Internet Monitoring Action Project

iMAP 2024 Internet Censorship Report: Executive Summary

Siti Nurliza Samsudin (Sinar Project) and **Numan Afifi** (Sinar Project)

Published/Produced by **Sinar Project**
team@sinarproject.org
https://sinarproject.org

About iMAP

The Internet Monitoring Action Project (iMAP) aims to establish regional and in-country networks that monitor network interference and restrictions to the freedom of expression online in 9 countries: Myanmar, Cambodia, Hong Kong, India, Indonesia, Malaysia, Philippines, Thailand, and Vietnam. Sinar Project works with national digital rights partners in these ten countries. The project is done via Open Observatory Network Interference (OONI) detection and reporting systems, and it involves the maintenance of test lists and the collection and analysis of measurements.

More information is available at imap.sinarproject.org. Any enquiries and suggestions about this report can be directed to team@sinarproject.org

How to use this report

This executive summary aims to provide an overview of the state of internet censorship in the nine countries covered under iMAP as a region. It highlights the overall trend of internet censorship, which includes the blocking of websites, instant messaging apps, circumvention tools, and network tampering, its similarities and differences across the nine countries in the region, and key events that happened during the coverage period that could potentially affect the trend of internet censorship.

This report is separated into the following sections:

- Executive Summary
  - This section explains the purpose of carrying out the study into the state of internet censorship and provides a general overview of socio-political situations across the nine countries.
- Key findings in the region
  - This section provides a general takeaway on the blocking of websites, internet censorship during elections, and a summary of findings across different categories of websites: gambling, news media, pornography, political criticism, social networking, terrorism and militants, and government websites. Charts and graphs are available here for visualisation.
- Contribute to the study
  - This section is created to help readers understand how they could contribute to the study and gather evidence of internet censorship.
- Annex: Methodology
  - Here the readers will find how the data is collected, measured and analysed for the purpose of iMAP 2024 country reports.

This executive summary is a good starting point for reference to gather a general understanding of what is being affected by internet censorship in the ten countries. Our target audience includes researchers working on digital rights or network interference who are searching for ideas and materials for further research, digital rights defenders or civil society organisations looking for materials to support their advocacy work, and journalists seeking to uncover internet censorship, among others.

Recommendations to the audience:

- Learn about supporting evidence related to internet censorship in Malaysia by reviewing research and case studies.
- Understand the latest developments of internet censorship in the country, in terms of methods of blockings and the websites affected by censorship.
- Support or advocate for changes in laws and policies to improve internet freedom in Malaysia.
- Take action and get involved by spreading awareness, signing petitions, or joining initiatives that fight against internet censorship.

The data collected relies on test lists that usually include some websites that are known to be blocked. The list does not reflect the complete list of blocked websites, and the discovery of blocked websites is dependent on which websites are tested.

Abbreviations

ALDR	Alcohol and Drugs
ANON	Anonymization and Circumvention tools
ASN	Autonomous System Number
COMT	Communication Tools
CTRL	Control Content
CULTR	Culture
DNS	Domain Name System
COMM	E-commerce
ECON	Economics
ENV	Environment
FILE	File-sharing
GMB	Gambling
GAME	Gaming
GOVT	Government
HACK	Hacking Tools
HATE	Hate Speech
HOST	Hosting and Blogging Platforms
HUMR	Human Rights Issues
HTTP	Hypertext Transfer Protocol
IGO	Intergovernmental Organisations
ICCPR	International Covenant on Civil and Political Rights
iMAP	Internet Monitoring Action Project
IP	Internet Protocol
ISP	Internet Service Provider
MMED	Media Sharing
MISC	Miscellaneous Content
NEWS	News Media
DATE	Online Dating
OONI	Open Observatory Network Interference

Table of Contents

Executive Summary

Purpose of the study

The purpose of the Internet Monitoring Action Project (iMAP) State of Internet Censorship Country Report is to understand whether and to what extent internet censorship events occurred through the collection and analysis of network measurements in 9 countries: Cambodia, Hong Kong (China), India, Indonesia, Malaysia, Myanmar, Philippines, Thailand, and Vietnam during the testing period from 1 July 2023 to 30 June 2024. In the 2022 edition, we included Timor-Leste in the study. However, it was only a one-off research.

The iMAP State of Internet Censorship Country Report covers the findings of network measurements collected through the Open Observatory of Network Interference's (OONI) OONI Probe app that measures the blocking of websites, instant messaging apps, circumvention tools and network tampering. The findings highlight the websites, instant messaging apps and circumvention tools confirmed to be blocked, the ASNs with censorship detected and the method of network interference applied. The report also provides background context on the network landscape combined with the latest legal, social and political issues and events which might affect the implementation of internet censorship in the country.

Whilst most information on online censorship is derived mainly from collections of news reports, this study looks to explore further by using the tools developed by the Open Observatory of Network Interference (OONI) that collects and makes available near real-time, detailed data on Internet interference together with the expertise and support from the researchers and country partners to understand the broader extent of internet censorship in the region and the control of the internet by the governments.

Overview of the socio-political situation in the region

Population	Max: 1.4 billion (India) Min: 7.5 million (Hong Kong (China)
Internet penetration (% of the population using the internet)	Max: 98% (Malaysia) Min: 44% (Myanmar)
Mobile subscriptions (per 100 inhabitants)	Max: 292 (Hong Kong (China) Min: 81 (India)
Freedom on the Net ranking (2024)	Partly free (6): • Cambodia • Hong Kong (China) • India • Indonesia • Malaysia • Philippines Not free (3): • Myanmar • Thailand • Vietnam
Religion	Buddhism-majority • Cambodia (98%) • Myanmar (88%) Catholicism-majority: • Philippines (79%) Hinduism-majority • India (80%) Islam-majority: • Indonesia (87%) • Malaysia (64%)
ICCPR Ratification	Yes (7): • Cambodia • Indonesia • India • Philippines • Thailand • Vietnam

	No (3): • Hong Kong (China) • Malaysia • Myanmar

Table: Indicators of the socio-political situation in the region

Overall Country Highlights

Internet freedom remains critically constrained in the countries the project covers, with no country achieving the "free" status. The trend of government-imposed internet regulations that restrict the flow of information and limit digital freedom continues to grow, with particular developments in Cambodia, Hong Kong, Myanmar, and Indonesia marking a significant shift towards increased digital repression. This summary provides a comparative analysis of the political, socio-economic, and legal landscapes affecting internet censorship across ten countries in the region.

Vietnam has strengthened its monitoring of digital spaces under the Communist Party's direction, with laws such as the 2018 Cybersecurity Law and Decree 15/2020/ND-CP targeting "fake news" and dissent. Vietnam's economic growth has brought substantial investment, which stricter regulations and expanded oversight of international platforms like Facebook and Google have accompanied.[1] The government's approach to internet censorship relies on extensive legal provisions that mandate content removal and impose fines, primarily targeting activists and bloggers[2].

In the Philippines, the Marcos administration has made notable strides in media regulation, especially with the SIM Registration Act[3], which mandates mobile identity verification, and the Data Privacy Act 2012, regulating personal data use. The Cybercrime Prevention Act has been used to prosecute journalists, exemplifying ongoing threats to press freedom. Concerns remain about increased government control over content related to national security and red-tagging practices that frame journalists and activists as communist insurgents.[4]

[1] *KIS Vietnam, "Vietnam Passes Cybersecurity Law Despite Privacy Concerns,"* accessed 28 October 2024, https://kisvn.vn/en/vietnam-passes-cybersecurity-law-despite-privacy-concerns/

[2] "*Blogging and the Emerging Media Ecosystem in Vietnam*," accessed 28 October 2024, https://www.viet-studies.net/kinhte/Blogging3ways_CSE_August17.pdf

[3] Official Gazette of the Philippines, "*Republic Act No. 11934*," accessed 28 October 2024, https://www.officialgazette.gov.ph/downloads/2022/10oct/20221010-RA-11934-FRM.pdf

[4] *FORUM-ASIA, "Red Tagging in the Philippines,"* accessed 28 October 2024, https://forum-asia.org/itv-redtagging/

Myanmar has seen internet freedoms nearly disappear under military rule since the 2021 coup, with the military using laws like the Electronic Transactions Law[5] and a new Cybersecurity Bill to prosecute dissidents.[6] Internet shutdowns are common in conflict zones, compounding the displacement crisis affecting over a million citizens. Myanmar's restrictive laws and constant internet censorship have effectively silenced the digital voices of opposition and human rights activists.

Malaysia has implemented the Cybersecurity Bill[7] and the revised Code of Ethics[8] for Journalists, heightening governmental control over digital content. While freedom of expression is constitutionally protected, sections of the Communications and Multimedia Act (CMA) and Sedition Act continue to restrict online speech, especially around politically sensitive topics. Concerns have been raised over potential abuse of powers, especially following new amendments that empower the Malaysian Communications and Multimedia Commission to enforce harsher penalties.

In Indonesia, President Joko Widodo's administration has seen increased use of the Electronic Information and Transactions (ITE) Law[9] to block content under the guise of safeguarding public interest. Recent legal changes have sparked opposition from civil society, highlighting concerns over online surveillance and content removal, particularly around sensitive topics such as the West Papua conflict and the country's rising political dynasties. The Personal Data Protection Law passed in 2022,[10] marks progress in data rights but is tempered by government authority to monitor data under vague national security terms.

[5] Electronic Transactions Law. (2004). https://freeexpressionmyanmar.org/wp-content/uploads/2017/07/Electronic-Transactions-Law-EN.pdf
[6] Gan, A., & See, K. (2022, February 12). Myanmar: The introduction of a prohibition on the use of virtual private networks. *Global Compliance News*. https://www.globalcompliancenews.com/2022/02/12/myanmar-the-introduction-of-a-prohibition-on-the-use-of-virtual-private-networks250122/
[7] Christopher & Lee Ong. (2024, March). *Upcoming Cyber Security Act: What you need to know.* Christopher & Lee Ong. https://www.christopherleeong.com/media/7832/2024_27_03-cybersecurity-bill.pdf
[8] *International Federation of Journalists (IFJ), "Malaysia: Journalism Code of Ethics Should Be Regulated by Media Industry,"* accessed 28 October 2024, https://www.ifj.org/media-centre/news/detail/category/press-releases/article/malaysia-journalism-code-of-ethics-should-be-regulated-by-media-industry.
[9] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, (2008). https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008
[10] Undang-undang tentang Pelindungan Data Pribadi, (2022). https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022

India has enacted several digital censorship laws under the Information Technology (IT) Act, with Section 69A[11] allowing the government to block content in the name of state security. Amendments to the IT Rules in 2023[12] have given rise to a government-run fact-check unit, enabling content takedowns on major platforms. This broad authority has faced significant judicial challenges, including from media groups and individuals, and is seen as a major development in regulating online information.

Hong Kong saw further erosion of internet freedom with the Safeguarding National Security Ordinance in 2024, effectively aligning Hong Kong's digital laws more closely with mainland China's. The law expands the scope of the National Security Law, making offences such as "endangering national security in relation to computers or electronic systems" punishable by up to 20 years in prison. This environment severely restricts freedom of speech online, with broader definitions of sedition applied to those criticising the government.

Cambodia has introduced the National Internet Gateway and the Domain Name Law[13] as part of its digital policy framework. These laws mandate local data storage and monitoring, creating an environment conducive to government censorship. Civil society organisations warn that such frameworks may lead to heightened surveillance and restrictions on journalists, activists, and independent media, especially as the Cambodian government seeks to centralise control over online information.

These countries illustrate a continued shift towards increasing governmental control over digital spaces in Southeast Asia. The rise of data localisation requirements, broader national security laws, and enhanced governmental authority to restrict online content highlight a critical need for ongoing monitoring of internet censorship and advocacy for digital freedoms across the region.

[11] *On the legality and constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* — The Centre for Internet and Society. (2021, June 21). https://cis-india.org/internet-governance/blog/on-the-legality-and-constitutionality-of-the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[12] *Challenge to the IT Rules 2023.* SCC Observer. https://www.scobserver.in/cases/challenge-to-the-it-rules-2023/

[13] Ogden, J. (2023, January 29). *Register .kh Domain Names in Cambodia - Cambodia Begins at 40*. Cambodia Begins at 40. https://www.cambodiabeginsat40.com/?p=41005

Key findings in the region

Blocking of websites

- Newly blocked websites were found in Malaysia, Myanmar, Indonesia, Hong Kong (China), India and Vietnam. In contrast, no new censorship was detected in Thailand, the Philippines, and Cambodia, although website blocking persists in these countries.
- Most websites blocked were related to pornography and gambling; however, news media and political criticism websites were also found to be blocked in all countries.
- Methods of blocking were primarily through DNS tampering, where network providers would serve a block page, 'address not found' error or unknown pages.
- While some countries, like Indonesia and Vietnam, have released official block lists, most government authorities or network providers do not actively notify when they censor critical or non-malicious websites.

Methods of blocking

The most common method of blocking through DNS. Based on OONI data, blocking methods detected by country are as follows:

Blocking method	Countries
DNS	All nine countries
HTTP	Myanmar Thailand India Vietnam
TLS/TCP	Myanmar Vietnam Hong Kong Indonesia India

Table: Methods of blocking by country

In most cases of internet censorship, governments would order network providers to block based on a list of websites. In the iMAP countries, these are mostly only partially available, except for Indonesia which has the TrustPositif list, although it is restricted access only for Indonesians IPs. In India there was one publicly released based on a Right to Information

request, but there were reports where the requests were denied due to national security. Other countries were similar whereby a small list of websites were reported to be blocked through news or CSOs such as Myanmar, Vietnam, Cambodia and Philippines during a specific period. Whereas no public block list has been released in Malaysia and Thailand as of date of writing.

Availability of block list	Countries
Full block list available	Indonesia
Partial block list available	Myanmar India Vietnam Philippines
No block list available	Malaysia Cambodia Thailand

Table: Summary of block lists status

On the other hand, block pages are pages where users will see when they attempt to access a blocked website. These are typically implemented by network providers, and so may differ from each other. The summary of implementation of blockpages by country is as follows:

Implementation of blockpages	Countries
Block pages implemented	National: • Indonesia • Thailand Certain ISPs only: • Vietnam • India • Myanmar • Philippines
No block pages implemented	• Malaysia (previously there was but had been removed) • Cambodia • Hong Kong

Table: Summary of implementation of block pages

Monitoring of Internet Censorship During Elections

During the elections held during the study period, internet censorship was monitored in Cambodia and Indonesia. The findings were as follows:

Country	Period	Findings
Cambodia	July 2023	• The opposition Candlelight Party was disqualified from the elections in May 2023. • Independent news websites that were blocked since February 2023 continued to be blocked during the elections.
Indonesia	May 2023	No censorship related to the elections was reported.

Table: Findings of monitoring of internet censorship during elections covered in the reporting period, July 2023-June 2024

Summary of findings by category

In this section, the analysis will cover the number of domains blocked, domains blocked in more than one country, and blockings by category. More details on the domains blocked or the context of blocking can be found in the specific country reports. Readers should also note the limitations of the website category as not all domains tested with OONI Probe have been categorized, and some of the websites may be miscategorised. There may also be websites that could belong to more than one category, but this was not captured in the data. Additionally, the charts below does not include Hong Kong, as the analysis had been conducted differently.

Gambling

Censorship of gambling websites is the most prevalent in Indonesia, Malaysia and Thailand, whereas in Myanmar and Cambodia there is little censorship detected, as compared to other categories.

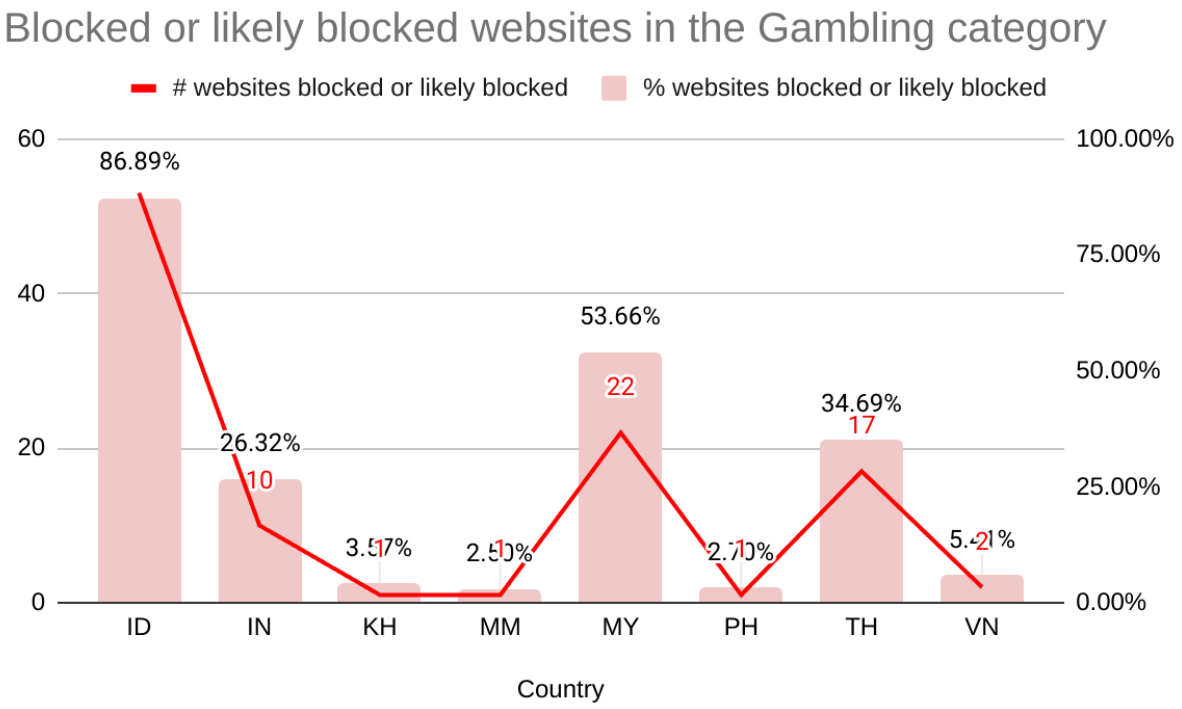

Chart 1: Blocked or likely blocked websites in the Gambling category by country

News Media

Censorship of news media websites continued in iMAP countries, where independent news media is often blocked.

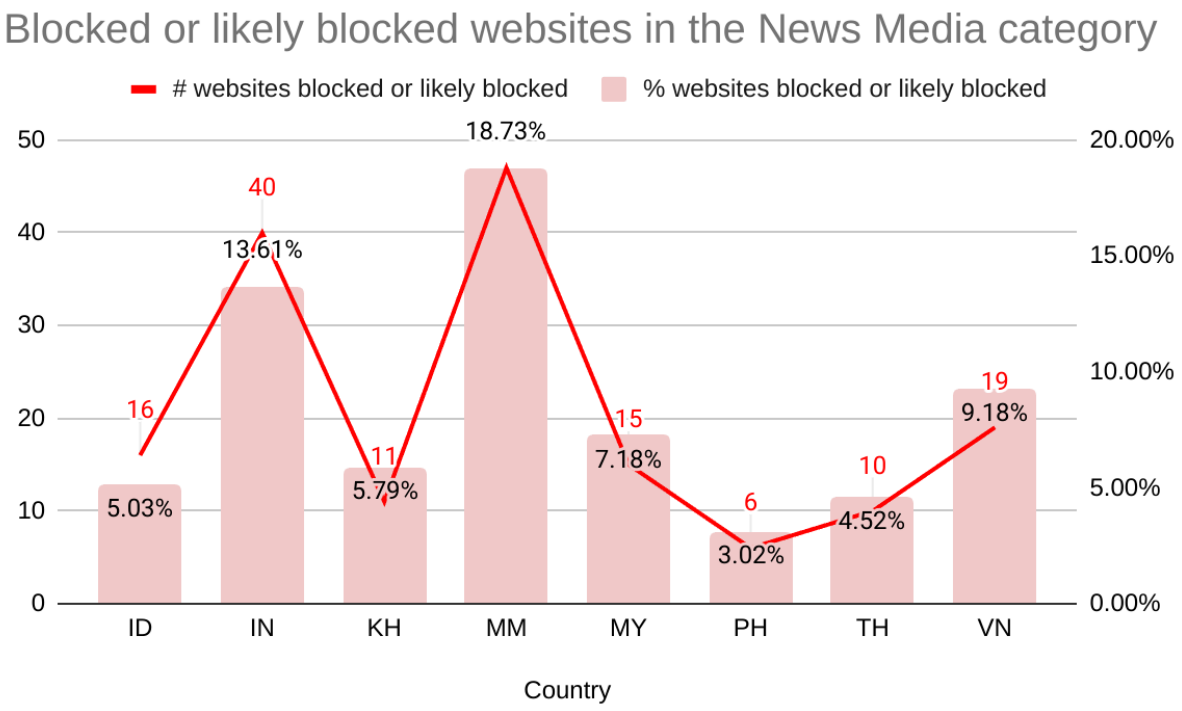

Chart 2: Blocked or likely blocked websites in the News Media category by country

In Myanmar, Athan Myanmar reported that the Ministry of Information (MoI) under the SAC revoked Mekong News' licence on December 24, 2023. After the coup, the military revoked the licences of fifteen media outlets in Myanmar, followed by blocking of their websites.

No.	Media outlets	Date of revoked	URL
1	Mizzima	March 8, 2021	https://eng.mizzima.com
2	DVB	March 8, 2021	https://english.dvb.no
3	Myanmar Now	March 8, 2021	https://myanmar-now.org/en/
4	Khit Thit	March 8, 2021	https://yktnews.com
5	7 Days	March 8, 2021	Not found
6	Tachileik News Agency	April 29, 2021	https://www.tachileik.net/mm
7	Myitkyina News Journal	April 29, 2021	https://www.myitkyinanewsjournal.com

No.	Media outlets	Date of revoked	URL
8	74 Media	April 29, 2021	https://www.the74media.com
9	Zayar Times	July 1, 2021	Not found

Table: Media outlets whose licenses were revoked in Myanmar and their respective websites.

In Malaysia, independent news websites were found newly blocked during the period of coverage, such as Utusan TV and Malaysia Now, as well as Guang Ming Daily, although only for 2 days.

In Cambodia, independent news websites such as VOD and Cambodia Daily had been blocked since February 2023 and were noticeably still blocked during the period of coverage.

LGBTQI+

Blocking of websites in the LGBT category were prevalent in Indonesia, Malaysia, India, Myanmar, Thailand and Vietnam. In particular, the website of the dating app Grindr was blocked in Malaysia during the period of coverage. It was also found blocked in Indonesia.

In Thailand, the websites found blocked (gayzeed.com, gboysiam.com and gthai.net) appear outdated and inactive, suggesting their continued blocking may reflect legacy censorship practices rather than recent enforcement actions.

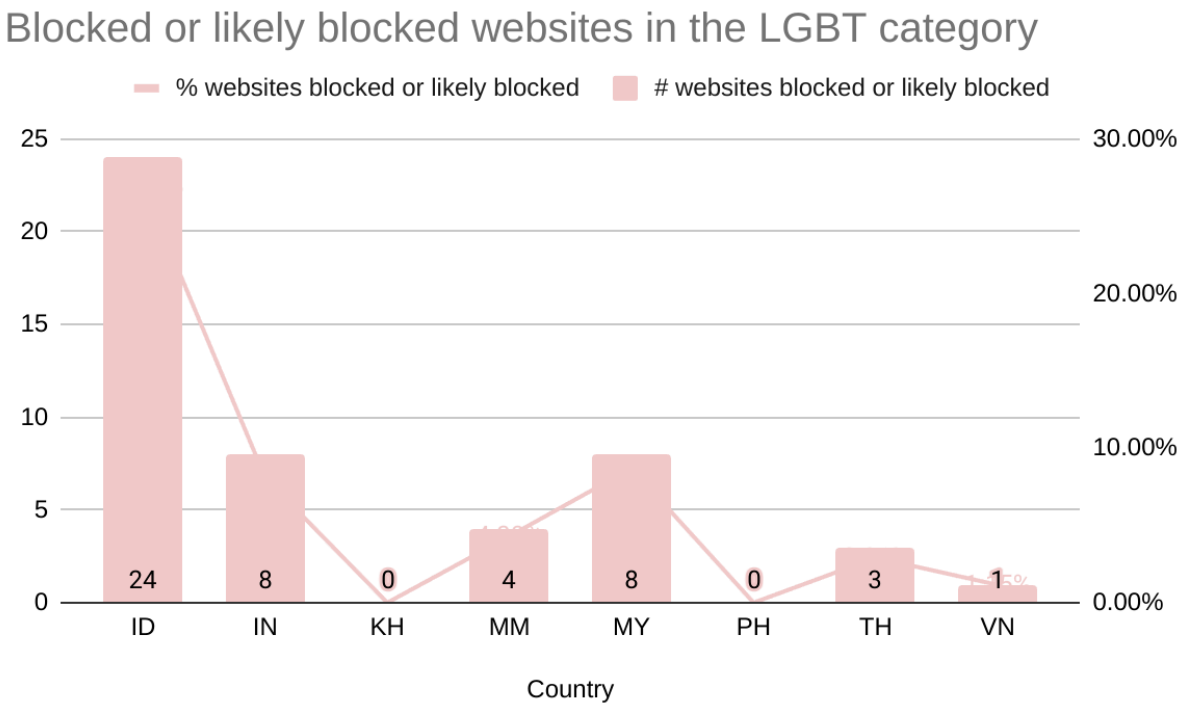

Chart 3: Blocked or likely blocked websites in the LGBT category by country

Pornography

Blocking of pornography websites were the most prevalent in India, Indonesia, Thailand and Malaysia. Among the websites that were found blocked in multiple countries were:

- www.xvideos.com
- pornhub.com
- www.pornhub.com
- www.youporn.com
- xhamster.com
- beeg.com
- www.sex.com
- www.xnxx.com
- www.bravoporn.com
- www.gotgayporn.com
- www.playboy.com
- www.wetplace.com
- asianleak.com
- hotgaylist.com
- onlyfans.com
- rule34.xxx

- www.89.com
- www.fuckingfreemovies.com
- www.hustler.com
- xvideos.com
- youjizz.com

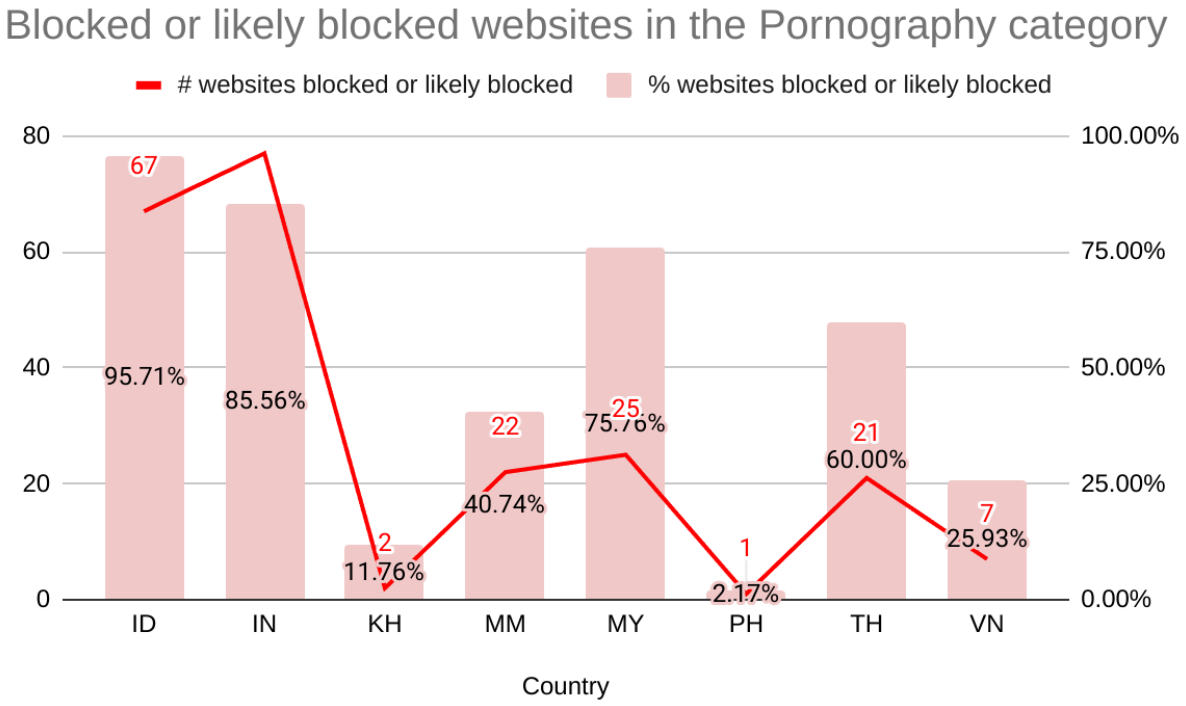

Chart 4: Blocked or likely blocked websites in the Pornography category by country

Political Criticism

Given that the freedom of expression online in the iMAP countries were either Partially Free or Not Free based on the Freedom on the Net reports, political criticism continued to be one of the content that is censored in these countries.

Country	Examples of Political Criticism websites found blocked
Myanmar	• democracyforburma.wordpress.com • drkokogyi.wordpress.com • nwayoomyanmar.com • sanooaung.wordpress.com
Cambodia	• www.ccimcambodia.org

Country	Examples of Political Criticism websites found blocked
Hong Kong	• www.hongkongwatch.org • 8964museum.com • samuelbickett.substack.com
India	• runforkashmir.org • standwithkashmir.org • www.bannedthought.net
Indonesia	• beritapolitikpelangi.blogspot.com • freepapua.com
Malaysia	• murrayhunter.substack.com • www.weechookeong.com • monyetistana.com
Philippines	• pamalakayaweb.wordpress.com • partisan-news.blogspot.com • umapilipinas.wordpress.com • www.arkibongbayan.org
Thailand	• alliance4democracy.blogspot.com • altthainews.blogspot.com • freedomforthai.carrd.co • progressivemovement.in.th
Vietnam	• doithoaionline.wordpress.com • exodusforvietnam.wordpress.com • huynhngocchenh.blogspot.com • khoi8406vn.blogspot.com

Table: Examples of Political Criticism websites found blocked by country

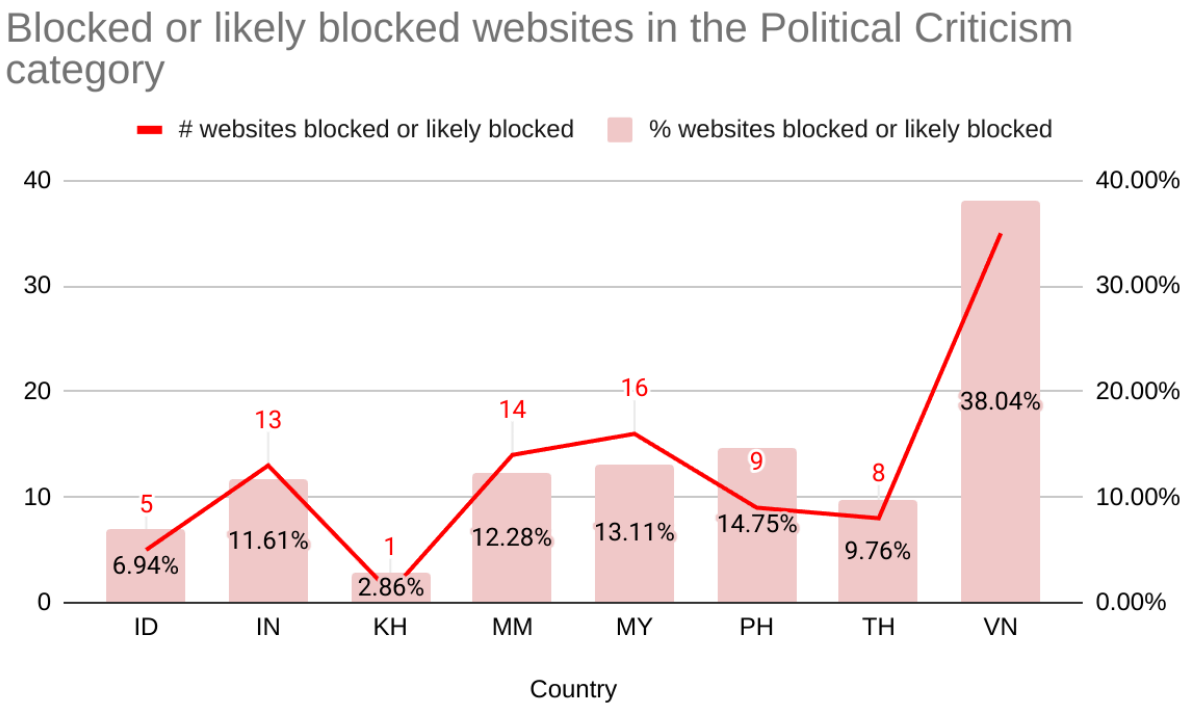

Chart 5: Blocked or likely blocked websites in the Political Criticism category by country

In Hong Kong (which is not depicted in the chart), Political Criticism websites were found blocked despite little censorship of Pornography and Gambling websites which are prevalent in other iMAP countries.

Social Networking and Communication Tools

Blocking of Social Networking and Communications Tools was most prevalent in Myanmar with 22 websites blocked including Facebook, X/Twitter, Instagram and Discord, as well as in Indonesia (e.g. Reddit and 4Chan) and in India (e.g. Weibo, Wechat, TikTok and Element).

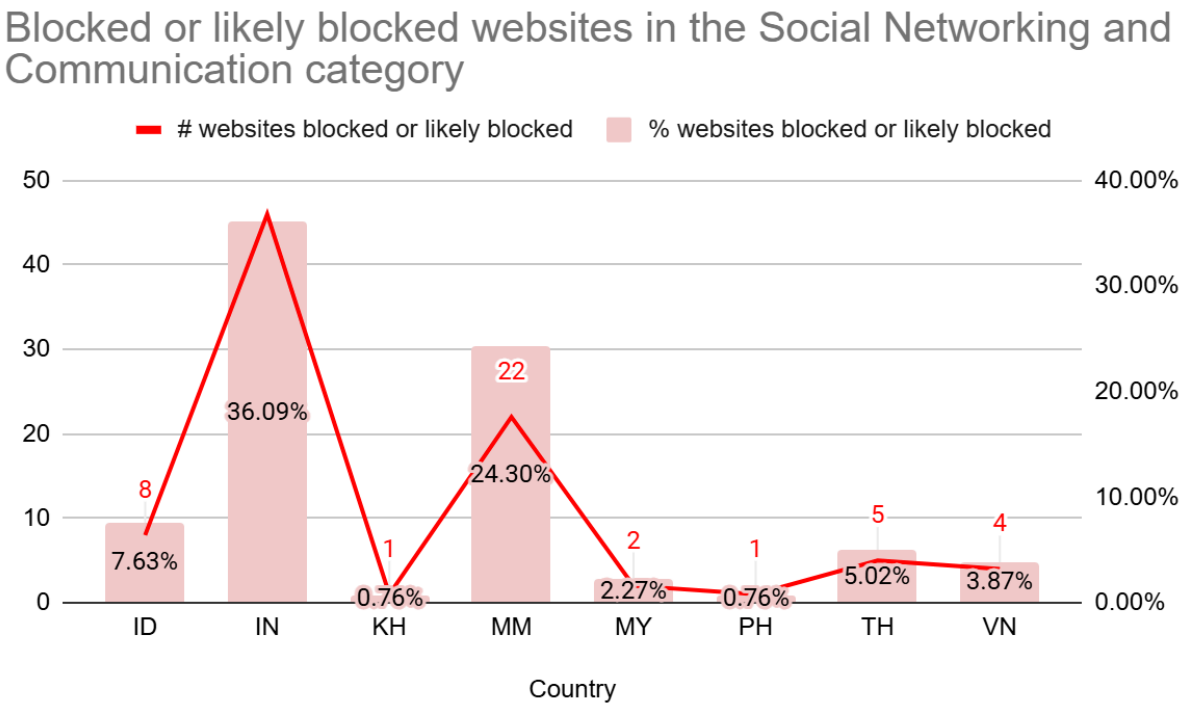

Chart 6: Blocked or likely blocked websites in the Social Networking and Communication category by country

Terrorism and Militants

Censorship of websites related to Terrorism and Militants were most prevalent in Indonesia, India and the Philippines. Particularly for the Philippines, the 4 websites found blocked were included in the list of websites ordered to be blocked by the government due to purported linkage to terrorism in 2022.

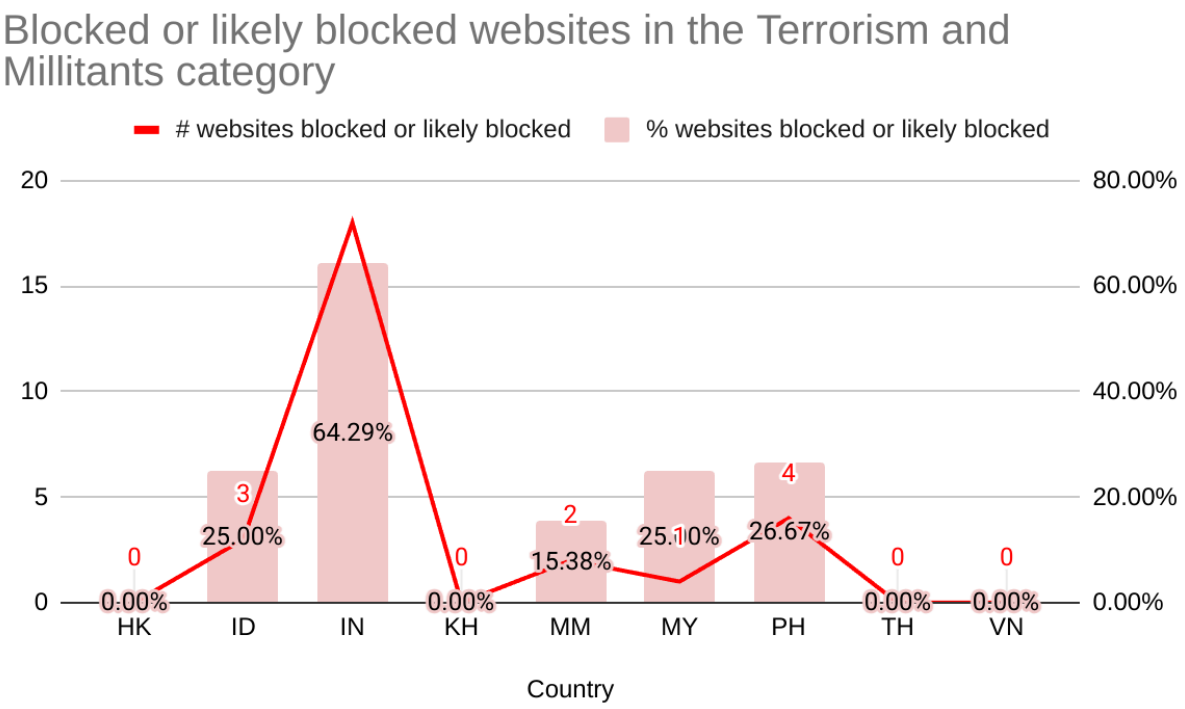

Chart 7: Blocked or likely blocked websites in the Terorrism and Militants category by country

Government

Significant censorship occurred in Myanmar, where the blocked websites were run by the National Unity Government (NUG), which has been declared by the State Administration Council (SAC) as an illegal terrorist organization.

In Hong Kong, it was found that US military websites were geoblocked in the country.

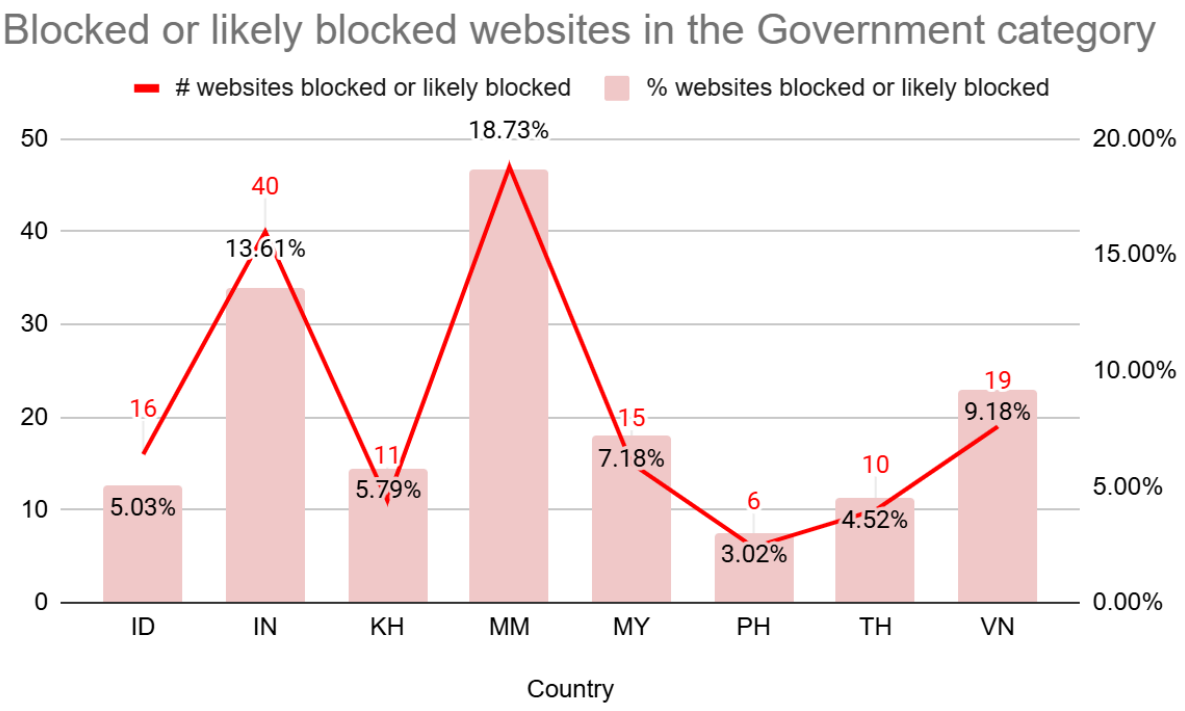

Chart 8: Blocked or likely blocked websites in the Government category by country

Blocking of Instant Messaging Apps

- Only four major Instant Messaging Apps are being tested on OONI: Facebook Messenger, Signal, Telegram and WhatsApp.
- Myanmar has recorded censorship of all Telegram and Whatsapp throughout the reporting period based on high anomalies.
- There was an issue with testing of Signal and Facebook Messenger in the OONI app resulting in false positives that had been removed from the analysis.

Blocking of Circumvention Tools

- Four types of circumvention tools were measured and analysed for the period of coverage: Psiphon and Tor. It should be noted that these tools are not popularly used in certain countries in the region, so it may be more beneficial to analyse the blocking of websites of circumvention tools instead (such as ProtonVPN, NordVPN, etc.).
- Myanmar has recorded censorship in Psiphon and Tor beginning in June 2024.

Contribute to the Study

If you would like to contribute to the OONI measurements, there are several ways to get involved:

- Perform testing on various platforms, both mobile (iOS and Android) and desktop, including the CLI on Linux platforms. The domains you test can be randomly selected from the Citizenlab Test Lists or custom test lists specific to your needs.
- Contribute to the test lists on GitHub or OONI.
- Translate the OONI Probe to your local language here.
- Participate in community discussions on the OONI Slack channel

Acknowledgements

We thank Khairil Yusof (Sinar Project) for his supervision and advisory support on the overall iMAP project and Numan Afifi (Sinar Project) for his valuable contributions to copyediting and report design. We would also like to thank the OONI team for their assistance in reviewing the methodology sections.

Additionally, we extend our gratitude to local partners, activists, academicians, researchers, and anonymous users for their assistance in running the OONI Probe.

Annex III: Glossary

DNS	DNS, which stands for Domain Name System, maps domain names to IP addresses. A domain is a name that is commonly attributed to websites (when they're created), so that they can be more easily accessed and remembered. For example, twitter.com is the domain of the Twitter website. However, computers can't connect to internet services through domain names, but based on IP addresses: the digital address of each service on the internet. Similarly, in the physical world, you would need the address of a house (rather than the name of the house itself) in order to visit it. The Domain Name System (DNS) is what is responsible for transforming a human-readable domain name (such as ooni.org) into its numerical IP address counterpart (in this case:104.198.14.52), thus allowing your computer to access the intended website.
HTTP	The Hypertext Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web to transfer or exchange data across the internet. The HTTP protocol allows communication between a client and a server. It does so by handling a client's request to connect to a server, and the server's response to the client's request. All websites include an HTTP (or HTTPS) prefix (such as http://example.com/) so that your computer (the client) can request and receive the content of a website (hosted on a server). The transmission of data over the HTTP protocol is unencrypted.
Heuristics	Heuristics obtain further confirmed blockings other than that which are detected based on OONI blocking fingerprints. More detailed explanation can be found here.
ISP	An Internet Service Provider (ISP) is an organization that provides services for accessing and using the internet. ISPs can be state-owned, commercial, community-owned, non-profit, or otherwise privately owned. Vodafone, AT&T, Airtel, and MTN are examples of ISPs.
Middle boxes	A middlebox is a computer networking device that transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding. Many Internet Service Providers (ISPs) around the world use middleboxes to improve network performance, provide users with faster access to websites, and for a number of other networking purposes.

	Sometimes, middleboxes are also used to implement internet censorship and/or surveillance. The OONI Probe app includes two tests designed to measure networks with the aim of identifying the presence of middleboxes.
TCP	The Transmission Control Protocol (TCP) is one of the main protocols on the internet. To connect to a website, your computer needs to establish a TCP connection to the address of that website. TCP works on top of the Internet Protocol (IP), which defines how to address computers on the internet. When speaking to a machine over the TCP protocol you use an IP and port pair, which looks something like this: 10.20.1.1:8080. The main difference between TCP and (another very popular protocol called) UDP is that TCP has the notion of a "connection", making it a "reliable" transport protocol.
TLS	Transport Layer Security (TLS) – also referred to as "SSL" – is a cryptographic protocol that allows you to maintain a secure, encrypted connection between your computer and an internet service. When you connect to a website through TLS, the address of the website will begin with HTTPS (such as https://www.facebook.com/), instead of HTTP.

A comprehensive glossary related to OONI can be accessed here: https://ooni.org/support/glossary/.

Annex IV: Methodology

Data

Data computed based on the heuristics for this report can be downloaded here: https://github.com/Sinar/imap-data whereas aggregated data can be downloaded from OONI Explorer.

Coverage

The iMAP State of Internet Censorship Country Report covers the findings of network measurement collected through Open Observatory of Network Interference (OONI) OONI Probe App that measures the blocking of websites, instant messaging apps, circumvention tools and network tampering. The findings highlight the websites, instant messaging apps and circumvention tools confirmed to be blocked, the ASNs with censorship detected and method of network interference applied. The report also provides background context on the network landscape combined with the latest legal, social and political issues and events which might have an effect on the implementation of internet censorship in the country.

In terms of timeline, this third iMAP report covers measurements obtained in the one-year period from 1 July 2023 to 30 June 2024. The countries covered in this round are Cambodia, Hong Kong (China), Indonesia, Malaysia, Myanmar, Philippines, Thailand, India, and Vietnam

How are the network measurements gathered?

Network measurements are gathered through the use of OONI Probe app, a free software tool developed by Open Observatory of Network Interference (OONI). To learn more about how the OONI Probe test works, please visit https://ooni.org/nettest/.

iMAP Country Researchers and anonymous volunteers run OONI Probe app to examine the accessibility of websites included in the Citizen Lab test lists. iMAP Country Researchers actively review the country-specific test lists to ensure up-to-date websites are included and context-relevant websites are properly categorised, in consultation with local communities and digital rights network partners. We adopt the approach taken by Netalitica in reviewing country-specific test lists.

It is important to note that the findings are only applicable to the websites that were examined and do not fully reflect all instances of censorship that might have occurred during the testing period.

How are the network measurements analysed?

OONI processes the following types of data through its data pipeline:

Country code

OONI by default collects the code which corresponds to the country from which the user is running OONI Probe tests from, by automatically searching for it based on the user's IP address through their ASN database the MaxMind GeoIP database.

Autonomous System Number (ASN)

OONI by default collects the Autonomous System Number (ASN) of the network used to run OONI Probe app, thereby revealing the network provider of a user.

Date and time of measurements

OONI by default collects the time and date of when tests were run to evaluate when network interferences occur and to allow comparison across time. UTC is used as the standard time zone in the time and date information. In addition, the charts generated on OONI MAT will exclude measurements on the last day by default.

Categories

The 32 website categories are based on the Citizenlab test lists: https://github.com/citizenlab/test-lists. As not all websites tested on OONI are on these test lists, these websites would have unclassified categories.

No.	Category Description	Code	Description
1	Alcohol & Drugs	ALDR	Sites devoted to the use, paraphernalia, and sale of drugs and alcohol irrespective of the local legality.
2	Religion	REL	Sites devoted to discussion of religious issues, both supportive and critical, as well as discussion of minority religious groups.
3	Pornography	PORN	Hard-core and soft-core pornography.

No.	Category Description	Code	Description
4	Provocative Attire	PROV	Websites which show provocative attire and portray women in a sexual manner, wearing minimal clothing.
5	Political Criticism	POLR	Content that offers critical political viewpoints. Includes critical authors and bloggers, as well as oppositional political organizations. Includes pro-democracy content, anti-corruption content as well as content calling for changes in leadership, governance issues, legal reform. Etc.
6	Human Rights Issues	HUMR	Sites dedicated to discussing human rights issues in various forms. Includes women's rights and rights of minority ethnic groups.
7	Environment	ENV	Pollution, international environmental treaties, deforestation, environmental justice, disasters, etc.
8	Terrorism and Militants	MILX	Sites promoting terrorism, violent militant or separatist movements.
9	Hate Speech	HATE	Content that disparages particular groups or persons based on race, sex, sexuality or other characteristics
10	News Media	NEWS	This category includes major news outlets (BBC, CNN, etc.) as well as regional news outlets and independent media.
11	Sex Education	XED	Includes contraception, abstinence, STDs, healthy sexuality, teen pregnancy, rape prevention, abortion, sexual rights, and sexual health services.
12	Public Health	PUBH	HIV, SARS, bird flu, centers for disease control, World Health Organization, etc
13	Gambling	GMB	Online gambling sites. Includes casino games, sports betting, etc.
14	Anonymization and circumvention tools	ANON	Sites that provide tools used for anonymization, circumvention, proxy-services and encryption.
15	Online Dating	DATE	Online dating services which can be used to meet people, post profiles, chat, etc
16	Social Networking	GRP	Social networking tools and platforms.

No.	Category Description	Code	Description
17	LGBT	LGBT	A range of gay-lesbian-bisexual-transgender queer issues. (Excluding pornography)
18	File-sharing	FILE	Sites and tools used to share files, including cloud-based file storage, torrents and P2P file-sharing tools.
19	Hacking Tools	HACK	Sites dedicated to computer security, including news and tools. Includes malicious and non-malicious content.
20	Communication Tools	COMT	Sites and tools for individual and group communications. Includes webmail, VoIP, instant messaging, chat and mobile messaging applications.
21	Media sharing	MMED	Video, audio or photo sharing platforms.
22	Hosting and Blogging Platforms	HOST	Web hosting services, blogging and other online publishing platforms.
23	Search Engines	SRCH	Search engines and portals.
24	Gaming	GAME	Online games and gaming platforms, excluding gambling sites.
25	Culture	CULTR	Content relating to entertainment, history, literature, music, film, books, satire and humour
26	Economics	ECON	General economic development and poverty related topics, agencies and funding opportunities
27	Government	GOVT	Government-run websites, including military sites.
28	E-commerce	COMM	Websites of commercial services and products.
29	Control content	CTRL	Benign or innocuous content used as a control.
30	Intergovernmental Organizations	IGO	Websites of intergovernmental organizations such as the United Nations.
31	Miscellaneous content	MISC	Sites that don't fit in any category (XXX Things in here should be categorised)

IP addresses and other information

OONI does not collect or store users' IP addresses deliberately. OONI takes measures to remove them from the collected measurements, to protect its users from potential risks. However, there may be instances where users' IP addresses and other potentially personally-identifiable information are unintentionally collected, if such information is included in the HTTP headers or other metadata of measurements. For example, this can occur if the tested websites include tracking technologies or custom content based on a user's network location.

Network measurements

The types of network measurements that OONI collects depend on the types of tests that are run. Specifications about each OONI test can be viewed through its git repository, and details about what collected network measurements entail can be viewed through OONI Explorer or through OONI's measurement API.

In order to derive meaning from the measurements collected, OONI processes the data types mentioned above to answer the following questions:

- Which types of OONI tests were run?
- In which countries were those tests run?
- In which networks were those tests run?
- When were tests run?
- What types of network interference occurred?
- In which countries did network interference occur?
- In which networks did network interference occur?
- When did network interference occur?
- How did network interference occur?

To answer such questions, OONI's pipeline is designed to answer such questions by processing network measurements data to enable the following:

- Attributing measurements to a specific country.
- Attributing measurements to a specific network within a country.
- Distinguishing measurements based on the specific tests that were run for their collection.
- Distinguishing between "normal" and "anomalous" measurements (the latter indicating that a form of network tampering is likely present).
- Identifying the type of network interference based on a set of heuristics for DNS tampering, TCP/IP blocking, and HTTP blocking.
- Identifying block pages based on a set of heuristics for HTTP blocking.
- Identifying the presence of "middle boxes" within tested networks.

According to OONI, false positives may occur within the processed data due to a number of reasons. DNS resolvers (operated by Google or a local ISP) often provide users with IP addresses that are closest to them geographically. While this may appear to be a case of DNS tampering, it is actually done with the intention of providing users with faster access to websites. Similarly, false positives may emerge when tested websites serve different content depending on the country that the user is connecting from, or in the cases when websites return failures even though they are not tampered with.

Furthermore, measurements indicating HTTP or TCP/IP blocking might actually be due to temporary HTTP or TCP/IP failures, and may not conclusively be a sign of network interference. It is therefore important to test the same sets of websites across time and to cross-correlate data, prior to reaching a conclusion on whether websites are in fact being blocked.

Since block pages differ from country to country and sometimes even from network to network, it is quite challenging to accurately identify them. OONI uses a series of heuristics to try to guess if the page in question differs from the expected control, but these heuristics can often result in false positives. For this reason OONI only says that there is a confirmed instance of blocking when a block page is detected.

Upon collection of more network measurements, OONI continues to develop its data analysis heuristics, based on which it attempts to accurately identify censorship events.

The full list of country-specific test lists containing confirmed blocked websites in Myanmar, Cambodia, Hong Kong, Indonesia, Malaysia, Philippines, Thailand, and Vietnam can be viewed here: https://github.com/citizenlab/test-lists.

Confirmed blocked OONI measurements were based on fingerprints recorded here https://github.com/ooni/blocking-fingerprints. These fingerprints are based on either DNS or HTTP blocking. Fingerprints recorded as confirmed blockings are either those implemented nationally or by ISPs.

Hence, heuristics as below were run on raw measurements on all countries under iMAP to further confirm blockings.

Firstly, IP addresses with more than 10 domains were identified. Then each of the IP address was checked for the following:

<table>
<tr><td colspan="6">Does the IP in question point to a government blockpage?</td></tr>
<tr><td>Yes</td><td colspan="5">No, page timed out or shows Content Delivery Network (CDN) page.</td></tr>
<tr><td>⬇</td><td colspan="5">⬇</td></tr>
<tr><td>Confirmed blocking</td><td colspan="5">What information can we get about the IP by doing a whois lookup?</td></tr>
<tr><td></td><td>Government entity</td><td>Local ISP[14]</td><td colspan="3">CDN[15] / Private IP</td></tr>
<tr><td></td><td>⬇</td><td>⬇</td><td colspan="3">⬇</td></tr>
<tr><td></td><td>Confirmed blocking</td><td>Likely Blocked or Inaccessible</td><td colspan="3">Do we get a valid TLS certificate for one of the domains in question when doing a TLS handshake and specifying the SNI</td></tr>
<tr><td></td><td></td><td></td><td>Yes</td><td>No, there were blocking fingerprints found.</td><td>No, timed out</td></tr>
<tr><td></td><td></td><td></td><td>⬇</td><td>⬇</td><td>⬇</td></tr>
<tr><td></td><td></td><td></td><td>False positive</td><td>Confirmed blocking</td><td>Sampled measurement is analyzed on</td></tr>
</table>

[14] In the case of India, there was evidence of popular websites hosting their site on the ISPs network for quicker loading times as the ISPs sometimes offer such edge networking services, hence websites redirected to local websites not marked as blocked.

[15] In general, websites redirected to popular CDN such as CloudFlare, Amazon, Google, etc. are marked as not blocked.

					OONI Explorer.

When blocking is determined, any domain redirected to these IP addresses would be marked as 'dns.confirmed'.
Secondly, HTTP titles and bodies were analyzed to determine blockpages. This example shows that the HTTP returns the text 'The URL has been blocked as per the instructions of the DoT in compliance to the orders of Court of Law'. Any domain redirected to these HTTP titles and bodies would be marked as 'http.confirmed'.

As a result, false positives are eliminated and more confirmed blockings are obtained.

In the 2022 report, only confirmed blockings based on OONI or new fingerprints were reported.

For this round of reporting in 2023, we had also further identified confirmed blockings by verifying blockings shown in news reports with OONI measurements. This is because there were blockings that could be not identified using the DNS or HTTP fingerprints. Typically, these websites were redirected to an unknown or bogon IP address, or had other unknown errors which are ambiguous on whether they are true or false positives of censorship. Hence, based on the news reports where the blocked websites were cited, confirmed blockings were further found by comparing available measurements on OONI. In particular for this study, we would mark them as confirmed blockings if there are more than 30 measurements and have an anomaly rate of more than 1% throughout the one-year period of study, in addition to manually checking the OONI measurements by cross-checking across networks, countries and time periods.

For this round of reporting in 2024, the confirmed blockings were further consolidated based on OONI's existing fingerprints and heuristics processed on the data during the coverage period, in addition to taking into account a weighted anomaly ratio, measurement count and past analysis of the country. In summary, these were the rules applied to obtain this year's list of confirmed and likely blockings.

	Confirmed blockings	Likely blockings or inaccessible
Malaysia	Confirmed by OONI only	None
Myanmar	• Confirmed by heuristics (govt block page) • Confirmed by OONI (govt block page)	High weighted anomaly ratio and confirmed by news report/ block notice
Thailand	• Confirmed by heuristics (govt block page) • Confirmed by OONI (govt block page)	High weighted anomaly ratio
Philippines	• Confirmed by heuristics (govt block page) • Confirmed by OONI (govt block page) • Confirmed by news report/ block notice	High weighted anomaly ratio
India	• Confirmed by OONI with at least 5 counts • Confirmed by heuristics (govt block pages)	High weighted anomaly ratio
Indonesia	• Confirmed by OONI with at least 5 counts • Confirmed by heuristics (govt block pages)	High weighted anomaly ratio
Vietnam	• Confirmed by heuristics (govt block page) • Confirmed by news report/ block notice	• High weighted anomaly ratio • Confirmed by OONI (due to being ISP redirects)
Cambodia	• Confirmed by news report/ block notice	• High weighted anomaly ratio • Confirmed by OONI (due to being ISP redirects)
Hong Kong	None	High weighted anomaly ratio

Weighted anomaly ratio: It is calculated by finding the ratio of the Anomaly and Confirmed counts over the total measurements per ASN factoring weights based on number of measurements per domain and per ASN. A high anomaly ratio is when the P90 of the anomaly ratio of a domain exceeds 90%.