Internet Monitoring Action Project

iMAP 2023 Internet Censorship Report: Executive Summary

By Siti Nurliza Samsudin (Sinar Project) and Kelly Koh (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 10 countries: Myanmar, Cambodia, Hong Kong, India, Indonesia, Malaysia, Philippines, Thailand, Vietnam and Timor-Leste. Sinar Project is currently working with national digital rights partners in these 10 countries. The project is done via Open Observatory Network Interference (OONI) detection and reporting systems, and it involves the maintenance of test lists as well as 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

Recommendations to audience:

- Supporting evidence of internet censorship
- Understanding what the latest development of internet censorship in the country is, in terms of methods of blockings and the websites affected by censorship.
- Policy advocacy
- Call to action

This report is not meant to provide comparison of measurements across countries or measurements among different website categories covered by the iMAP project.

How to Use This Report

This executive summary aims to provide an overview of the state of internet censorship in the 10 countries covered under iMAP as a region. It serves to highlight the overall trend of internet censorship that includes the blocking of websites, instant messaging apps, circumvention tools and network tampering, its similarities and differences across 10 countries in the region, as well as 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 10 countries.
- Key findings in the region
  - This section provides a general takeaway on the blocking of websites, internet censorship during elections, and 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 as visualisation.
- Contribute to the study
  - This section is created to help readers understand how they could contribute to the study and the gathering of evidence of internet censorship.
- Annex: Methodology
  - Here the readers will find how the data is collected, measured and analysed for the purpose of iMAP 2023 country reports.

This executive summary is a good starting point for reference to gather a general understanding on what is being affected by internet censorship in the 10 countries. Our target audience includes researchers working on digital rights or network interference who are in search of ideas and materials for further research, digital rights defenders or civil society organisations looking for materials to support their advocacy work, journalists seeking to uncover internet censorship, among others.

Recommendations to audience:

- Supporting evidence of internet censorship
- Understanding what is the latest development of internet censorship in the country, in terms of methods of blockings and the websites affected by censorship
- Policy advocacy
- Call for action

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

Abbreviations

ALDR	Alcohol & 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
POLR	Political Criticism
PORN	Pornography
PROV	Provocative Attire
PUBH	Public Health
REL	Religion
SRCH	Search Engines

ALDR	Alcohol & Drugs
XED	Sex Education
GRP	Social Networking
MILX	Terrorism and Militants
TCP	Transmission Control Protocol
TLS	Transport Layer Security

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 collection and analysis of network measurements in 10 countries: **Cambodia, Hong Kong (China), India, Indonesia, Malaysia, Myanmar, Philippines, Thailand, Timor-Leste and Vietnam** during the testing period from **1 July 2022 to 30 June 2023**. However, in Timor-Leste the study was based on measurements recorded from 1 May 2023 to 31 August 2023.

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 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.

Whilst most information on online censorship is largely derived 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 wider extent of internet censorship in the region and the control of the internet by the governments.

Overview of socio political situation in the region

Population	Max: 1.4 billion (India) Min: 1.3 million (Timor-Leste)
Internet penetration (% of population using the internet)	Max: 96% (Malaysia) Min: 44% (Myanmar)
Mobile subscriptions (per 100 inhabitants)	Max: 292 (Hong Kong (China) Min: 88 (India)
Freedom on the Net ranking (2022)	Free (1): • Timor-Leste 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 (78%) • Timor-Leste (98%) Hinduism-majority • India (80%) Islam-majority: • Indonesia (87%) • Malaysia (64%)
ICCPR Ratification	Yes (7): • Cambodia • Indonesia • India • Philippines • Thailand • Timor-Leste • Vietnam

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

Table: Indicators of socio political situation in the region

Specific Country Highlights

There are no countries in the region that have gained the status of achieving internet freedom considered as “free”, except for Timor-Leste. Similar to the previous edition of the report, governments in the region are increasingly imposing Internet regulations in a manner that restricts the flow of information across national borders and limits internet freedom.

Despite **Cambodia** being a party to the International Covenant on Civil and Political Rights (ICCPR) that provides protection to the freedom of expression which can only be restricted in limited circumstances of legality, legitimacy and necessity under Article 19(3), the Inter-Ministerial Prakas (proclamation) on Website and Social Media Control was adopted in May 2018 to impose obligation on all internet service providers to install surveillance software to monitor content circulated on the internet. The new National Internet Gateway requiring internet service providers in Cambodia to reroute internet traffic through a regulatory body will enable monitoring of online activity.

Internet freedoms in **Hong Kong** continue to diminish. The imposition of the National Security Law has led to political websites showing dissident contents to be blocked on the grounds of national security.

Indonesia has extensive laws on content removal. Handling of Internet Sites Containing Negative Content Ministerial Regulation No 19 of 2014 enables the Ministry of Information and Communications (Kominfo) to mandate ISPs to block internet content that are deemed to carry negative elements, such as pornography, hoaxes, and issues concerning ethnicity, religion, race and intergroup relations (SARA) conflict. The Electronic Information and Transactions (ITE) Law No 11 of 2008 with its amendment in 2016 under article 40 enables preventative measures to be taken against the dissemination of information, enabling the government to terminate access to information that are deemed to be in violation of laws.

Whilst **Malaysia** does not have an extensive range of legal instruments to restrict internet freedom, nevertheless sections 211 and 233 of the Communications and Multimedia Act 1998 and the Penal Code have often been used on a wide range of online contents that are deemed to be offensive, including contents critical of government or satirical artwork depicting politicians or monarchy. The Evidence Act places prima facie responsibilities on website owners over any wrongdoing committed by third party such as offensive comments left on the website.

Since the takeover by Military Junta, **Myanmar** has been under regular internet shutdown and disruptions. The Electronic Transactions Law has been used to criminalize online activity such as the spread of fake news, cyber-attacks and cyber-terrorism; and to provide the

government the ability to access data when there is a suspected offence. A draft Cybersecurity Law has been circulated which gives broad powers to the Military Junta to seize ISP user information.

In the **Philippines**, news media that are critical of the ruling administration face the risk of being linked to communist insurgency. Internet service providers were ordered to block news sites Bulatlat and Pinoy Weekly over purported ties to communist-terrorist groups.

Thailand has a restrictive internet environment that heavily penalises crimes committed against defaming, insulting and threatening the monarchy under the Penal Code. The Computer Crimes Act allows justification for blocking of websites with pornographic contents, matters related to national security, and information that could instigate public panic.

Vietnam extends its control over internet content to international tech giants. Facebook and Google have been requested to impose control and removal of accounts and contents, and to hand over potentially vast amounts of data. Bloggers, activists and social media users who are vocal on controversial issues relating to human rights, democracy, the communist party and the state are heavily surveilled by authorities.

Recent years saw the rise of amendments made to Information Technology Act 2000 in **India** that were introduced for content blocking and takedown on social media intermediaries and digital media publishers, empowerment of fact-check unit that indirectly controls the flow on information on social media, with the responsibility on intermediaries to take down contents identified to be false. During the coverage period, more than 10 instant messaging apps were found to be blocked in the conflict-inflicted region of Jammu and Kashmir under the pretext of national security. The trend of blocking of China-based mobile applications continued. The GitHub platform was affected by court-ordered blocking of URL, until it was subsequently lifted.

As one of the newest sovereign states in the world, **Timor-Leste** faces growing economic inequality and infrastructure issues. Internet price is one of the most expensive in Asia, but with limited coverage and below-satisfactory connection and speed. Whilst several laws and policies were introduced in recent years to govern internet space targeting online criticism, there is no evidence of government-ordered internet censorship found thus far, though there were several instances of internet outages.

Key findings in the region

Blocking of websites

- All of the countries had at least one recorded case of automatically confirmed censorship, except for Timor-Leste where we did not find any censorship but there were many failed tests due to poor connectivity in the country.

- Based on the findings in all of the countries, the categories with the most blockings are Pornography, Gambling and Provocative Attire. However at the country level, this varies; for instance these categories are barely blocked in Hong Kong, whereas Poronography, Social Networking and Media Sharing are the top categories for Myanmar and Political Criticism for Vietnam. In India, Terrorism and Militants websites are found to be likely blocked.
- The most common method of blocking is via DNS, followed by HTTP.

Blocking method	Countries
DNS	Cambodia, Malaysia, Philippines
DNS+HTTP	Hong Kong (China), Indonesia, India, Thailand, Myanmar, Vietnam

Table: Most common method of blocking by country

Monitoring of internet censorship during elections

During the elections held in the study period, monitoring of internet censorship was done in Thailand and Timor-Leste. Findings were as follows:

Country	Period	Findings
Thailand	May 2023	ectreport.com, which was a website that published unofficial election results, was unavailable on the night of 14 May 2023. This was also found inaccessible on OONI data, although there was no block page to confirm that it was a government or ISP mandated censorship.
Timor-Leste	May 2023	No censorship found; although the testing resulted in high anomalies and failures due to poor internet connectivity.

Table: Findings of monitoring of internet censorship during elections covered in the reporting period, July 2022-June 2023

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 anomaly rate 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 websites 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.

Gambling

As in the 2022 edition of the report, the Gambling category recorded the second highest number of blocked or likely blocked websites. Except for Cambodia, Hong Kong and Timor-Leste, all other countries had at least one website in this category blocked. In Indonesia, almost 70% of Gambling websites tested were blocked or likely blocked.

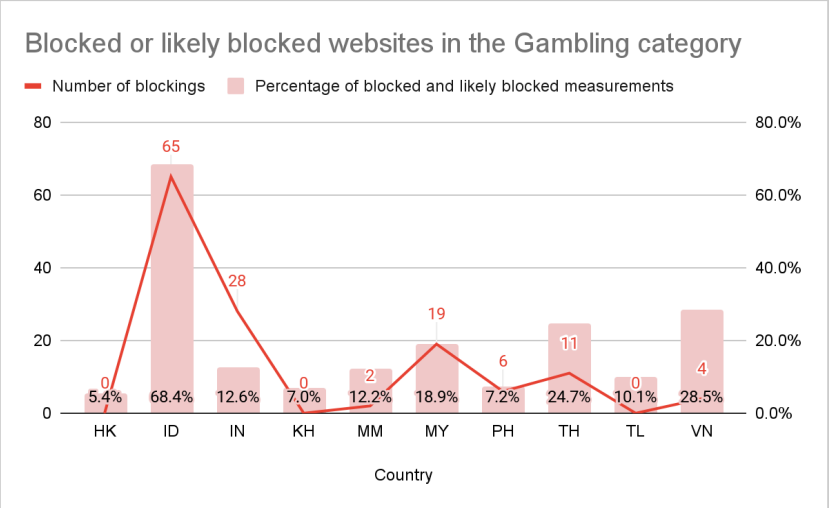

Chart: Blocked or likely blocked websites in the Gambling category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

News Media

Censorship of News Media websites were found most prevalent in Myanmar with 14.1% likelihood of blocking and 48 confirmed blocked websites, as well as in Vietnam with 16.5% likelihood of blocking and 30 confirmed blocked websites. These 2 countries were also considered as Not Free in the Freedom on the Net report.

Since February 2023, Cambodia had reported new cases of censorship of websites in the category, particularly websites of the independent news media. These websites were also blocked during their general elections held in July 2023.

Among the websites found blocked in the iMAP countries are:

Country	Examples of NEWS websites blocked
Cambodia	• https://english.cambodiadaily.com/ • https://vodhotnews.com/
Indonesia	• https://opinibangsa.com/ • https://suaranews.id/
India	• https://news.sina.com.cn/ • https://currentaffairspk.com/

Country	Examples of NEWS websites blocked
Malaysia	• https://www.malaysia-chronicle.com/ • https://www.malaysia-today.net/
Myanmar	• https://myanmar-now.org/en/ • https://www.bnionline.net/en
Philippines	• https://bulatlat.com/ • https://pinoyweekly.org/
Vietnam	• https://www.baocalitoday.com/ • https://www.bbc.com/vietnamese/

Table: Examples of NEWS websites blocked under iMAP countries

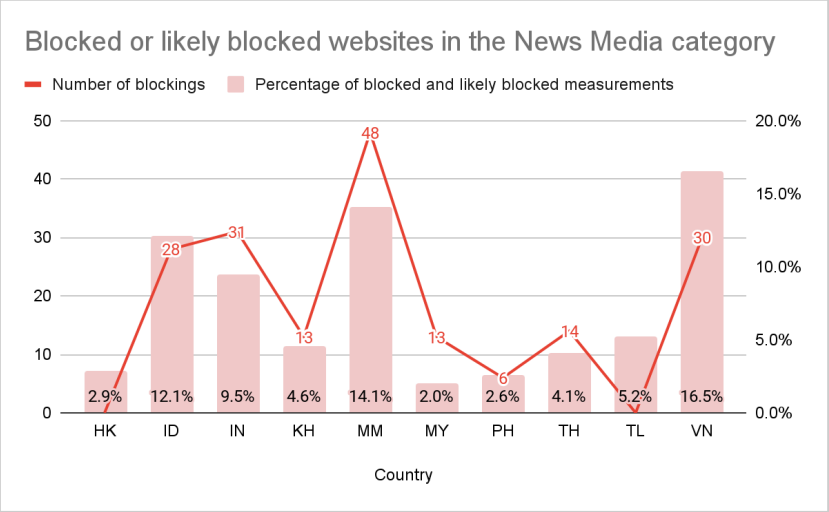

Chart: Blocked or likely blocked websites in the News Media category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

LGBTQI+

Blocking of LGBTQI+ websites was prevalent in Indonesia, Malaysia, India, Myanmar, Philippines, Thailand and Vietnam. Among the websites blocked in multiple countries are:

- gaytoday.com
- www.gay.com
- www.gayegypt.com
- www.gayscape.com
- www.ifge.org
- www.planetromeo.com
- www.queernet.org

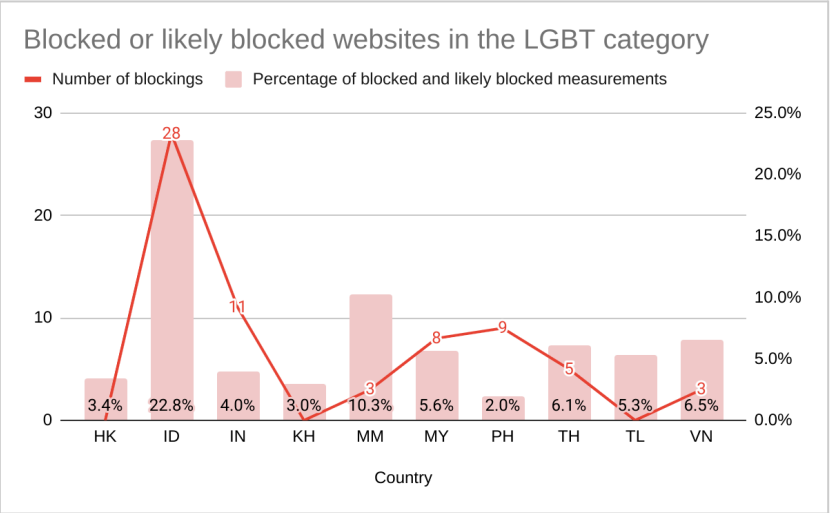

Chart: Blocked or likely blocked websites in the LGBT category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

Pornography

Similar to last year, Pornography was the category with the highest number of blockings. Likelihood of blocking exceeds 50% in India and Indonesia. However, there is little censorship recorded in this category in Cambodia and Hong Kong, as well as in Timor-Leste (which has no recorded censorship in any category).

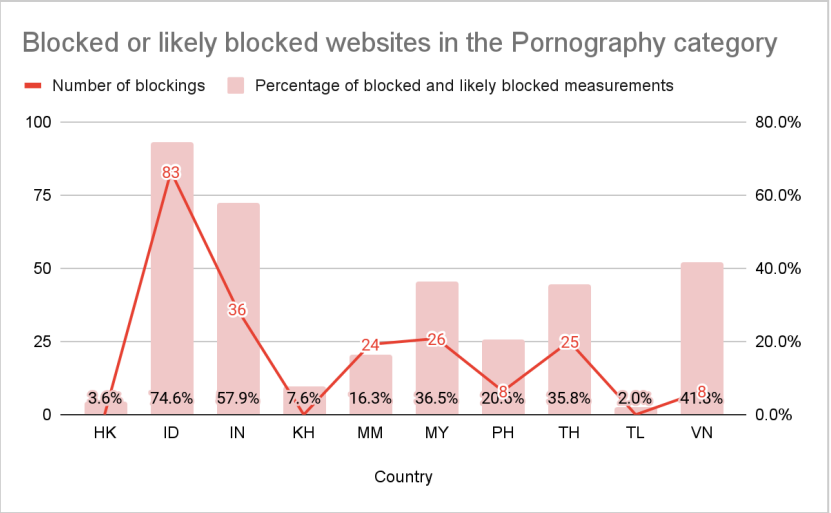

Chart: Blocked or likely blocked websites in the LGBT category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

Political Criticism

Censorship of Political Criticism websites were most prevalent in Vietnam, with 46 confirmed blockings. There are also significant anomalies found in Hong Kong, Indonesia, India, Myanmar, and the Philippines. Among the websites found blocked in the iMAP countries are:

Country	Examples of POLR websites blocked
Hong Kong (China)	• https://8964museum.com/ • https://blockedbyhk.com/
Indonesia	• https://partaikomunisindonesia.wordpress.com/page/3/ • http://indonbodoh.blogspot.com/
India	• https://kashmircivitas.com/ • https://clarionproject.org/
Malaysia	• https://www.bersih.org/ • https://edisisiasatmy.blogspot.com/
Myanmar	• https://aungsanu.com/my • https://mmpeacemonitor.org/
Philippines	• http://partisan-news.blogspot.com/ • https://angpamalakaya.org/
Vietnam	• http://datviet.free.fr/ • http://goken.free.fr/
Thailand	• http://fb.watch/3aiaDnGJTi • http://progressivemovement.in.th/article/3258

Notably, in the Philippines, 6 out of the 26 websites ordered to be blocked by the government in July 2022 belonged to the Political Criticism category. These websites were blocked because of purported linkage to "communist terrorist groups". In Hong Kong, where there were blockings of Political Criticism websites previously, the censorship of the same websites was unable to be confirmed during this period due to low measurements.

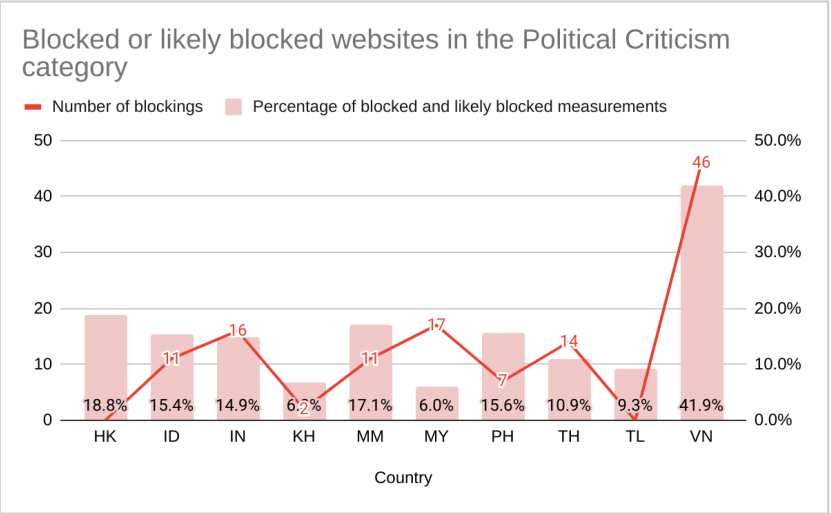

Chart: Blocked or likely blocked websites in the Political Criticism category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

Social Networking

Blocking of Social Networking and Communications tools was most prevalent in Myanmar with 27 websites blocked including Facebook, Twitter, Instagram and Discord, as well as in Indonesia (e.g. Reddit and 4Chan) and in India (e.g. TikTok and Element). In Hong Kong, Viber was found blocked, although only on an enterprise ISP. Other websites were mostly bulletin boards which are run locally.

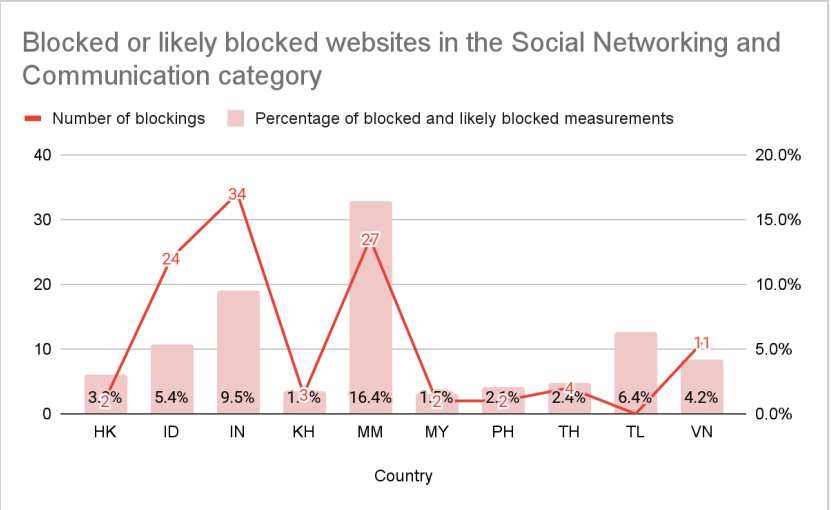

Chart: Blocked or likely blocked websites in the Social Networking and Communication category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

Terrorism and Militants

During this study period, censorship of websites related to Terrorism and Militants were most prevalent in Indonesia, India and the Philippines. Particularly for the Philippines, the websites were included in the 26 websites ordered to be blocked by the government due to purported linkage to terrorism.

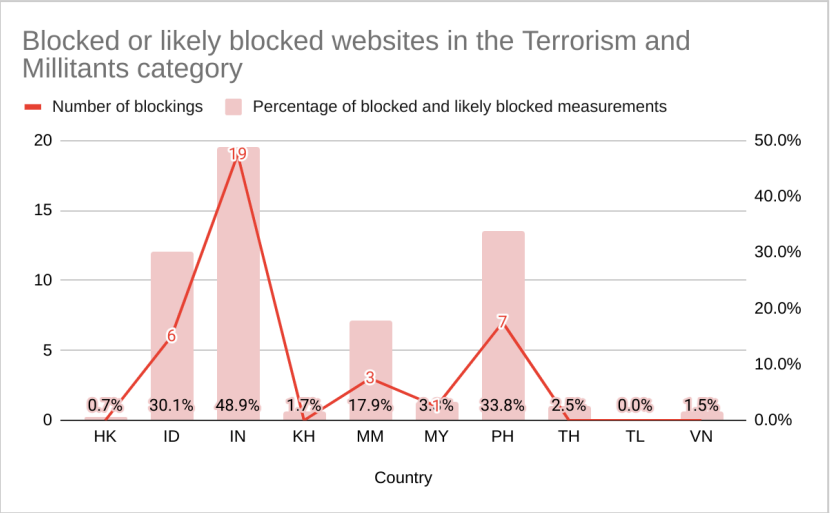

Chart: Blocked or likely blocked websites in the Terrorism and Militants category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

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 blocked in the country, whereas in Timor-Leste, significant anomalies were found – showing results of poor connectivity and little access to information provided online by the government.

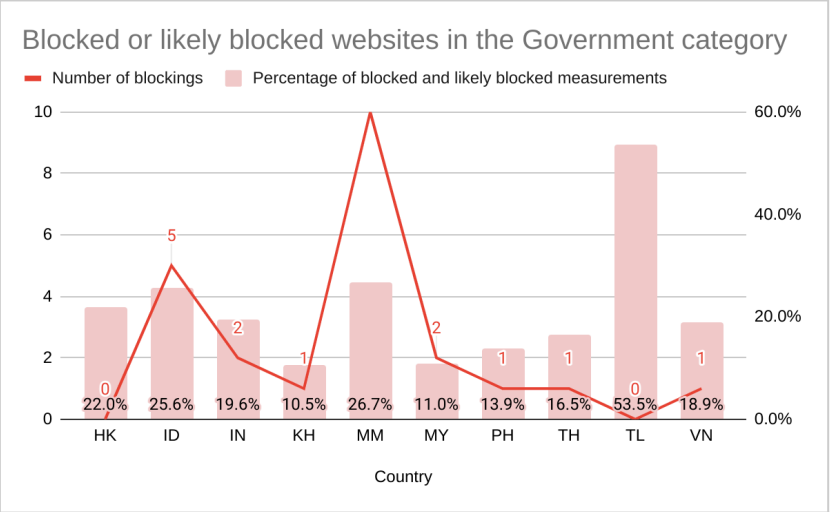

Chart: Blocked or likely blocked websites in the Government category. Blocked or likely blocked indicate testing on OONI that resulted in either Confirmed Blocked, Anomaly or Failure measurements.

Blocking of Instant Messaging Apps

- There are only four major Instant Messaging Apps being tested on OONI: Facebook Messenger, Signal, Telegram and WhatsApp.
- Myanmar has recorded censorship of Facebook Messenger and Whatsapp throughout the reporting period based on high anomalies.
- Vietnam recorded possible censorship of Facebook Messenger in February 2023 but only on certain networks.
- 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

- There are four types of circumvention tools measured on OONI: Psiphon, Tor, Tor Snowflake and RiseupVPN. It should be noted that these tools are not popularly used in certain countries in the region, so it may be more useful to analyze blocking of websites of circumvention tools instead (such as ProtonVPN, NordVPN, etc.).
- There is a high anomaly rate (more than 99%) on testing of Psiphon in the Philippines but this needs to be investigated further to eliminate the possibility of false positives.
- A significant number of anomalies was recorded on Tor Snowflake in Malaysia, Hong Kong and Timor-Leste but these are likely false positives.

Contribute to the study

There are various ways one may contribute to OONI measurements:

- **Testing:** You may test on various platforms, both on Mobile (iOS and Android) and Desktop (Windows and macOS), including on the CLI on Linux platforms. The domains you test can be either randomly selected from the Citizen Lab Test Lists or custom test lists specific to your needs.
- **Contribute to the test lists:** You can contribute to the test lists on GitHub or through OONI's Test Lists Editor..
- **Translate** the OONI Probe to your local language here.
- Participate in community discussions on OONI's Slack channel.

Annex: 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. The OONI API enables you to perform your own analysis of OONI data. For batch consumption of OONI data, you can fetch the whole OONI dataset from the Amazon S3 bucket.

Coverage

The iMAP State of Internet Censorship Country Report covers the findings of network measurements collected through the 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, as well as ASNs with censorship detected and the methods 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 affected the implementation of internet censorship in the country.

In terms of timeline, this iMAP report covers measurements obtained in the one-year period from **1 July 2022 to 30 June 2023**. The countries covered in this round are Cambodia, Hong Kong, Indonesia, Malaysia, Myanmar, Philippines, Thailand, Vietnam, Timor Leste, and India.

How are the network measurements gathered?

Network measurements are gathered through the use of the OONI Probe app, a free software tool developed by the 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 the 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

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

Autonomous System Number (ASN)

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

Date and time of measurements

By default, OONI collects the time and date of when tests were run in order to determine when network interferences occur and to allow for comparison across time. The time and date data uses UTC as the standard time zone. In addition, the charts generated on OONI MAT exclude measurements on the last day by default. This means that when filtering the measurements by dates, for instance – from 1 January to 31 December – measurements on 31 December would be excluded.

Categories

The 32 website categories are based on the Citizenlab test lists: https://github.com/citizenlab/test-lists. As not all tested websites available in the OONI dataset are included in these test lists, some 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.
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 organisations. Includes pro-democracy content, anti-corruption content as well as

No.	Category Description	Code	Description
			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, including 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, centres 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.
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.

No.	Category Description	Code	Description
19	Hacking Tools	HACK	Sites dedicated to computer security, including news and tools. This includes malicious and non-malicious content.
20	Communication Tools	COMT	Sites and tools for individual and group communications. This 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 Organisations	IGO	Websites of intergovernmental organisations 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. To protect its users from potential risks, OONI takes measures to remove IP addresses from the collected measurements. 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 GitHub 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?
- On which networks were those tests run?
- When were the 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 measurement 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 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; they 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 before reaching a conclusion on whether websites are in fact being blocked.

Since censorship differs from country to country and sometimes even from network to network, it is quite challenging to accurately identify and confirm it in an automated way. 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 automatically confirms an instance of blocking when a block page is detected or when DNS resolution returns an IP associated with censorship.

Upon the collection of more network measurements, OONI continues to develop its data analysis heuristics, based on which it attempts to accurately identify censorship events. OONI is advancing its data analysis capabilities to automatically detect and characterise more forms of internet censorship through their data analysis tool.

The full lists of websites that were tested in Myanmar, Cambodia, Hong Kong, Indonesia, Malaysia, Philippines, Thailand, and Vietnam can be viewed here: https://github.com/citizenlab/test-lists.

Verifying OONI measurements

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. The fingerprints recorded as confirmed blockings are either those implemented nationally or by ISPs.

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

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

<table>
<tr><td colspan="5">Does the IP in question point to a government blockpage?</td></tr>
<tr><td>Yes</td><td colspan="4">No, page timed out or shows Content Delivery Network (CDN) page.</td></tr>
<tr><td>⬇</td><td colspan="4">⬇</td></tr>
<tr><td>Confirmed blocking</td><td colspan="4">What information can we get about the IP by doing a whois lookup?</td></tr>
<tr><td rowspan="5"></td><td>Government or Local ISP*</td><td colspan="3">CDN / Private IP</td></tr>
<tr><td>⬇</td><td colspan="3">⬇</td></tr>
<tr><td>Confirmed blocking</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 rowspan="3"></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></tr>
<tr><td>False positive</td><td>Confirmed blocking</td><td>Sampled measurement is analysed on OONI Explorer.</td></tr>
</table>

*Note: 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 are only marked as ‘Potentially Blocked’.

When blocking is determined, any domain redirected to these IP addresses will be marked as “dns.confirmed”.

Secondly, HTTP titles and bodies were analysed 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 further identified confirmed blockings by verifying blockings shown in news reports with OONI measurements. This is because there were blockings that could not be identified using the DNS or HTTP fingerprints. Typically, these websites were redirected to an unknown or bogon IP address, or they had other unknown errors that were ambiguous as to whether they were 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 the available measurements on OONI. For this study in particular, we marked them as confirmed blockings if there were more than 30 measurements and an anomaly rate of more than 1% throughout the one-year period of study. In addition, we manually checked the OONI measurements by cross-checking across networks, countries, and time periods.