Internet Monitoring Action Project

iMAP Hong Kong (China) 2024 Internet Censorship Report

Siti Nurliza Samsudin (Sinar Project), **Stephania Aves Taboada** (Sinar Project), **and Independent Researchers** (Anonymous)

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 nine countries: Myanmar, Cambodia, Hong Kong, India, Indonesia, Malaysia, Philippines, Thailand, and Vietnam. Sinar Project is currently working with national digital rights partners in these nine 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.

About Sinar Project

Sinar Project is a civic tech initiative that uses open technology, open data, and policy analysis to systematically make important information public and more accessible to the Malaysian people. It aims to improve governance and encourage greater citizen involvement in the nation's public affairs by making the Malaysian Parliament and Government more open, transparent, and accountable. More information is available at https://sinarproject.org.

How to use this report

This report provides an overview of the state of internet censorship in Hong Kong. It is not meant to provide a comparison of measurements across countries or measurements among different website categories covered by the iMAP project.

Recommendations to readers:

- Learn about supporting evidence related to internet censorship in Hong Kong 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 Hong Kong.
- Take action and get involved by spreading awareness, signing petitions, or joining initiatives that fight against internet censorship.

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

POLR	Political Criticism
PORN	Pornography
PROV	Provocative Attire
PUBH	Public Health
REL	Religion
SRCH	Search Engines
XED	Sex Education
GRP	Social Networking
MILX	Terrorism and Militants
TCP	Transmission Control Protocol
TLS	Transport Layer Security

Table of Content

About iMAP 2
About Sinar Project 2
How to use this report 2
Abbreviations 3
Table of Content 5
Key Findings 6
Introduction 6
Background 7
Legal Environment 9
Hong Kong Basic Law 9
Legislative Context 9
Hong Kong National Security Law & Legislative Reform 10
Safeguarding National Security Ordinance 11
Reported Cases of Internet Censorship 13
Network Landscape 14
Findings on Internet Censorship in Hong Kong 15
Blocking of Websites 15
Hong Kong Watch website 16
8964 Online Museum website 16
Samuel Bickett Substack 17
Government Category 17
Methods of Blocking of Websites 17
Findings on Internet Takedowns 18
Acknowledgement of Limitations 19
Conclusion 21
Contribute to the Study 21
Acknowledgements 21
Annex I: List of Confirmed Blockings 22
Annex II: List of ISPs 23
Annex III: Glossary 24
Annex IV: Methodology 26

Key Findings

- The key findings of the study showed that internet censorship in Hong Kong mainly affects websites in the Political Criticism and Government categories, in particular websites related to the US military.
- Unlike many other countries in Southeast Asia, there is little censorship in categories such as Porn and Gambling.
- The most commonly used method of blocking by ISPs is DNS tampering, including effects of censorship from mainland China.

Introduction

The Open Observatory of Network Interference (OONI), Sinar Project, and a group of independent Hong Kong researchers collaborated on a joint study to evaluate the state of internet censorship in Hong Kong. In this report, the team uses the collection and analysis of network measurements to examine the extent of internet censorship events in the country.

This study aims to increase the transparency of internet controls in Hong Kong. This report is the third of the series, and it highlights the socioeconomic background, legal landscape, as well as the network landscape that potentially affects internet censorship in the country, followed by censorship findings based on the data collected.

Selected scope of ISPs in this report:

- AS4515 & AS4760 & AS38819 - PCCW HKT
- AS9231 & AS131872 - China Mobile Hong Kong
- AS9269 & AS9381 & AS10103 - Hong Kong Broadband Network
- AS9304 & AS10118 - Hutchison Global Communications (Hong Kong)
- AS9908 - HK Cable TV
- AS17924 - SmarTone Mobile Communications

Background

Population	7.5 million[1]
Internet penetration (% of population using the internet)	96.6%[2]
Mobile subscriptions (per 100 inhabitants)	292[3]
Freedom on the Net ranking	Not available
Religion (%)	Other or no religion: 54.3%, Buddhism or Taoism: 27.9%, Protestant: 6.7%, Roman Catholic: 5.3%, Islam: 4.2%, Hinduism: 1.4%, Sikhism: 0.2%[4]
ICCPR Ratification	No

Hong Kong, a special administrative region of China,[5] is an ex-colony of the United Kingdom and was previously known as one of the most popular free ports and major trade centres in Asia. Its population of roughly 7.5 million is 100% urban[6] and inclusively spans across different ethnicities and religions.

Historically, Great Britain signed the "Sino-British Joint Declaration" with the People's Republic of China to resolve the "Agreement on the Future of Hong Kong" for both countries. China regained sovereignty to the ex-colony in July 1997 and "preserves Hong Kong's familiar legal system and the rights and freedoms enjoyed there."[7] In contrast to China, Hong Kong looks up to the principle of "One Country, Two Systems",[8] the very foundation of the organic "Hong Kong Basic Law".[9]

[1] The Government of the Hong Kong Special Administrative Region. (2024, February 20). Year-end Population for 2023 [20 Feb 2024]. *Census and Statistics Department*. https://www.censtatd.gov.hk/en/press_release_detail.html?id=5386

[2] The Government of the Hong Kong Special Administrative Region. (2024, June 27). Thematic Household Survey Report - Report No. 80 - Internet and Personal Computer Penetration. *Census and Statistics Department*. https://www.censtatd.gov.hk/en/wbr.html?ecode=B11302012024XX02&scode=453

[3] World Bank (2022) https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=HK

[4] CIA (2016). *The World Factbook – Hong Kong*. https://www.cia.gov/the-world-factbook/countries/hong-kong/

[5] 中华人民共和国行政区划. (2005). http://www.gov.cn/test/2005-06/15/content_18253.html

[6] https://www.cia.gov/the-world-factbook/countries/hong-kong/

[7] Speech signing the Joint Declaration | Margaret Thatcher Foundation. (1984, December 19). https://www.margaretthatcher.org/document/105817

[8] Horace Yeung, & Flora Huang. (2015). "One Country Two Systems" as Bedrock of Hong Kong's Continued Success: Fiction or Reality? Boston College International and Comparative Law Review, 38(2), 191. http://repository.essex.ac.uk/18431/

[9] Basic Law - Home (EN). (n.d.). https://www.basiclaw.gov.hk/en/index/

Politically, Hong Kong has been governed by a hybrid regime[10] since July 1997. The Chief Executive is the head of government,[11] and the Standing Committee of the National People's Congress is in charge of appointing the elected Chief Executive.[12] Chief Executive candidates are vetted and approved only by the Committee for Safeguarding National Security without a straightforward appeal mechanism.[13]

In 2019 and early 2020, citizens of Hong Kong demonstrated widespread Anti-ELAB (Anti Extradition Law Amendment Bill) protests in response to the amendment bill on extradition conditions for fugitive offenders proposed by the Hong Kong government. On 30 June 2020, the Standing Committee of the National People's Congress unanimously decided[14,15] to enact and implement the Hong Kong National Security Law. A countermeasure to the mass protests on the street, this law established the legislative power for local authorities to implement censorship based on national security grounds.

In 2023, an amendment was passed to a law to eliminate most directly elected states on local district councils, thus reducing the proportion of directly elected seats from some 90% to just about 20%. These seats were the last major political representative bodies chosen by the public, and now the rest of the seats will be filled by members appointed by the chief executive. There will also be a vetting process for all incoming councilors to ensure "patriotism".

The 2023 Hong Kong District Council elections were held 10 December 2023 for all 18 District Councils of Hong Kong. This election was the first after the passing of the National Security Law in 2020 and the electoral changes.

[10] Cheng, E. W. (2016). Street Politics in a Hybrid Regime: The Diffusion of Political Activism in Post-colonial Hong Kong. The China Quarterly, 226, 383–406. https://doi.org/10.1017/s0305741016000394

[11] Basic Law - Basic Law - Chapter II (EN). (n.d.). https://www.basiclaw.gov.hk/en/basiclaw/chapter2.html

[12] Basic Law - Basic Law - Chapter II (EN). (n.d.). https://www.basiclaw.gov.hk/en/basiclaw/chapter2.html

[13] Improve Electoral System - Candidate Eligibility Review Mechanism. (n.d.). https://www.cmab.gov.hk/improvement/en/qualification-review/index.html

[14] Presidium elected, agenda set for China's annual legislative session. (n.d.). http://www.npc.gov.cn/englishnpc/c23934/202005/ce05b9dfce7546209e6630e7ba73a653.shtml

[15] Regan, H. (2020, June 30). China passes sweeping Hong Kong national security law. CNN. https://edition.cnn.com/2020/06/29/china/hong-kong-national-security-law-passed-intl-hnk/index.html

Legal Environment

There have been no updates since the 2022 edition of this report.

Hong Kong Basic Law

The Hong Kong Basic Law, which serves as organic law, is also seen as a constitutional document[16] by the Hong Kong government. It guarantees that all residents of Hong Kong are equal before the law and possess inviolable rights to "freedom of speech, of the press and of publication; freedom of association, of assembly, of procession and of demonstration; and the right and freedom to form and join trade unions, and to strike".[17]

Legislative Context

At present, there are three major criminal laws pertaining to computer crimes in Hong Kong:

- Cap. 106 Telecommunications Ordinance
    - Section 27A Unauthorized access to computer by telecommunications
- Cap. 200 Crimes Ordinance
    - Section 60 Destroying or damaging property
    - Section 161 Access to computer with criminal or dishonest intent

Over the past ten years, certain computer crime cases have been dismissed differently because of frail to no evidence of the defendant purposefully stealing or gaining without authorization information from online information systems.

For instance, on 3 July 2019, a flight passenger Chan was released from court with a bind-over condition,[18] only because he discovered that an electronic boarding pass website leaked information to other users by changing a few characters in the web address field. In this court case, Chan stated that he had notified the airline company and the Privacy Commissioner for Personal Data immediately after discovering the vulnerability. However, there were no replies from both parties for three weeks. Instead, Chan was arrested and prosecuted for "unauthorized access to computer by telecommunications" by the authorities, who accused Chan of having accessed the personal information of other passengers.

[16] Basic Law - Home (EN). (n.d.). https://www.basiclaw.gov.hk/en/index/
[17] Basic Law - Basic Law - Chapter III (EN). (n.d.). https://www.basiclaw.gov.hk/en/basiclaw/chapter3.html
[18] 港航網上系統現漏洞 男乘客通告不果反被指取用資料 准守行為. (2019, July 3). 香港01. https://web.archive.org/web/20221021043142/https://www.hk01.com/%E7%A4%BE%E6%9C%83%E6%96%B0%E8%81%9E/347780/%E6%B8%AF%E8%88%AA%E7%B6%B2%E4%B8%8A%E7%B3%BB%E7%B5%B1%E7%8F%BE%E6%BC%8F%E6%B4%9E-%E7%94%B7%E4%B9%98%E5%AE%A2%E9%80%9A%E5%91%8A%E4%B8%8D%E6%9E%9C%E5%8F%8D%E8%A2%AB%E6%8C%87%E5%8F%96%E7%94%A8%E8%B3%87%E6%96%99-%E5%87%86%E5%AE%88%E8%A1%8C%E7%82%BA

A better illustration of the legislative landscape would be the recent judicial review filed by Hong Kong citizen Cheuk-Kin Kwok. The applicant hopes to stop the government from nullifying vaccination exemption letters through a declaration in the Gazette. However, soon after the court ruled in favor of Kwok, Chief Executive John Lee Ka-Chiu amended the law, empowering concrete legal rights to the health secretary in nullifying exemption letters upon “reasonable grounds”.

Also, as the current ruling party in Hong Kong took sides with Beijing, this led to great convenience for the government and pro-Beijing parties on policy-making and legislative changes. For example, on 21 October 2022, the Hong Kong government published in the Gazette an amendment bill proposal to the Cap. 138A “Pharmacy and Poisons Regulations” to further restrict antipyretic drug sales.[19] Without any opposition from the Legislative Council, drugs like aspirin and paracetamol will be added to the “Schedule 1” list of poisons in a year. General citizens then can only purchase simple painkillers like Tylenol and Panadol (common brand names for paracetamol) from registered pharmacies, dispensaries, government-sanctioned “listed sellers of poisons”, or clinics. On the complementary side, Cap. 134 “Dangerous Drugs Ordinance” rules that the possession of poisons listed in “Schedule 1” can lead to fines or imprisonment for up to 7 years.

Hong Kong National Security Law & Legislative Reform

Currently, there are a total of 66 articles inside the Hong Kong National Security Law in effect, with three prominent articles affecting the global population:

- Article 38: This Law applies to offenses committed against the Hong Kong Special Administrative Region from outside the Region by a person who is not a permanent resident of the Region.
- Article 43: The department for safeguarding national security of the Police Force of the Hong Kong Special Administrative Region may “require a person, who is suspected, on reasonable grounds, of having in possession information or material relevant to investigation, to answer questions and furnish such information or produce such material.”
- Article 47: The courts of the Hong Kong Special Administrative Region shall obtain a certificate from the Chief Executive to certify whether an act involves national security or whether the relevant evidence involves State secrets when such questions arise in the adjudication of a case. The certificate shall be binding on the courts.

[19] Pharmacy and Poisons (Amendment) (No. 5) Regulation 2022. (n.d.). https://www.legco.gov.hk/yr2022/english/subleg/negative/2022ln194-e.pdf

As of writing, there are no valid explanations or justifications from court judgements or valuable legislative perspectives for cybercrime charges using the Hong Kong National Security Law.

The Law Reform Commission of Hong Kong has put together a cybercrime-specific legislative reforming committee.[20] On July 2022, the sub-committee published a consultation paper[21] that proposed five cybercrime categories: “illegal access to program or data”, “illegal interception of computer data”, “illegal interference of computer data”, “illegal interference of computer system”, and “making available or possessing a device or data for committing a crime” in the documents from the committee.

Safeguarding National Security Ordinance

In March 2024, Hong Kong passed a new security local law, and it took only 11 days for the Ordinance to be passed unanimously. According to Human Rights Watch, this new law would “eliminate the last vestiges of fundamental freedoms in the city” as it “makes the freedoms of association, assembly, and peaceful civil society activism criminal offenses”.

The ordinance is enacted to implement the new Article 23 of the Hong Kong Basic Law; where it states that Hong Kong “shall enact laws on its own to prohibit any act of of treason, secession, sedition, subversion against the Central People's Government, or theft of state secrets, to prohibit foreign political organizations or bodies from conducting political activities in the Region, and to prohibit political organizations or bodies of the Region from establishing ties with foreign political organizations or bodies."

Regarding this law, Amnesty International is of the viewpoint that “it introduces mainland China’s definition of “national security” and “state secrets” which is extremely broad and can relate to any economic, social, technological or scientific developments, even when they have never been officially classified as secrets”. The law also creates a new offense that is “collaborating with external forces with intent to bring about an interference effect and uses improper means” and carries a maximum 14-year sentence. Furthermore, it expands the scope of “espionage” to if one publishes false or misleading information through the “collaborations”. These external forces could include foreign governments, foreign political parties, international organizations, foreign organizations that pursue political ends, as well as any related individual or party to these organizations.

[20] Cybercrime Sub-committee of the Law Reform Commission. (n.d.). https://www.hkreform.gov.hk/en/projects/cybercrime.htm

[21] Cybercrime Sub-committee of the Law Reform Commission. (2022). Cyber-Dependent Crimes and Jurisdictional Issues: (HKLRC Consultation Paper). The Law Reform Commission of Hong Kong. https://www.hkreform.gov.hk/en/publications/cybercrime.htm

Additionally, the law expands the scope of the sedition law and increases the maximum jail sentence from two years to seven years. Freedom of speech is almost totally restricted, as criticism towards the government can lead up to 10 years of imprisonment. Furthermore, the law explicitly states that "that an intention to incite violence is not necessary to convict a person of sedition, contrary to the common law principle that speech that doesn't incite violence should not be punished under the law." This means that any criticism of the Hong Kong or Chinese government could potentially fall under its scope. As the diaspora community is also targeted, the law can be used to punish Hong Kong residents who have moved abroad and committed national security offenses by taking measures to cancel passports or suspend professional qualifications. This may further exacerbate the state of censorship, including on the internet.

The new law also obliges any Chinese citizens to notify the police if they know that another person has committed, or is about to commit, treason. Furthermore, the new law grants extra powers for police and fewer legal rights for detainees, as it prohibits consultation with any lawyer in the first 48 hours after their arrest or a chosen lawyer while in detention.

In terms of technology, the law includes an offense on "endangering national security in relation to computers or electronic systems", where the terms are as broad as the rest in the law but has potential for imprisonment of up to 20 years.

Reported Cases of Internet Censorship

During the period of censorship, the Wikipedia page Internet censorship in Hong Kong reported several websites to be blocked:

- hkchronicles.com
- hkleaks.info
- blockedbyhk.com
- goodhope.school
- www.tjc.gov.tw
- twtjcdb.tjc.gov.tw
- www.pct.org.tw
- www.dpp.org.tw
- 2021hkcharter.com
- 8964museum.com
- 8964tiananmen.com
- www.hongkongwatch.org
- www.hkdc.us
- www.goarmy.com*
- samuelbickett.substack.com

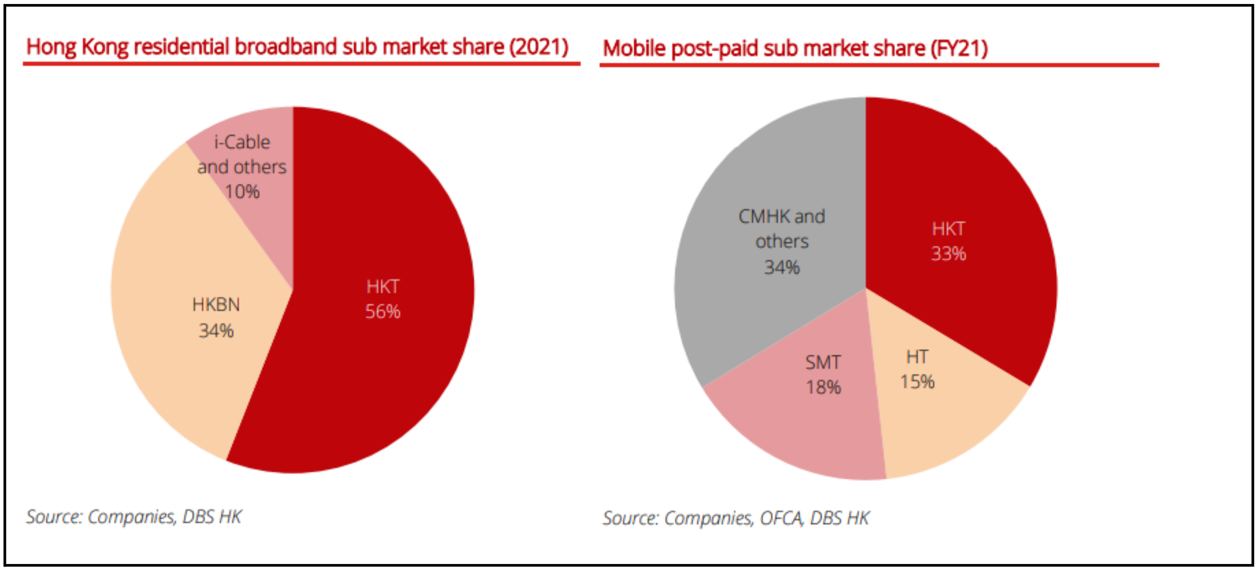
Note: www.goarmy.com may have been geoblocked based on the 2023 edition of the report.

Following the new security law, there had been reports of self-censorship, particularly in the art industry.

Network Landscape

(No update since the 2022 edition)

Prominent internet service providers (ISPs) in Hong Kong include PCCW-Hong Kong Telecom (HKT), Hong Kong Broadband Network Limited (HKBN), China Mobile Hong Kong Company Limited (CMHK), SmarTone Telecommunications Holdings Limited, Hutchison Telecommunications Hong Kong Holdings Limited (HT), and i-Cable. The charts below illustrate their respective market shares in terms of residential broadband and mobile internet:



Source: DBS Group Research on Hong Kong Telecom Sector

In April 2020, 5G services were commercially launched. In the meantime, local mobile network operators (MNOs) have been actively rolling out their 5G networks. At present, 5G coverage in Hong Kong has exceeded 90% of the population.[22]

[22] https://www.5g.gov.hk/en/what-is-5g/coverage.html

Findings on Internet Censorship in Hong Kong

All of the findings are based on data collected through OONI from 1 July 2023 to 30 June 2024.

Blocking of Websites

Throughout the one-year period, 1.8 measurements from 2,558 websites were tested. As of 30 June 2024, the test list contained 1,666 websites in the Global Test List and 143 websites in the Hong Kong Test List.

	Jul-Sep 2023	Oct-Dec 2023	Jan-Mar 2024	Apr-Jun 2024	Total
Measured	567,348	361,152	435,069	455,269	1,818,838
Domain	2,217	2,236	2,305	2,493	2,558
ASNs	43	36	44	45	81

Table 1: Summary of OONI web connectivity measurements for Hong Kong from 1 July 2023 to 30 June 2024.

Based on OONI data, there is no known block page found in Hong Kong. It is also difficult to analyze known blocked websites as most of them are now inactive, making it challenging to confirm any blocking for Hong Kong. Currently, existing confirmed blockings for Hong Kong in OONI data appear to be false positives. Hence, we found confirmed blockings manually through the Wikipedia page on Internet censorship in Hong Kong, corroborated these with OONI data, and eliminated pages that are no longer active. Using this method, three confirmed blocked websites were found:

Domain	Website description
www.hongkongwatch.org	Hong Kong Watch is an NGO based in the UK that monitors the conditions of human rights, freedoms, and rule of law in Hong Kong.[23]
8964museum.com	An online museum which documented stories of the June 4 Tiananmen crackdown.[24]
samuelbickett.substack.com	A political commentary blog by an American lawyer.

[23] https://en.wikipedia.org/wiki/Hong_Kong_Watch

[24] https://www.thestandard.com.hk/breaking-news/section/4/178192/June-4-museum-goes-online

Unlike other countries under iMAP where heuristics based on blocking fingerprints and weighted anomaly ratio is calculated to obtain confirmed or likely blockings (further details as in Annex IV), domains that exceeded the threshold of weighted anomaly ratio (90%) are no longer active. Whereas for websites that are reportedly blocked, the weighted anomaly ratio at the domain level was found to be too low (e.g. 43% for www.hongkongwatch.org), likely due to the high number of ASNs.

However, by ASN, the anomaly is more prevalent:

Hong Kong Watch website

ASN	Network Name	Weighted anomaly rate
4515	PCCW HKT	0.00%
4760	PCCW HKT	4.81%
9231	China Mobile Hong Kong	30.00%
9269	Hong Kong Broadband Network	50.82%
9304	Hutchison Global Communications (Hong Kong)	0.00%
9381	Hong Kong Broadband Network	27.27%
9908	HK Cable TV	0.00%
10118	Hutchison Global Communications (Hong Kong)	13.33%
17924	SmarTone Mobile Communications	70.00%
38819	PCCW HKT	0.00%

8964 Online Museum website

ASN	Network Name	Weighted anomaly rate
4515	PCCW HKT	0.00%
4760	PCCW HKT	38.86%
9231	China Mobile Hong Kong	30.00%
9269	Hong Kong Broadband Network	48.76%
9304	Hutchison Global Communications (Hong Kong)	0.00%
9381	Hong Kong Broadband Network	0.00%
9908	HK Cable TV	0.00%
10118	Hutchison Global Communications (Hong Kong)	57.14%
17924	SmarTone Mobile Communications	12.86%

Samuel Bickett Substack

ASN	Network Name	Weighted anomaly rate
10118	Hutchison Global Communications (Hong Kong)	15.00%
38819	PCCW HKT	30.00%

Government Category

Similar to the 2023 edition, it was found that a large number of government websites, particularly related to the US military, resulted in anomaly or failure under OONI testing. This is consistent with Censored Planet's findings in 2020, where they reported that these websites were geoblocked from Hong Kong.

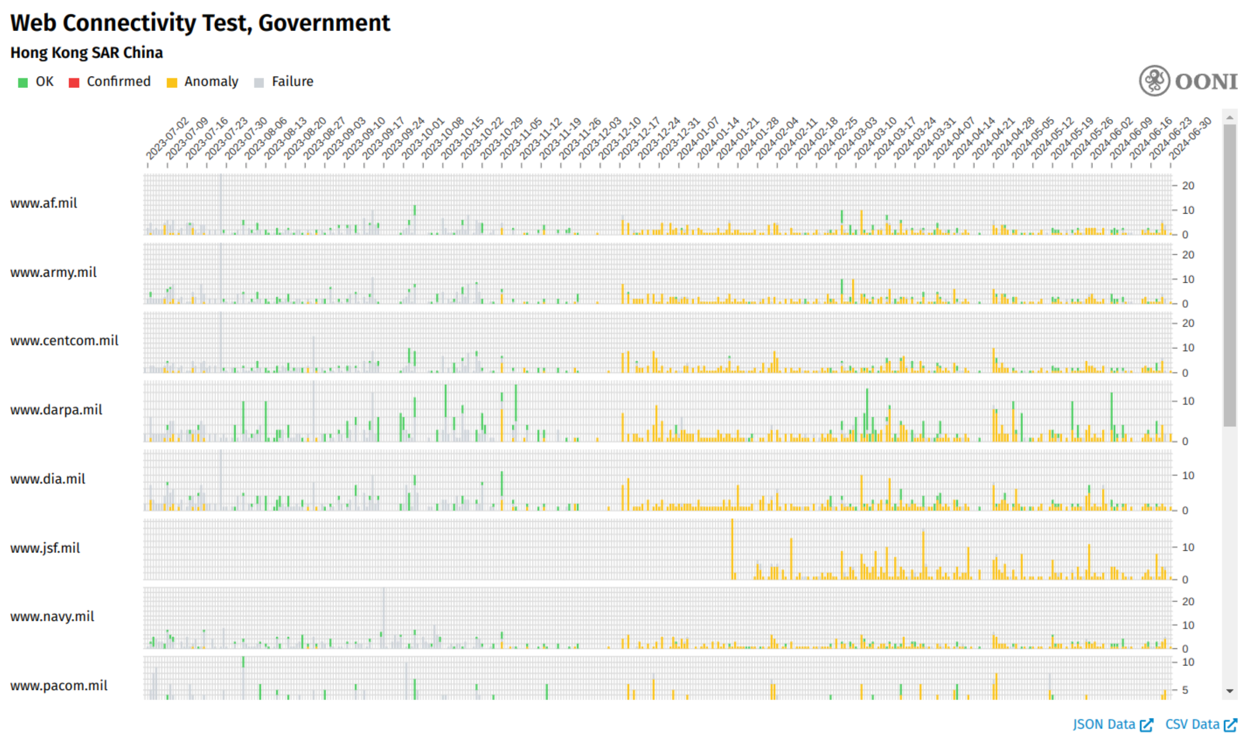


Figure 1: Potentially blocked websites in the Government category.

Methods of Blocking of Websites

There have been no block pages detected in Hong Kong based on OONI's measurements.

Using 8964museum.com to analyze the methods of censorship in the country, it was found that the methods used include DNS tampering where the address resulted in a nxdomain error, TLS, and TCP.

Findings on Internet Takedowns

Based on the Google Transparency Report, the government had requested Google to remove 164 items on its sites in the first half of 2023, with over 30% of those related to privacy and security issues. The 164 items include five YouTube videos featuring a documentary about an imprisoned activist during the 2019 unrest in Hong Kong and a Google Drive folder URL of a form that encouraged participants to submit videos of themselves singing the protest song.

Acknowledgement of Limitations

- **Period of study**
  To examine the most recent censorship trends and events, we limited the findings of this study to OONI network measurements collected from 1 July 2023 to 30 June 2024.

- **Vantage points**
  Although OONI network measurements were collected from several vantage points in Hong Kong, the OONI Probe tests were not run consistently on each network, nor on all networks in the country.

- **Use of domain as a unit of measurement of websites**
  In general, "URL" (or in OONI's terms - input) and "domain" are interchangeable terms used to refer to a website. In the OONI test list, the full URLs are input in the probe to be tested for censorship, similar to a URL starting with "https" or "http" in a browser. The URLs are measured for censorship by OONI Probe with the Web Connectivity experiment, which is designed to measure whether access to tested URLs is interfered with through DNS tampering, TCP/IP blocking, an HTTP transparent proxy, or through TLS interference. However, when analyzing results on OONI, the reader should be aware that there are differences in the numbers concerning the specific input or domain, as a different volume of measurements may have been collected for a URL (e.g. https://www.hrw.org/asia/cambodia) in comparison to a domain (e.g. www.hrw.org).

  In the 2023 report, we based our analysis primarily on URLs because they were thought to provide more context on the reason why the web page was blocked and could be categorized more similarly to the Citizen Lab test lists, which are URL format. However, in this 2024 report, we based our analysis on domains, so readers will need to be cautious about making year-to-year comparisons.

- **Confirmed blockings vs. Likely blockings or Inaccessible**
  The confirmed blocked websites are based on the data where the testing result shows a trace to a government or ISP block page. This typically means a block page is served when the user tries to access the website on a particular network or that DNS resolution returns an IP address associated with censorship. These cases are automatically annotated as "confirmed blocked" based on fingerprints added to OONI's database. When a website is found to be confirmed blocked, it may be blocked only on specific networks and remain accessible on the rest. Confirmed blockings may also be specific based on the URL; for example, https://abc.com/ may be censored but not https://www.abc.com/.

In this 2024 report, confirmed blockings and likely blockings were consolidated based on the country. See the section on verifying OONI measurements.

- **Test lists**
  The websites tested for censorship on OONI are either from the Citizen Lab test lists or additional websites tested by OONI Probe users. While the websites in the test lists are categorized based on specific standardized categories, the percentage of blocked or likely blocked cases may not necessarily reflect the entire state of internet censorship in the country, as only sampled websites are included in the testing.

- **Differences in numbers with OONI data**
  The findings in this report were obtained after further processing the data from OONI. This involved obtaining more confirmed blockings and eliminating false positives through additional heuristics and manual verification by iMAP researchers based on country or local context. While these heuristics will eventually be added to OONI's fingerprints, OONI will only process them for future testing.

  Additionally, iMAP researchers have categorized blocked websites that were not part of the Citizen Lab test lists but were tested on OONI via custom test lists. Hence, the figures in this report may differ from the results on OONI Explorer.

- **Testing of instant messaging apps and circumvention tools**
  The instant messaging apps and circumvention tools are limited to those tested on OONI. Therefore, the results may not reflect the state of censorship of apps more commonly used in individual countries.

- **Lack of local researchers to verify most of the report findings**
  As the situation in Hong Kong has become more restrictive, collaboration with our local researchers is increasingly challenging. As such, no local researcher was able to verify most of the findings in this report. The findings in this report are based on research that was found in publicly available resources.

Conclusion

As in previous editions of the iMAP report in Hong Kong, internet censorship was observed in the categories of political criticism websites, human rights websites, and government (US military) websites. This is in contrast to other countries in the region where porn, gambling, and online scam websites are the most commonly blocked.

With the new security law in place where internet freedom continues and be increasingly restricted, these incidences of internet censorship are expected to continue, especially when criticism towards the government is criminalized.

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 on Mobile (iOS and Android) and Desktop, including on the CLI on Linux platforms. The domains you test can be either randomly selected from the Citizenlab Test Lists or custom test lists specific to your needs.
- Contribute to the test lists on GitHub or on OONI.
- Translate the OONI Probe to your local language here.
- Participate in community discussions on the OONI Slack channel or our Volunteers Telegram Channel.

Acknowledgements

We would like to thank local partners, activists, academicians, researchers, and anonymous users in Hong Kong for their assistance in running the OONI Probe.

We would like to thank Khairil Yusof (Sinar Project) for his supervision and advisory support on the overall iMAP project, as well as Numan Afifi (Sinar Project) for his valuable contributions in copyediting and report design.

Annex I: List of Confirmed Blockings

Domain	Link to OONI Explorer
www.hongkongwatch.org	https://explorer.ooni.org/chart/mat?probe_cc=HK&since=2023-07-01&until=2024-07-01&time_grain=day&axis_x=measurement_start_day&axis_y=domain&test_name=web_connectivity&domain=www.hongkongwatch.org
8964museum.com	https://explorer.ooni.org/chart/mat?probe_cc=HK&since=2023-07-01&until=2024-07-01&time_grain=day&axis_x=measurement_start_day&axis_y=domain&test_name=web_connectivity&domain=8964museum.com
samuelbickett.substack.com	https://explorer.ooni.org/chart/mat?probe_cc=HK&since=2023-07-01&until=2024-07-01&time_grain=day&axis_x=measurement_start_day&axis_y=domain&test_name=web_connectivity&domain=samuelbickett.substack.com

Annex II: List of ISPs

Selected scope of ISPs in this report:

- AS4515 & AS4760 & AS38819 - PCCW HKT
- AS9231 & AS131872 - China Mobile Hong Kong
- AS9269 & AS9381 & AS10103 - Hong Kong Broadband Network
- AS9304 & AS10118 - Hutchison Global Communications (Hong Kong)
- AS9908 - HK Cable TV

AS17924 - SmarTone Mobile Communications

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 second 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 (China), Indonesia, Malaysia, Myanmar, Philippines, Thailand, India, Vietnam and Timor-Leste.

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.

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. 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><b>Confirmed blocking</b></td><td colspan="5">What information can we get about the IP by doing a whois lookup?</td></tr>
<tr><td rowspan="6"></td><td>Government entity</td><td>Local ISP[25]</td><td colspan="3">CDN[26] / Private IP</td></tr>
<tr><td>⬇</td><td>⬇</td><td colspan="3">⬇</td></tr>
<tr><td><b>Confirmed blocking</b></td><td><b>Likely Blocked or Inaccessible</b></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></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></tr>
<tr><td></td><td><b>False positive</b></td><td><b>Confirmed blocking</b></td><td>Sampled measurement is analyzed on</td></tr>
</table>

[25] 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.

[26] 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%.