost Networks Ltd. Interhost | tier 1 hosting servers & network solutions in israel, 2025. URL <https://interhost.co.il/>.

Cloudflare. Cloudflare blog - policy, 2025. URL <https://blog.cloudflare.com/tag/policy/>.

Citizen Lab. Citizen lab test lists repository, 2025. URL <https://github.com/citizenlab/test-lists>. GitHub repository.

Open Observatory of Network Interference. Web Connectivity Test. <https://ooni.org/nettest/web-connectivity/>, . [Accessed 02-03-2025].

Open Observatory of Network Interference. Psiphon Test. <https://ooni.org/nettest/psiphon/>, . [Accessed 02-03-2025].

Open Observatory of Network Interference. Psiphon Test GitHub.

<https://github.com/ooni/spec/blob/master/nettests/ts-015-psiphon.md>, .
[Accessed 02-03-2025].

Open Observatory of Network Interference. Tor Test.
<https://ooni.org/nettest/tor/>, . [Accessed 02-03-2025].

Open Observatory of Network Interference. Tor Test GitHub.
<https://github.com/ooni/spec/blob/master/nettests/ts-023-tor.md>, .
[Accessed 02-03-2025].

Open Observatory of Network Interference. RiseUp VPN Test GitHub.
<https://github.com/ooni/spec/blob/master/nettests/ts-026-riseupvpn.md>, .
[Accessed 02-03-2025].

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

Open Observatory of Network Interference. WhatsApp Test.
<https://ooni.org/nettest/whatsapp/>, . [Accessed 02-03-2025].

Open Observatory of Network Interference. WhatsApp Test GitHub.
<https://github.com/ooni/spec/blob/master/nettests/ts-018-whatsapp.md>, .
[Accessed 02-03-2025].

Open Observatory of Network Interference. Facebook Messenger Test.
<https://ooni.org/nettest/facebook-messenger/>, . [Accessed 02-03-2025].

Open Observatory of Network Interference. FaceBook Test. <https://github.com/ooni/spec/blob/master/nettests/ts-019-facebook-messenger.md>, .
[Accessed 02-03-2025].

Open Observatory of Network Interference. Telegram Test GitHub.
<https://github.com/ooni/spec/blob/master/nettests/ts-020-telegram.md>, .
[Accessed 02-03-2025].

Open Observatory of Network Interference. Signal Test.

<https://ooni.org/nettest/signal>, . [Accessed 02-03-2025].

Open Observatory of Network Interference. Signal Test GitHub.

<https://github.com/ooni/spec/blob/master/nettests/ts-029-signal.md>, .
[Accessed 02-03-2025].

Open Observatory of Network Interference. HTTP Header Field Manipulation Test.

<https://ooni.org/nettest/http-header-field-manipulation/>, . [Accessed
02-03-2025].

Open Observatory of Network Interference. HTTP Invalid Request Line Test.

<https://ooni.org/nettest/http-invalid-request-line/>, . [Accessed
02-03-2025].

Open Observatory of Network Interference (OONI). Risks of using ooni, 2025. URL

<https://ooni.org/about/risks/>. Accessed: 2025-03-22.

OpenSSH Project. Openssh manual, 2025. URL

<https://www.openssh.com/manual.html>. Accessed: 2025-03-22.

Encyclopædia Britannica. Julian assange biography, 2025. URL

<https://www.britannica.com/biography/Julian-Assange>. Accessed:
2025-03-22.

Encyclopædia Britannica. Edward snowden biography, 2025. URL

<https://www.britannica.com/biography/Edward-Snowden>. Accessed:
2025-03-22.

MIFTAH. Freedom of press violations 2000-2003, 2003. URL

<https://miftah.org/Display.cfm?DocId=4450&CategoryId=8>. Accessed:
2025-03-22.

Unknown. Israel war and censorship. *ScienceDirect*, 2025. URL

<https://www.sciencedirect.com/science/article/pii/S0363811117300231>.
Accessed: 2025-03-22.

Open Observatory of Network Interference (OONI). OONI Probe CLI Installation Guide for Ubuntu/Debian, 2024. URL

<https://ooni.org/install/cli/ubuntu-debian>.

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.

A1.2 Website Connectivity Tests: my-websites.txt

- `https://pbc.ps`
- `https://adultfriendfinder.com`
- `https://use-application-dns.net`
- `https://mgid.com`
- `https://exoclick.com`
- `https://rawa.org`
- `https://hamas.com`
- `https://coronavirus.app/`
- `https://chika.aangat.lahat.computer/`
- `https://censored.tv/`

- <https://outlook.live.com/>
- <http://kremlin.ru/>
- <https://kk.wikipedia.org/>
- <https://ru.wiktionary.org/>
- <https://ru.wikisource.org/>
- <https://pl.wikipedia.org/>
- <https://www.gov.ie/en/campaigns/c36c85-covid-19-coronavirus/>
- <https://ircz.de/>
- <https://thepiratebay.org/>
- <https://he.wikipedia.org/>
- <https://he.wikisource.org/>
- <https://he.wiktionary.org/>
- <http://www.phenoelit.org/>
- <https://www.pc2call.com/>
- <https://dnsleaktest.com/>
- <http://www.eurogrand.com/>
- <http://www.utorrent.com/>
- <http://www.socom.mil/>
- <https://www.rarbg.to/>
- <https://www.mp3.com/>
- <http://www.bittornado.com/>
- <http://www.bitcomet.com/>
- <https://thepiratebay.org/>
- <https://libgen.me/>
- <https://libgen.life/>
- <https://kickasstorrents.to/>
- <https://kat.am/>
- <http://www.oic-oci.org/>
- <http://www.islamdoor.com/>
- <https://www.icconnecthere.com/>
- <https://www.bittorrent.com/>
- <https://app.simplelogin.io/>
- <http://abpr2.railfan.net/>
- <https://www.xroxy.com/>
- <https://www.secfirst.org/>
- <http://www.queernet.org/>
- <https://secfirst.org/>
- <https://1.1.1.1/>
- <https://www.gamku.com/>
- <https://www.onlinearabicasino.com/>
- <http://www.absinth.com/>
- <https://www.literotica.com/>
- <https://www.iasj.net/>

- <https://nazarene.org/>
- <http://www.on-instant.com/>
- <http://www.maillinator.com/>
- <http://www.euthanasia.cc/>
- <http://www.blogeasy.com/>
- <http://alhikmae.com/>
- <https://www.jsf.mil/>
- <https://www.rte.ie/>
- <https://www.chatgpt.com/>
- <https://www.independent.ie/>
- <https://www.dailymail.co.uk/>
- <https://www.bbc.com/>
- <https://www.donedeal.ie/>
- <https://www.yahoo.com/>
- <https://www.daft.ie/>
- <https://www.rip.ie/>
- <https://www.irishtimes.com/>
- <https://www.tiktok.com/>
- <https://www.irishtimes.com/>
- <https://www.theguardian.com/>
- <https://www.aib.ie/>
- <https://www.sky.com/>
- <https://www.thejournal.ie/>
- <https://www.news.sky.com/>
- <https://www.nytimes.com/>
- <https://www.thesun.ie/>
- <https://www.met.ie/>
- <https://www.skysports.com/>
- <https://www.dublinlive.ie/>
- <https://www.boards.ie/>
- <https://www.bbc.co.uk/>
- <https://www.irishmirror.ie/>
- <https://www.xvideos.com/>
- <https://www.imdb.com/>
- <https://www.breakingnews.ie/>
- <https://www.galwaybeo.ie/>
- <https://www.lekmanga.net/>
- <https://www.shabakaty.com/>
- <https://www.kurdcinama.com/>
- <https://www.xhamster.com/>
- <https://www.reddit.com/>
- <https://www xnxx.com/>
- <https://www.kurdsutitle.net/>
- <https://www.like-manga.net/>

- <https://www.topcinema.cam/>
- <https://www.telegram.org/>
- <https://www.egydead.fyi/>
- <https://www.arabshentai.com/>
- <https://www.uptodown.com/>
- <https://www.beenar.net/>
- <https://www xnxx-arabic.com/>
- <https://www.witanime.cyou/>
- <https://www.dailymotion.com/>
- <https://www.lodynet.io/>
- <https://www.weather.com/>
- <https://www.hentaislayer.net/>
- <https://www.live.com/>
- <https://www.xhexperience.xyz/>
- <https://www.theporndude.com/>
- <https://www.xvideos-ar.com/>
- <https://www.azoramoon.com/>
- <https://www.kisskh.co/>
- <https://www.kurdfilm.krd/>
- <https://www.arabx.cam/>
- <https://www.sexalarab.com/>
- <https://www.netflix.com/>
- <https://www.discord.com/>
- <https://www.twitch.tv/>
- <https://www.chess.com/>
- <https://www.tumblr.com/>
- <https://www.deviantart.com/>
- <https://www.wattpad.com/>
- <https://www.omegle.com/>
- <https://www.lichess.org/>
- <https://www.spankbang.com/>
- <https://www.bilibili.com/>
- <https://www.redtube.com/>
- <https://www.9gag.com/>
- <https://www.onlyfans.com/>
- <https://www.fanfiction.net/>
- <https://www.artstation.com/>
- <https://www.furaffinity.net/>
- <https://www.poki.com/>
- <https://www.vk.com/>
- <https://www.creepypasta.com/>
- <https://www.zoro.to/>
- <https://www.youporn.com/>
- <https://www.etsy.com/>

- <https://www.vimeo.com/>
- <https://www.pixiv.net/>
- <https://www.rule34.xxx/>
- <https://www.redgifs.com/>
- <https://www.stripchat.com/>
- <https://www.opera.com/>
- <https://www.wikipedia.com/>
- <https://www.foxnews.com/>
- <https://www.porn.com/>
- <https://www.russia.tv/>
- <https://www.rt.com/>
- <https://www.beeg.com/>
- <https://www.4chan.org/>
- <https://www.crunchyroll.com/>
- <https://www.mozilla.org/>

A1.2.1 my-websites Results: Ireland

Blocking Method	Websites
TCP/IP	http://www.socom.mil https://www.mp3.com http://www.bittornado.com https://libgen.life http://www.oic-oci.org https://doh.centraleu.pi-dns.com/dns-query?... https://im0-tub-com.yandex.net/... https://www.xroxy.com http://www.queernet.org https://www.gamku.com https://www.onlinearabiccasinno.com https://www.iasj.net https://www.shabakaty.com http://alhikmae.com
DNS	https://thepiratebay.org https://kickasstorrents.to https://www.icconnecthere.com https://www.rt.com
HTTP	http://www.euthanasia.cc

A1.2.2 my-websites Results: Israel

Blocking Method	Websites
TCP/IP	http://www.socom.mil https://www.mp3.com http://www.bittornado.com https://libgen.life http://www.oic-oci.org https://doh.centraleu.pi-dns.com/dns-query?dns=q80BAAABAAAAAAAAA3d3 https://im0-tub-com.yandex.net/i?id=462f375c96139f1e41d919b44be2d78 https://www.xroxy.com http://www.queernet.org https://www.onlinearabiccasino.com https://www.iasj.net http://alhikmae.com https://www.shabakaty.com
DNS	https://www.gamku.com
HTTP	http://www.euthanasia.cc

A1.3 sample_aljazeeraurls.txt

- <https://www.aljazeera.com/news/liveblog/2022/10/16/ukraine-russia-live-news-russian-forces-repel-ukraine-advances/>
- <https://www.aljazeera.com/economy/2023/10/27/shifting-politics-make-india-a-hotbed-for-israel-hamas-war-misinformation/>
- <https://www.aljazeera.com/economy/2022/10/10/what-a-us-recession-would-mean-for-the-world/>

- <https://www.aljazeera.com/economy/2021/10/11/energy-crunch-qatar-says-lng-production-maxed-out/>
- <https://www.aljazeera.com/economy/2006/12/15/made-in-china-worrying-the-us/>
- <https://www.aljazeera.com/economy/2009/10/14/video-russian-pensioners-struggle/>
- <https://www.aljazeera.com/economy/2009/10/20/video-lebanon-firms-invest-in-iraq/>
- <https://www.aljazeera.com/economy/2014/10/12/israeli-blockade-cripples-gazas-economy/>
- <https://www.aljazeera.com/economy/2024/10/10/td-bank-pleads-guilty-to-us-charges-faces-business-restrictions/>
- <https://www.aljazeera.com/economy/2024/10/11/boeing-to-cut-10-workforce-delay-777x-delivery-as-strike-takes-toll/>
- <https://www.aljazeera.com/economy/2024/10/11/indias-ratan-tata-the-man-who-knew-how-to-think-big-and-bold/>
- <https://www.aljazeera.com/economy/2024/10/11/indonesia-eyes-hefty-tariffs-on-china-as-businesses-decry-cheap-imports/>
- <https://www.aljazeera.com/economy/2024/10/11/taiwan-says-four-employees-of-apple-supplier-foxconn-arrested-in-china/>
- <https://www.aljazeera.com/economy/2024/10/11/teslas-robotaxi-event-was-long-on-musk-promises-short-on-details/>
- <https://www.aljazeera.com/economy/2024/10/14/acting-us-labour-secretary-to-meet-with-boeing-and-union-to-end-impasse/>
- <https://www.aljazeera.com/economy/2024/10/14/poorest-countries-in-worst-financial-shape-since-two-thousand-six-world-bank-say>

- <https://www.aljazeera.com/economy/2024/10/15/air-taxi-growth-demands-efficient-vertiports-and-traffic-control-systems/>
- <https://www.aljazeera.com/gallery/liveblog/2024/6/4/israels-war-on-gaza-live-pressure-mounts-on-israel-hamas-to-cease-fire/>
- <https://www.aljazeera.com/news/liveblog/2022/10/10/several-explosions-heard-in-ukraine-capital-kyiv/>
- <https://www.aljazeera.com/news/liveblog/2022/10/11/russia-ukraine-live-news-more-strikes-hit-zaporizhzhia/>
- <https://www.aljazeera.com/news/liveblog/2022/10/12/russia-ukraine-live-news-biden-doubts-use-of-nuclear-weapons/>
- <https://www.aljazeera.com/news/liveblog/2022/10/13/jan-6-panel-live-news-us-committee-holds-9th-public-hearing/>
- <https://www.aljazeera.com/news/liveblog/2022/10/13/ukraine-russia-live-news-kyiv-area-hit-by-kamikaze/>
- <https://www.aljazeera.com/news/liveblog/2022/10/14/russia-ukraine-live-news-ukraine-retook-75-kherson-settlements/>
- <https://www.aljazeera.com/news/liveblog/2022/10/15/russia-ukraine-live-news-shelling-fire-at-russian-fuel-depot/>
- <https://www.aljazeera.com/news/liveblog/2022/10/16/la-liga-real-madrid-vs-barcelona-as-it-happened/>
- <https://www.aljazeera.com/economy/longform/2022/12/22/the-protests-that-exposed-cracks-in-chinas-middle-class-dream/>
- <https://www.aljazeera.com/economy/longform/2023/11/24/a-fire-two-deaths-and-the-business-of-elder-care-in-india/>
- <https://www.aljazeera.com/economy/longform/2023/7/12/sri-lankas-fishermen-face-double-whammy-of-climate-and-economy-3/>

- [https://www.aljazeera.com/economy/longform/2024/4/20/
when-will-our-good-days-come-the-mumbai-cook-voting-in-indias-elections/](https://www.aljazeera.com/economy/longform/2024/4/20/when-will-our-good-days-come-the-mumbai-cook-voting-in-indias-elections/)
- [https://www.aljazeera.com/economy/longform/2024/4/24/
parallel-economy-how-russia-is-defying-the-wests-boycott/](https://www.aljazeera.com/economy/longform/2024/4/24/parallel-economy-how-russia-is-defying-the-wests-boycott/)
- [https://www.aljazeera.com/economy/longform/2024/5/2/
after-years-of-decline-a-new-generation-of-organised-labour-rises-in-us/](https://www.aljazeera.com/economy/longform/2024/5/2/after-years-of-decline-a-new-generation-of-organised-labour-rises-in-us/)
- [https://www.aljazeera.com/economy/longform/2024/6/11/
the-future-is-dark-inside-the-brazilian-businesses-shattered-by-floods/](https://www.aljazeera.com/economy/longform/2024/6/11/the-future-is-dark-inside-the-brazilian-businesses-shattered-by-floods/)
- [https://www.aljazeera.com/features/longform/2021/11/16/
snatched-away-the-indigenous-women-taken-on-the-highway-of-tears/](https://www.aljazeera.com/features/longform/2021/11/16/snatched-away-the-indigenous-women-taken-on-the-highway-of-tears/)
- [https://www.aljazeera.com/features/longform/2021/11/19/
after-cop26-letdown-can-indias-gen-z-climate-warriors-prevail/](https://www.aljazeera.com/features/longform/2021/11/19/after-cop26-letdown-can-indias-gen-z-climate-warriors-prevail/)
- [https://www.aljazeera.com/features/longform/2021/11/29/
hunted-how-indigenous-women-are-disappearing-in-canada/](https://www.aljazeera.com/features/longform/2021/11/29/hunted-how-indigenous-women-are-disappearing-in-canada/)