



Internet Monitoring Action Project

# iMAP Hong Kong (China) 2023 Internet Censorship Report

By Independent Researchers (Anonymous),  
Siti Nurliza Samsudin (Sinar Project) and Kelly Koh (Sinar Project)

Published/Produced by Sinar Project  
[team@sinarproject.org](mailto:team@sinarproject.org)  
<https://sinarproject.org>

© Sinar Project 2023  
[Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)

## **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 ten countries: Myanmar, Cambodia, Hong Kong (China), India, Indonesia, Malaysia, Philippines, Thailand, Timor-Leste, 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](https://imap.sinarproject.org). Any enquiries and suggestions about this report can be directed to [team@sinarproject.org](mailto: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 public affairs of the nation by making the Parliament and the Malaysian Government more open, transparent and accountable. More information is available at <https://sinarproject.org>.

## **How to Use This Report**

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

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

## 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 Organizations
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 Contents**

<b>About iMAP</b>	<b>2</b>
<b>About Sinar Project</b>	<b>2</b>
<b>How to Use This Report</b>	<b>2</b>
<b>Abbreviations</b>	<b>3</b>
<b>Table of Contents</b>	<b>5</b>
<b>Key Findings</b>	<b>6</b>
<b>Introduction</b>	<b>6</b>
<b>Background</b>	<b>6</b>
Legal Environment	8
Hong Kong Basic Law	8
Legislative Context	8
Hong Kong National Security Law & Legislative Reform	9
Reported Cases of Internet Censorship	11
Network Landscape	11
<b>Findings on Internet Censorship in Hong Kong</b>	<b>12</b>
Blocking of Websites	12
Confirmed Blockings	14
Political Criticism	14
Government	15
Methods of Blocking of Websites	16
Blocking of Instant Messaging Apps	17
Blocking of Circumvention Tools	17
<b>Acknowledgement of Limitations</b>	<b>18</b>
<b>Conclusion</b>	<b>20</b>
Contribute to the study	20
<b>Acknowledgements</b>	<b>20</b>
<b>Annex I: List of confirmed blockings</b>	<b>21</b>
<b>Annex II: List of ISPs</b>	<b>22</b>
<b>Annex III: Glossary</b>	<b>27</b>
<b>Annex IV: Methodology</b>	<b>29</b>
Data	29
Coverage	29
How are the network measurements gathered?	29
How are the network measurements analysed?	29
Country code	30
Autonomous System Number (ASN)	30
Date and time of measurements	30
Categories	30
IP addresses and other information	32
Network measurements	33
Verifying OONI measurements	35

## Key Findings

- The key findings of the study showed that internet censorship in Hong Kong is mainly affecting 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

Since the enactment of the Hong Kong national security law until the present moment, at least four political and dissident-related websites have been nationally blocked on national security grounds. Freedoms of speech, civil society, and pro-democratic press, and publication have also suffered from high-pressure crackdowns from local authorities, as reported in the 135th session of the UN Human Rights committee.

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. Throughout this report, the team examines whether internet censorship events persist in the country through the collection and analysis of network measurements.

This study aims to increase the transparency of internet controls in Hong Kong. This report is the second 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 findings based on the data collected.

## Background

<b>Population</b>	7.4 million <sup>1</sup>
<b>Internet penetration (% of population using the internet)</b>	96% <sup>2</sup>
<b>Mobile subscriptions (per 100 inhabitants)</b>	292 <sup>3</sup>

<sup>1</sup> World Bank (2022) <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=HK>

<sup>2</sup> World Bank (2022) <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=HK>

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

<b>Freedom on the Net ranking (2022)</b>	42/100; Partly free <sup>4</sup>
<b>Religion (%)</b>	Other or no religion: 54.3%, Buddhist or Taoist: 27.9%, Protestant: 6.7%, Roman Catholic: 5.3%, Muslim: 4.2%, Hindu: 1.4%, Sikh: 0.2% <sup>5</sup>
<b>ICCPR Ratification</b>	No

Hong Kong, a special administrative region of China,<sup>6</sup> 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 7.4 million is 100% urban<sup>7</sup> 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.”<sup>8</sup> In contrast to China, Hong Kong looks up to the principle of “One Country, Two Systems”<sup>9</sup>, the very foundation laid in the organic “Hong Kong Basic Law”.<sup>10</sup>

Politically, Hong Kong has been governed by a hybrid regime<sup>11</sup> since July 1997. The Chief Executive is the head of government.<sup>12</sup> The Standing Committee of the National People’s Congress is in charge of appointing the elected Chief Executive.<sup>13</sup> Chief Executive candidates are vetted and only approved by the Committee for Safeguarding National Security without a straightforward appealing mechanism.<sup>14</sup>

In 2019 and early 2020, citizens of Hong Kong demonstrated widespread Anti-ELAB (Anti Extradition Law Amendment Bill) protests in responding to the amendment bill on extradition conditions for fugitive offenders proposed by the Hong Kong government. On 30 June 2020,

<sup>4</sup> Freedom House (2022). *Freedom in The World 2023*.

<https://freedomhouse.org/country/hong-kong/freedom-world/2023>

<sup>5</sup> CIA (2016). *The World Factbook – Hong Kong*.

<https://www.cia.gov/the-world-factbook/countries/hong-kong/>

<sup>6</sup> 中华人民共和国行政区划. (2005). [http://www.gov.cn/test/2005-06/15/content\\_18253.html](http://www.gov.cn/test/2005-06/15/content_18253.html)

<sup>7</sup> <https://www.cia.gov/the-world-factbook/countries/hong-kong/>

<sup>8</sup> Speech signing the Joint Declaration | Margaret Thatcher Foundation. (1984, December 19).

<https://www.margaretthatcher.org/document/105817>

<sup>9</sup> 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/>

<sup>10</sup> Basic Law - Home (EN). (n.d.). <https://www.basiclaw.gov.hk/en/index/>

<sup>11</sup> 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>

<sup>12</sup> Basic Law - Basic Law - Chapter II (EN). (n.d.).

<https://www.basiclaw.gov.hk/en/basiclaw/chapter2.html>

<sup>13</sup> Basic Law - Basic Law - Chapter II (EN). (n.d.).

<https://www.basiclaw.gov.hk/en/basiclaw/chapter2.html>

<sup>14</sup> Improve Electoral System - Candidate Eligibility Review Mechanism. (n.d.).

<https://www.cmab.gov.hk/Improvement/en/qualification-review/index.html>

the Standing Committee of the National People's Congress unanimously decided<sup>15,16</sup> 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%. The 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 councillors to ensure “patriotism”.

The 2023 Hong Kong District Council elections are scheduled on 10 December 2023 for all 18 District Councils of Hong Kong. This election will be the first after the passing of the National Security Law in 2020 and the electoral changes.

## Legal Environment

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

### Hong Kong Basic Law

The Hong Kong Basic Law, which served as organic law, is also seen as a constitutional document<sup>17</sup> by the Hong Kong government. It has guaranteed 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”.<sup>18</sup>

### Legislative Context

There are three major criminal laws currently ruling 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, some computer crime cases have been dismissed differently because of frail to no evidence of the defendant purposefully stealing or without authorization to gain information from online information systems.

---

<sup>15</sup> Presidium elected, agenda set for China's annual legislative session. (n.d.).

<http://www.npc.gov.cn/englishnpc/c23934/202005/ce05b9dfce7546209e6630e7ba73a653.shtml>

<sup>16</sup> 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>

<sup>17</sup> Basic Law - Home (EN). (n.d.). <https://www.basiclaw.gov.hk/en/index/>

<sup>18</sup> Basic Law - Basic Law - Chapter III (EN). (n.d.).

<https://www.basiclaw.gov.hk/en/basiclaw/chapter3.html>



For instance, on 3 July 2019, a flight passenger Chan was released from court with a bind-over condition,<sup>19</sup> only because he found out the 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 immediately notified the airline company and the Privacy Commissioner for Personal Data right after discovering the vulnerability. However, there were no replies from both parties after three weeks. Instead, Chan was then arrested and prosecuted for “unauthorized access to computer by telecommunications” by the authorities, accusing Chan of having accessed the personal information of other passengers.

A side note to better illustrate 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 ruling in favour 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, given that the current ruling party in Hong Kong took sides with Beijing, this curated 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<sup>20</sup>. 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 offences under this Law 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 ... requiring a person, who is suspected, on reasonable grounds, of having in possession information or material

<sup>19</sup> 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>

<sup>20</sup> Pharmacy and Poisons (Amendment) (No. 5) Regulation 2022. (n.d.).

<https://www.legco.gov.hk/yr2022/english/subleg/negative/2022In194-e.pdf>

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.

As of writing, no court judgements or valuable legislative perspectives give valid explanations and justification for cybercrime charges using the Hong Kong National Security Law.

The Law Reform Commission of Hong Kong has gathered a cybercrime-specific legislative reforming committee<sup>21</sup>. On July 2022, the sub-committee published a consultation paper<sup>22</sup>. Inside, it proposes 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.

---

<sup>21</sup> Cybercrime Sub-committee of the Law Reform Commission. (n.d.).

<https://www.hkreform.gov.hk/en/projects/cybercrime.htm>

<sup>22</sup> 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>

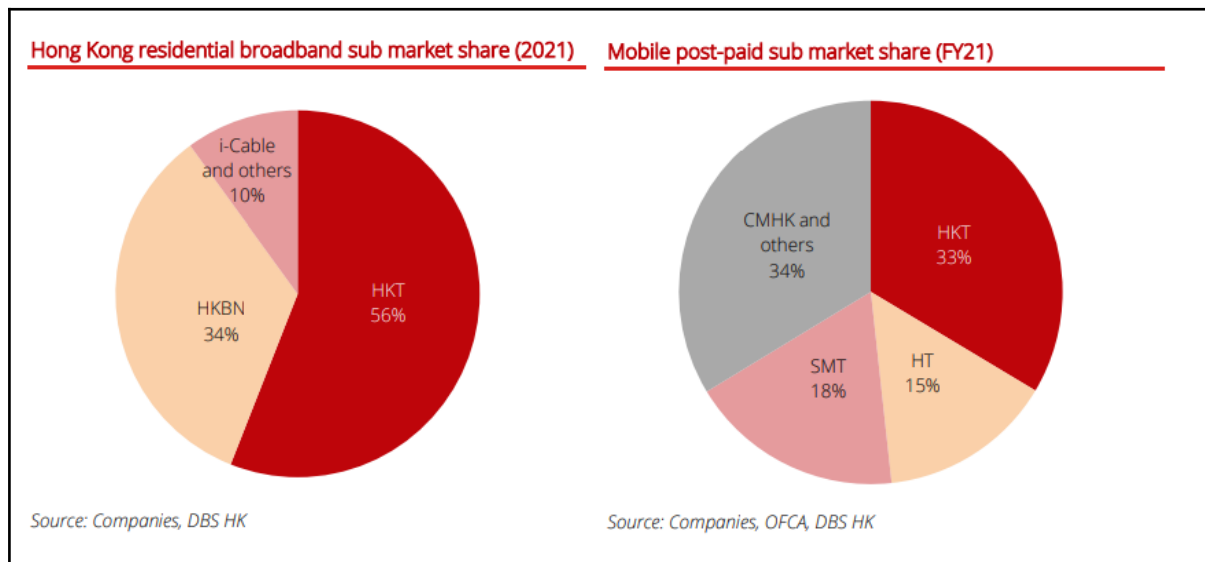
## Reported Cases of Internet Censorship

In 2023, Hong Kong has reported several cases of website blockings:

- [Singapore newspaper article on Biden's 'dictator' comment blocked in Hong Kong](#)
- [Blocking of GitLab in Apple phones](#)
- [Blocking of website belonging to HKDC](#), i.e., Hong Kong Democracy Council, an organisation for Hong Kong people in the United States.

## Network Landscape

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 show 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.<sup>23</sup>

<sup>23</sup> <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 2022 to 30 June 2023.

### Blocking of Websites

Throughout the one-year period, 2.4 million measurements from 3,397 websites were tested on OONI. As of 30 June 2023, the test list contained 1,629 websites in the Global Test List and 609 websites in the Hong Kong Test List. Based on OONI measurements, we will generally use the following terms in this report:

- **Measured or Measurement Counts:** Refers to the total number of measurements collected through OONI Probe.
- **Blocked:** Refers to “Confirmed Blocked” in OONI measurements, which are measurements from websites that are automatically confirmed to be blocked (e.g., a block page was served).
- **Likely Blocked:** Refers to “Anomaly” and “Failure” in OONI measurements. Anomalies are measurements that show signs of potential blocking ;however, [false positives](#) can occur. Failures refer to failed experiments in OONI testing, although they can sometimes be [symptomatic of censorship](#) (except in India).

	Jul-Sep 2022	Oct-Dec 2022	Jan-Mar 2023	Apr-Jun 2023	Total
Measured	652,948	598,797	467,792	648,443	2,367,980
Blocked	0	0	64	27	88
Block rate	0.00%	0.00%	0.01%	0.00%	0.00%
Input	2,444	2,930	2,318	2,538	3,397
ASNs	42	43	39	48	85

Table 1: Summary of OONI web connectivity measurements for Hong Kong from 1 July 2022 to 30 June 2023

Four websites were found to be confirmed blocked. The full list of these confirmed blocked websites can be found in Annex I.

Category	Category description	OONI Probe Measurements	Number of blocked and likely blocked measurements	Percentage of blocked and likely blocked measurements
ALDR	Alcohol & Drugs	34,265	938	2.7%
ANON	Anonymization and circumvention tools	165,268	10,638	6.4%
COMM	E-commerce	24,740	378	1.5%
COMT	Communication Tools	155,779	3,830	2.5%
CTRL	Control content	16,402	76	0.5%
CULTR	Culture	83,026	2,979	3.6%
DATE	Online Dating	18,896	139	0.7%
ECON	Economics	22,069	1,174	5.3%
ENV	Environment	50,954	1,558	3.1%
FILE	File-sharing	52,785	2,714	5.1%
GAME	Gaming	20,509	598	2.9%
GMB	Gambling	30,612	1,660	5.4%
GOVT	Government	50,343	11,095	22.0%
GRP	Social Networking	230,631	8,054	3.5%
HACK	Hacking Tools	29,779	2,638	8.9%
HATE	Hate Speech	5,748	91	1.6%
HOST	Hosting and Blogging Platforms	150,899	6,779	4.5%
HUMR	Human Rights Issues	222,073	6,301	2.8%
IGO	Intergovernmental Organisations	5,021	41	0.8%
LGBT	LGBT	126,699	4,258	3.4%
MILX	Terrorism and Militants	5,304	38	0.7%
MISC	Miscellaneous content	2,073	5	0.2%
MMED	Media sharing	108,375	3,095	2.9%
NEWS	News Media	223,725	6,517	2.9%
POLR	Political Criticism	119,787	22,479	18.8%
PORN	Pornography	29,317	1,061	3.6%
PROV	Provocative Attire	15,249	2,286	15.0%
PUBH	Public Health	72,488	1,863	2.6%
REL	Religion	129,360	5,842	4.5%
SRCH	Search Engines	52,994	3,592	6.8%

Category	Category description	OONI Probe Measurements	Number of blocked and likely blocked measurements	Percentage of blocked and likely blocked measurements
XED	Sex Education	39,186	1,463	3.7%

Table 2: Summary of OONI web connectivity measurements for Hong Kong from 1 July 2022 to 30 June 2023 by category

*Note: Blocked and likely blocked measurements include Confirmed Blocked, Anomaly, and Failures on OONI measurements.*

## Confirmed Blockings

During the period of study, OONI measurements confirmed only four websites to be blocked. They were found blocked on the following enterprise ISPs:

- AS45102 Alibaba (US) Technology Co., Ltd. (AS45102)
- HKBN Enterprise Solutions HK Limited (AS9381)
- Amazon.com, Inc. (AS16509)
- INTERNET HARBOUR INTERNATIONAL CO.LIMITED (AS64096)

However, only less than 10 measurements were recorded for each of the websites during the study period.

Input	Category	Number of measurements	Percentage of blocked or likely blocked
<a href="http://www.hothk.com/">http://www.hothk.com/</a>	Social Networking	1,555	2.4%
<a href="https://64museum.blogspot.com/">https://64museum.blogspot.com/</a>	Human Rights Issues	1,372	1.0%
<a href="https://getlantern.org/">https://getlantern.org/</a>	Anonymization and circumvention tools	1,493	0.9%
<a href="https://www.viber.com/">https://www.viber.com/</a>	Communication Tools	2,717	1.3%

Table 3: Confirmed website blockings in Hong Kong based on OONI measurements, June 2022-July 2023

On the other hand, while there were [reported blockings](#) in the media, there were no measurements on OONI to corroborate the reports.

## Political Criticism

Out of all blocked or likely blocked categories, Political Criticism has one of the highest rates at 18.8%. However, many of the websites were found to be inactive. While this may be a limitation of the outdated test list, it may also be due to self-censorship in Hong Kong as there is also a lack of new websites in the category.

After filtering out the inactive websites, the following three websites were found to be active, although they may not have been used or maintained by the website owners. These websites were also found to be blocked in the 2022 edition of the iMAP report.

Input	Number of measurements	Percentage of blocked or likely blocked
<a href="https://8964museum.com/">https://8964museum.com/</a>	1,563	43.2%
<a href="https://blockedbyhk.com/">https://blockedbyhk.com/</a>	1,894	36.6%
<a href="https://hkchronicles.com/">https://hkchronicles.com/</a>	1,733	33.1%

Table 4: Potentially blocked websites in the Political Criticism category

## Government

Another category with a high percentage of blocked or likely blocked is Government, with a rate of 22%. There were 14 websites found with a blocking rate of more than 50% in this category. An analysis of the websites found that the potentially blocked websites are related to the US military. This is consistent with [Censored Planet's findings in 2020](#), where they reported that these websites were geoblocked from Hong Kong.

Input	Number of measurements	Percentage of blocked or likely blocked
<a href="http://www.sealswcc.com/">http://www.sealswcc.com/</a>	902	97.8%
<a href="http://www.jsf.mil/">http://www.jsf.mil/</a>	983	96.8%
<a href="http://www.stratcom.mil/">http://www.stratcom.mil/</a>	972	83.1%
<a href="http://www.usafa.af.mil/">http://www.usafa.af.mil/</a>	828	62.1%
<a href="http://www.navy.mil/">http://www.navy.mil/</a>	785	58.7%
<a href="http://www.pacom.mil/">http://www.pacom.mil/</a>	823	60.4%
<a href="http://www.centcom.mil/">http://www.centcom.mil/</a>	851	61.2%
<a href="http://www.uscg.mil/">http://www.uscg.mil/</a>	868	61.4%
<a href="http://www.southcom.mil/">http://www.southcom.mil/</a>	846	60.5%
<a href="https://www.af.mil/">https://www.af.mil/</a>	850	61.4%
<a href="https://www.army.mil/">https://www.army.mil/</a>	788	56.6%
<a href="http://www.socom.mil/">http://www.socom.mil/</a>	1114	54.6%
<a href="https://www.darpa.mil/">https://www.darpa.mil/</a>	773	54.9%
<a href="https://www.dia.mil/">https://www.dia.mil/</a>	604	56.8%

Table 5: 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. However, blocking fingerprints were detected from DNS tampering coming from China's censorship. These are the methods of blockings used by the ISPs based on the confirmed blockings:

ASN	Method of blocking	Example OONI measurement
AS45102 - Alibaba (US) Technology Co., Ltd.	HTTP response includes IP address 10.10.34.x, which is frequently used as internet censorship response. This ASN belongs to China which is subject to the Great Firewall filtration.	<a href="#">Link</a>
AS9381 - HKBN Enterprise Solutions HK Limited	DNS tampering, whereby the DNS answer is redirected to IP belonging to Facebook and DoD Network Information Center. This is consistent with the <a href="#">findings of this paper where they use random IP addresses as DNS answers</a> .	<a href="#">Link</a>
AS64096 - INTERNET HARBOUR INTERNATIONAL CO.LIMITED	DNS tampering, whereby the DNS answer is redirected to an unknown IP "2001::1".	<a href="#">Link</a>
AS16509 Amazon.com, Inc.		<a href="#">Link</a>

Table 6: Methods of blocking websites in Hong Kong

Nevertheless, these are the only confirmed censorships that were able to be detected. After analysing potentially blocked US military websites by a major ISP PCCW-HKT, like [this measurement](#), the DNS query resulted in an NXDOMAIN error.



## Blocking of Instant Messaging Apps

There were no signs of censorship on instant messaging apps as tested on OONI.

	Facebook Messenger	Signal	Telegram	Whatsapp
<b>Total Measurements</b>	25,253	19,075	25,246	25,307
<b>Percentage of blocked and likely blocked</b>	5.0%	1.9%	1.1%	1.5%

Table 7: OONI measurements on instant messaging apps for Hong Kong from 1 July 2022 to 30 June 2023

Note:

1. Failed measurements are discarded this table.
2. As the updates on these apps are beyond OONI's control, the OONI probe may experience testing issues due to app changes that happen from time to time. Hence, failed measurements or anomalies that were identified as false positives were discarded from the table. In particular, these include failed measurements and Signal measurements from 4-30 May 2023.

## Blocking of Circumvention Tools

There does not appear to be blocking of circumvention tools, although there is a high percentage of anomalies for Psiphon and Tor Snowflake which needs to be investigated further.

	Psiphon	Tor	Tor Snowflake	Vanilla Tor
<b>Total Measurements</b>	25,159	24,947	19,613	19,511
<b>Percentage of blocked and likely blocked</b>	13.8%	2.1%	34.3%	0.0%

Table 8: OONI measurements on circumvention tools for Hong Kong from 1 July 2022 to 30 June 2023

Note: Failed measurements are discarded from this table.

## **Acknowledgement of Limitations**

- **Period of study**

This study's findings are limited to network measurements collected from 1 July 2022 to 30 June 2023 in order to examine the most recent censorship trends and events.

- **Vantage points**

Although the network measurements were collected from 85 vantage points in Hong Kong, testing using the OONI software testing was not run consistently across all networks.

- **Use of input/URL as 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, 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 censorship can involve tampering of DNS, HTTP, or other types of censorship. Depending on the method, the blocking can either be at the URL or domain level. However, when analysing results on OONI, the reader needs to note that there are differences in the numbers with respect to the specific input or domain.

In the 2022 report, domain was used as a unit of measurement of a website so as to reduce duplicates when measuring the number of websites blocked. For this 2023 report, however, input is used instead, as it may give more context as to why the web page is blocked. The findings would also be categorised more accurately according to the CitizenLab test lists, which are in URL format. To better understand the findings on the state of censorship, we used percentage of blocked or likely blocked instead of actual counts based on OONI test results.

- **Differences in numbers with OONI data**

The findings in this report have been further processed from OONI's data, whereby more confirmed blockings were obtained and false ones eliminated 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 categorised blocked websites that were not part of the CitizenLab test lists but were tested on OONI via custom test lists. Hence, the figures in this report may differ from the results on the OONI Explorer.

- **Testing of instant messaging apps and circumvention tools**

The instant messaging apps and circumvention tools included in this report are limited to those tested on OONI. Therefore, they may not reflect the state of censorship of apps more commonly used in India.

- **Security concerns in Hong Kong**

Due to security concerns in Hong Kong, the implementation of the iMAP project was limited, especially in terms of the level of measurements and maintenance of the country test list. Additionally, due to self-censorship, fewer websites had been added to the current test list.

## **Conclusion**

Based on the study findings, 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.

On the other hand, self-censorship and security concerns in the country have impacted the project, particularly the level of measurements and the maintenance of the test list.

## **Contribute to the study**

There are various ways one may contribute to the OONI measurements:

- Testing: You may test 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: You can 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's Slack 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.

## Annex I: List of confirmed blockings

Blocked Websites	Categories	ASN	Details
<a href="http://www.hothk.com/">http://www.hothk.com/</a>	Social Networking	45102	<a href="#">Link</a>
<a href="https://64museum.blogspot.com/">https://64museum.blogspot.com/</a>	Human Rights Issues	9381	<a href="#">Link</a>
<a href="https://getlantern.org/">https://getlantern.org/</a>	Anonymization and Circumvention tools	9381	<a href="#">Link</a>
<a href="https://www.viber.com/">https://www.viber.com/</a>	Communication Tools	16509, 64096	<a href="#">Link</a>

## Annex II: List of ISPs

The following list contains the local Hong Kong ISPs probed within the study period:

ASN	ASN Name	ASN Ownership/ Description	ASN Registration Country
AS3363	HKUST-AS-HK	Hong Kong University of Science and Technology	HK
AS3661	ERX-CUHKNET	The Chinese University of Hong Kong	HK
AS4515	ERX-STAR	HKT Limited	HK
AS4528	HKU-AS-HK	The University of Hong Kong	HK
AS4760	HKTIMS-AP	HKT Limited	HK
AS9231	IPEOPLESNET-AS-AP	China Mobile Hong Kong Company Limited	HK
AS9269	HKBN-AS-AP	Hong Kong Broadband Network Ltd.	HK
AS9304	HUTCHISON-AS-AP	HGC Global Communications Limited	HK
AS9381	HKBNES-AS-AP	HKBN Enterprise Solutions HK Limited	HK
AS9908	HKCABLE2-HK-AP	HK Cable TV Ltd	HK
AS10103	HKBN-AS-AP	HK Broadband Network Ltd.	HK
AS10118	HTCL-IAS-HK-AP	Hutchison Telephone Company Limited	HK
AS17924	SMARTONE-MB-AS-AP	SmarTone Mobile Communications Ltd	HK
AS24000	LIHGL-AS-AP	<a href="https://24.hk">24.hk</a> global BGP	HK
AS24002	SCMP-AS-HK-AP	South China Morning Post Publishers Limited. English	HK
AS38819	HKCSL-AS-AP	HKCSL GPRS NETWORK	HK
AS58453	CMI-INT-HK	Level 30, Tower 1	HK
AS64096	BIH-GLOBAL	BIH-Global Internet Harbor	HK
AS133073	SZKF-AS-AP	TELEGLOBAL COMMUNICATION SERVICES LIMITED	HK
AS133752	LEASEWEB-APAC-HKG-10	Leaseweb Asia Pacific pte. ltd.	HK
AS135330	ADCDATACOM-AS-AP	<a href="https://ADCDATA.COM">ADCDATA.COM</a>	HK

ASN	ASN Name	ASN Ownership/ Description	ASN Registration Country
AS135391	AOFEI-HK	AOFEI DATA INTERNATIONAL COMPANY LIMITED	HK
AS136907	HWCLOUDS-AS-AP	HUAWEI CLOUDS	HK
AS137872	PEOPLESPHONE-HK	China Mobile Hong Kong Company Limited	HK
AS137969	HKBIL-AS-AP	HONG KONG BRIDGE INFO-TECH LIMITED	HK
AS138997	EDCL-AS-AP	Eons Data Communications Limited	HK
AS140096	Shanghai Huajuan Information Technology Co., Ltd.		HK
AS132422	Hong Kong Business Telecom Limited		HK
AS4605	Hong Kong Baptist University		HK
AS10099	China Unicom (Hong Kong) Operations Limited		HK
AS55536	Pacswitch Globe Telecom Limited		HK
AS135377	U-CLOUD INFORMATION TECHNOLOGY (HK) LIMITED		HK
AS149651	Better Cloud Limited		HK
AS17764	Hong Kong Metropolitan University		HK
AS4616	The Hong Kong Polytechnic University		HK
AS9229	Speedcast Limited		HK
AS133929	TWOWIN CO., LIMITED		HK
AS38136	Akari Networks Limited		HK
AS18013	ASLINE LIMITED		HK
AS51089	SnapStack Limited		HK
AS9312	xTom Hong Kong Limited		HK
AS141735	Asia Satellite Telecommunications Co. Ltd.		HK
AS133115	HK Kwafong Group Limited		HK
AS17554	Citic Telecom International (Data) Limited		HK
AS146952	INSTART		HK
AS147293	NEARROUTE LIMITED		HK

ASN	ASN Name	ASN Ownership/ Description	ASN Registration Country
AS64022	Kamatera, Inc.		HK
AS64021	Hong Kong Business Telecom Limited		HK
AS10222	Multibyte Info Technology Limited		HK
AS136038	HDTIDC LIMITED		HK
AS134196	Cloudie Limited		HK
AS141167	AgotoZ HK Limited		HK

The following list is the foreign Hong Kong ISPs probed within the study period:

ASN	ASN Name	ASN Ownership/ Description	ASN Registration Country
AS6939	HURRICANE		US
AS8075	MICROSOFT-CORP-M SN-AS-BLOCK		US
AS9009	M247		GB
AS13335	CLOUDFLARENET	Cloudflare	US
AS16509	AMAZON-02	Amazon	US
AS21859	ZEN-ECN		US
AS45102	ALIBABA-CN-NET	Alibaba US Technology Co., Ltd.	CN
AS54574	DMIT-LEGACY		US
AS60068	CDN77	Datacamp Limited	GB
AS199524	GCORE		LU
AS49901	KUIPER NETWORK LTD		UK
AS40065	CNSERVERS LLC		US



ASN	ASN Name	ASN Ownership/ Description	ASN Registration Country
AS147049	PacketHub S.A.		AU
AS137409	GSL Networks Pty LTD		AU
AS133398	Tele Asia Limited		AU
AS4842	Tianhai InfoTech		CN
AS7586	Cloudfort IT		CN
AS9808	China Mobile		CN
AS23764	China Telecom Global Limited		CN
AS213320	EXFLUX NETWORKS UK LTD		DK
AS138678	Grandbo Technology Development Corporation		PH
AS10122	BIGO TECHNOLOGY PTE. LTD.		SG
AS212238	Datacamp Limited		UK
AS48024	NEROCLOUD LTD		UK
AS396982	Google LLC		US
AS906	DMIT Cloud Services		US
AS53850	GorillaServers, Inc.		US
AS3491	PCCW Global, Inc.		US
AS41378	Kirino LLC		US
AS54203	Strong Technology, LLC.		US
AS399606	Imaging Bay, Inc.		US

---

ASN	ASN Name	ASN Ownership/ Description	ASN Registration Country
AS19527	Google LLC		US
AS328608	Africa on Cloud		ZA

## Annex III: Glossary

DNS	<p>DNS stands for “Domain Name System” and it maps domain names to IP addresses.</p> <p>A domain is a name that is commonly attributed to websites when they’re created. It allows websites to be more easily accessed and remembered. For example, twitter.com is the domain of the Twitter website.</p> <p>However, computers can’t connect to internet services through domain names. They do so through 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.</p> <p>The Domain Name System (DNS) 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.</p>
HTTP	<p>The Hypertext Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web to transfer or exchange data across the internet.</p> <p>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.</p> <p>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).</p> <p>The transmission of data over the HTTP protocol is unencrypted.</p>
Heuristics	<p>Heuristics obtain further confirmed blockings other than those which are detected based on OONI blocking fingerprints. More detailed explanation is found <a href="#">here</a>.</p>
ISP	<p>An Internet Service Provider (ISP) is an organisation that provides services for accessing and using the internet.</p> <p>ISPs can be state-owned, commercial, community-owned, non-profit, or otherwise privately owned.</p> <p>Vodafone, AT&amp;T, Airtel, and MTN are examples of ISPs.</p>
Middle boxes	<p>A middlebox is a computer networking device that transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding.</p>

	<p>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.</p> <p>Middleboxes are sometimes also used to implement internet censorship and/or surveillance.</p> <p>The OONI Probe app includes two tests designed to measure networks with the aim of identifying the presence of middleboxes.</p>
TCP	<p>The Transmission Control Protocol (TCP) is one of the main protocols on the internet.</p> <p>To connect to a website, your computer needs to establish a TCP connection to the address of that website.</p> <p>TCP works on top of the Internet Protocol (IP), which defines how to address computers on the internet.</p> <p>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.</p> <p>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.</p>
TLS	<p>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.</p> <p>When you connect to a website through TLS, the address of the website will begin with HTTPS (such as <a href="https://www.facebook.com/">https://www.facebook.com/</a>), instead of HTTP.</p>

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 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 GeolIP 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.

## 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, 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 content calling for changes in leadership, governance issues, legal reform. Etc.

No.	Category Description	Code	Description
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.
19	Hacking Tools	HACK	Sites dedicated to computer security, including news and tools. This includes malicious and non-malicious content.

No.	Category Description	Code	Description
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 [git repository](#), and details about what collected network measurements entail can be viewed through [OOONI Explorer](#) or through [OOONI'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 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 confirms an instance of blocking when a block page is detected.

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.








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. 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:

Does the IP in question point to a government blockpage?			
Yes	No, page timed out or shows Content Delivery Network (CDN) page.		
			
Confirmed blocking	What information can we get about the IP by doing a whois lookup?		
	Government or Local ISP*	CDN / Private IP	
			
	Confirmed blocking	Do we get a valid TLS certificate for one of the domains in question when doing a TLS handshake and specifying the SNI?	
	Yes	No, there were blocking fingerprints found.	No, timed out.
			
<b>False positive</b>	<b>Confirmed blocking</b>	Sampled measurement is analysed on OONI Explorer.	

\*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.