

Internet Monitoring Action Project

iMAP Cambodia 2023

Internet Censorship

Report

By Lam Socheat (API), Tan Thary (API), Nop Vy (CamboJA), Chhan Sokunthea (CCIM), Siti Nurliza Samsudin (Sinar Project), and Kelly Koh (Sinar Project)

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

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

How to Use This Report

Recommendations to audience:

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

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

About Advocacy Policy Institute

The Advocacy and Policy Institute (API) is a Cambodian non-governmental organisation active in advocacy, policy influencing, good governance, and civic engagement. Capacity building and dialogue facilitation are at the heart of our efforts towards democratic and sustainable development. More information is available at <https://apiinstitute.org/>.

About CamboJA Journalist Alliance Association

CamboJA is Cambodia's only independent network of professional journalists. It was founded by a number of journalists, including former reporters from the Cambodia Daily and Phnom Penh Post, both of which were subjected to government repression in the run-up to the 2018 general elections.

Due to growing restrictions on media freedom and freedom of expression, 20 professional journalists from different media outlets held a meeting on the media situation in Cambodia in February 2019, during which CamboJA was initiated. Eventually, 15 of them agreed to form the governing body of CamboJA and became board members, aiming to establish a sustainable independent body that can carry out the mission to promote access to information and press freedom, strengthen the professionalism of journalists, and support their livelihoods.

About Cambodia Center for Independent Media

The Cambodian Center for Independent Media (CCIM) was established in the first quarter of 2007 and duly registered with the Ministry of Interior on 15 June 2007 as a non-governmental organisation (NGO). CCIM was organised to work towards the promotion of independent media, press freedom, freedom of expression, access to information, and internet freedom. The mission of CCIM envisions a Cambodian society where every citizen is provided with comprehensive and up-to-date information and empowered to promote democracy, governance, and respect for human rights. CCIM strengthened the capacity building for aspiring journalists, citizen journalists, and youth related to basic journalism and digital rights, including the provision of legal support for professional and unprofessional journalists.

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>.

Abbreviations

The content of the report was stated with abbreviated words and their full names are stated in this table.

ALDR	Alcohol & Drugs
ANON	Anonymization and circumvention tools
ASN	Autonomous System Number
COMT	Communication Tools
CTRL	Control content
CULTR	Culture
DRWG	Digital Rights Working Group
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 Contents

About iMAP	1
How to Use This Report	1
About Advocacy Policy Institute	2
About CamboJA Journalist Alliance Association	2
About Cambodia Center for Independent Media	2
About Sinar Project	2
Abbreviations	3
Table of Contents	5
Key Findings	7
Introduction	8
Background	8
Social, Political, and Economic Landscape	9
Legal Environment	9
Legal Updates	9
Freedom of Expression	10
Freedom from Interference	13
Freedom from Censorship	13
Free Access to Information	14
Inter-Ministerial Prakas (Proclamation) No. 17017	14
National Internet Gateway ¹⁸	15
Draft Law on Cybersecurity	16
Domain Name Registration Sub-Decree	16
Reported Cases of Internet Censorship	16
Network Landscape	17
Mobile Phone Subscriptions	18
Fixed Phone Subscriptions	18
Licences	19
Mobile Companies	20
Internet Service Providers	20
Certificates	21
Instant Messaging	21
Findings on Internet Censorship in Cambodia	22
Blocking of websites	22
Confirmed blocked websites by category	25
Blocking of news websites	26
Blocking of instant messaging apps	27
Blocking of circumvention tools	27
Acknowledgement of Limitations	28
Conclusion and recommendations	30
Registration of Domain Name System (.kh)	31
Contribute to the study	31
Acknowledgements	32

Annex I: List of confirmed blockings	33
Annex II: List of Internet Service Providers (ISPs)	38
Annex III: Glossary	39
Annex IV: Methodology	41
Data	41
Coverage	41
How are the network measurements gathered?	41
How are the network measurements analysed?	41
Country code	42
Autonomous System Number (ASN)	42
Date and time of measurements	42
Categories	42
IP addresses and other information	44
Network measurements	45
Verifying OONI measurements	46

Online news sites and other websites are periodically blocked in Cambodia, particularly those that disseminate information that could be perceived as a threat to the ruling government.¹

Key Findings

- From July 2022 to June 2023, there were 2,201 websites measured by the OONI Probe tool. The results showed that in Cambodia, 37 (22 global websites and 15 Khmer websites) out of 2201 websites were blocked or censored using Domain Name System Blocking from the Internet Service Providers (Viettel, Ezecom, Wicam, CamSIM, Private Company (iSEEK)). The blocking method used was DNS attempting, whereby the website would be redirected to a timed-out IP address belonging to an ISP or the bogon IP address of 127.0.0.1. Several popular news outlets were also found to be censored: Voice of Democracy (VOD), Radio Free Asian (RFA), and Cambodia Daily.
- WhatsApp, Facebook Messenger, Signal, Telegram, and the Tor network were accessible across all tested networks throughout the testing period, and no censorship was detected for those applications.²
- Based on the analysis and findings of the report, we reiterate the recommendations made by the OHCHR. It is recommended that the State (Cambodia) review and revise its current and pending legislation, including the Sub-Decree on National Internet Gateway and the amendments to the Press Law, the leaked draft cyber security law, and the draft laws on cybercrimes. We also recommend that the draft access to information law be passed in order to avoid the use of vague terminology and overly broad restrictions. The UN Human Rights Committee further recommends the state ensures that in the formulation and enforcement of its legislation, including Ministerial Sub-Decrees, any restrictions on the exercise of freedom of expression and association comply with the strict requirements of articles 19 (3) and 22 of the covenants on civil and political rights and convention on human rights.
- The government should review and consider uplifting the websites detected as blocked by the OONI Probe that exercise the rights and freedom of expression and internet freedoms.

¹ Freedom House. (2021). *Cambodia*. <https://freedomhouse.org/country/cambodia/freedom-net/2021>

² Even though no censorship is found here, Facebook's Response 2020 on Cambodia Human Rights Impact Assessment points "Facebook was a vital platform for human rights defenders, but defenders used it with a significant degree of self-censorship".

Introduction

Online news sites and other websites are periodically blocked in Cambodia, particularly those that disseminate information that could be perceived as a threat to the ruling government. However, all of these platforms should be accessible from all networks 24 hours a day in order to promote Digital Rights and Freedom of Expression through online platforms, especially for social media and all websites.

To examine the current state of internet censorship in Cambodia, the Open Observatory of Network Interference (OONI), Sinar Project, and the Advocacy and Policy Institute with the participation of Digital Right Working Group (DRWG) collaborated on a joint study to examine whether internet censorship events were persisting in the country through data collection and analysis of network measurements. The aim of this study, which ran from 1 July 2022 to 30 June 2023, is to uncover trends of internet censorship.

The Open Observatory of Network Interference (OONI) is a global community that has measured Internet censorship since 2012. OONI tests the blocking of websites and apps and measures the speed and performance of the network. Find out more about OONI at <https://ooni.org/>.

The limitation of this report is that it is based only on data generated from OONI, which is obtained from people in Cambodia and across the globe voluntarily running OONI Probe. The intention is to monitor the websites of individual organisations, their partners, and any members that may be blocked at any time, particularly during the national elections and other circumstances.

Background

Population in January 2023	16.86 million ³
Internet penetration in September 2022 (% of population using the internet)	18 million (106.06%) ⁴
Mobile subscriptions in Sept 2022 (per 100 inhabitants)	19.60 Million (115%) ⁵

³ *Digital 2023: Cambodia — DataReportal – Global Digital Insights*. (2023, February 13). DataReportal – Global Digital Insights. <https://datareportal.com/reports/digital-2023-cambodia>

⁴ *Internet Subscriptions | Telecommunication Regulator of Cambodia*. (n.d.). Internet Subscriptions | Telecommunication Regulator of Cambodia. <https://trc.gov.kh/en/internet-subscriptions/>

⁵ *Mobile Phone Subscriptions | Telecommunication Regulator of Cambodia*. (n.d.). Mobile Phone Subscriptions | Telecommunication Regulator of Cambodia. <https://trc.gov.kh/en/mobile-phone-subscriptions/>

Freedom on the Net ranking in 2022	43/100; Partly free ⁶
Religion (%)	Buddhism: 97.9%, Islam: 1.1%, Christianity: 0.5%, Others: 0.6% ⁷
ICCPR Ratification	Yes

Table 1: The data in the table were obtained from different resources and thus cover different periods of references.

Social, Political, and Economic Landscape

During the period of study, the Candlelight Party, a liberal political and opposite party in Cambodia was disqualified to run in the 2023 elections. The election commission has demanded the Candlelight Party submit its original registration document from the Ministry of Interior in order to register for the election. That document was lost when the police raided the CNRP headquarters in 2017, and the party [took part in subsequent polls](#) by submitting a photocopy of the letter, according to Aljazeera news.⁸

Furthermore, in the 7th Cambodian election, 18 parties did not have an opposite party. The election campaign took place from 1 July 2023 to 21 July 2023, while the election day was on 23 July 2023.

Legal Environment

Legal Updates

The draft Cybercrime Law became known when the Post and Telecommunications Department under the Ministry of Transport and Communications revealed the final draft. The Civil Society Organization had insistently requested the Ministry to publicly release version one of the final draft in order to give them enough time to input in the law. However, the Civil Society Organization did not receive any response from the Ministry, and the Draft Cybersecurity law was already input into some suggestions and sent to the Post and Telecommunication Department under the Ministry of Transport and Communications.

Conversely, the Data Privacy Law was officially released to some Civil Society Organisations that had worked on the Digital Right and Freedom of Expression material. They will prioritise taking action to input this law.

⁶ *Cambodia: Freedom on the Net 2022 Country Report* | Freedom House. (n.d.). Freedom House. <https://freedomhouse.org/country/cambodia/freedom-net/2022>

⁷ *Population of Cambodia 2023 | Religion in Cambodia* | Find Easy. (2021, June 6). Find Easy. <https://www.findeasy.in/population-of-cambodia/>

⁸ *Cambodia's main opposition party barred from July election*. (2023, May 17). Cambodia's Main Opposition Party Barred From July Election | Elections News | Al Jazeera. <https://www.aljazeera.com/news/2023/5/17/cambodias-main-opposition-party-barred-from-july-election>

The Domain Name law required companies to register a national domain (.kh) to their website and email before January 2023. Although the deadline is not strictly enforced⁹, the law hadn't been run past the Civil Society Organizations.

Using national safety and security protection as a justification, the Cambodian government has drafted, enacted, and enforced several laws and legal regulations. However, these have been criticised as tools used by the government to increase their control over internet usage, affecting citizens' basic rights to freedom of expression.¹⁰

Freedom of Expression

Constitution

Article 41 of the Constitution guarantees freedom of expression. However, Article 41 stipulates that, in exercising freedom of expression, “no one shall exercise these rights to infringe upon the honour of others, or to affect the good customs of society, public order and national security”. As evidenced in later national legislation and non-legal measures, the state has actively promulgated measures to roll back guarantees of internet freedom based on such concerns regarding honour, public order, and national security. Article 41 also provides for regulation of the media by stating that the “regime of the media shall be determined by law”.

The latest amendment to the Constitution in 2018 further diminished compliance with international standards. An amendment to Article 49 — concerning respect for the constitution and laws and defending the nation — was the most damaging to fundamental freedoms. The amendment now obligates “Every Khmer citizen to uphold national interest” and to refrain from “conducting any activities which either directly or indirectly affect the interests of the Kingdom of Cambodia and of Khmer citizens.” When justifying the necessity of the amendment, Minister of Interior Sar Kheng singled out activists, HRDs, and opposition members for their appeals to the international community to impose sanctions on Cambodia over its crackdown on opposition and civil society (Nachemson & Dara, 2018). In this context, it is evident that Article 49 as amended can be easily used to curtail freedom of expression online, especially when the statement criticises the state or emphasises a call to action against the State. Any dissent against the government can prompt disproportionate legal actions penalising the exercise of freedom of expression.⁹

Penal Code

The 2009 Penal Code contains vaguely worded provisions on “plotting”, sharing “false information” and “incitement to commit a felony,” which have been used to charge internet

⁹ Ogden, J. (2023, January 29). *Register .kh Domain Names in Cambodia - Cambodia Begins at 40*. Cambodia Begins at 40. <https://www.cambodiabeginsat40.com/?p=41005>

¹⁰ *Cambodia: Internet Censorship, Control Expanded*. (2021, February 19). Cambodia: Internet Censorship, Control Expanded | Human Rights Watch. <https://www.hrw.org/news/2021/02/18/cambodia-internet-censorship-control-expanded>

users for posting and sharing critical content on social media. Criminal defamation is provided for under Article 305 of the 2009 Penal Code. Furthermore, spreading disinformation and conspiracy are criminalised under Article 425 and 453, while laws related to incitement and provocation to commit crimes are stipulated under Articles 494 and 495. The latest amendment in 2018 introduced Article 437 bis, or the *lèse-majesté* provision, to the Code.

Article 305 on public defamation stipulates that “any allegation or slanderous charge that undermines the honour or the reputation of a person or an institution” is a criminal offence. The crime can be committed through several means. These categories of assessment apply to all provisions mentioned in this section and cover the common activities of most users online, such as the writing and sharing of posts on online platforms or social media. If these online actions are deemed defamatory, the act is punishable by fines between 24.60 USD to 2,460 USD. Article 305, in tandem with other provisions in the Penal Code, has been disproportionately used to silence criticism by opposition politicians and critics.

Article 425 (false information) criminalises the “communication or disclosure of any false information with a view to inducing a belief that destruction, defacement or damage dangerous to other persons will be carried out”. This has been utilised by local authorities as criminalising the dissemination of information they perceive as fake news, including critical comments directed at the government that they believe may potentially cause political instability or damage to their reputation. The use of this Article to penalise an individual can result in imprisonment from one to two years, or a fine ranging from 490 USD to 981 USD. Similarly, Article 453 on conspiracy and plotting against the government criminalises “any scheme set up between several persons to commit a criminal attempt, and this scheme was materialised by one or several concrete actions, constitutes a conspiracy”. Individuals charged can face a minimum of five and up to ten years of imprisonment. The article has been misused to criminalise dissent against the state, even in instances where there is no evidence of plotting.

The provisions most frequently used to persecute members of the opposition, government critics, activists, and media professionals are Articles 494 and 495 (incitement to commit a felony). Under Article 495, incitement to “commit a felony or to disturb social security” by means identified in Article 494, the same as those under Article 305, is “punishable by imprisonment from six months to two years and a fine from one million to four million Riels, where the incitement was ineffective”.

Article 437 bis (*lèse-majesté*) prohibits criticism of the King and outlines penalties of between one to five years imprisonment and monetary fines ranging from 500 USD to 2,460 USD. Following Thailand's lead in prosecuting political critics for *lèse-majesté*, this provision encroaches on social media users' online freedoms (Boyle and Chhengpor, 2018). Internet users can be charged with this crime through any “word, gesture, writing, picture or other media which affects the dignity of the individual”.¹⁰

2019 Draft Law on Access to Information

The updated draft law, which contains protections for whistleblowers and has the potential to positively impact free expression online if approved and enforced, was released to the public in August 2019. It raised concerns about the law's adherence to international human rights standards, as well as its use of broad and unclear standards that could threaten access to information and freedom of expression. For example, the law narrowly defines the type of information and institutions it applies to; lacks effective oversight procedures; permits public authorities to deny disclosure in various overly broad situations; and contains a criminal libel and defamation provision. In August 2020, the law was finalised and was set to be approved by the Council of Ministers¹¹; however, due to delays because of the pandemic, the law had not yet been sent to parliament until the end of 2021.¹¹

Law on Telecommunications

The 2015 Law on Telecommunication imposes generic obligations on telecommunication service providers, which authorities claim will enhance service access in the countryside and rural areas. Within the broad range of regulations, however, the law also functions as a legal tool to monitor internet activity. Freedom of expression is threatened through the imposition of monitoring actors (Articles 70 and 71), decreased data protection (Articles 97 and 6) and the criminalization of free speech on radio, television, online, and in private messages (Article 80).

Article 6 requires “all telecommunications operators and persons involved with the telecommunications sector” to provide MPTC with “the telecommunications, information and communication technology service data”. The lack of definition as to who this legitimate authority is remains highly problematic and could potentially lead to arbitrary surveillance. Hence the law — by allowing surveillance of electronic devices — enables Cambodian authorities to actively phone-tap and monitor online discourses to selectively persecute targeted individuals.

Article 80 states that the “establishment, installation, and utilisation of equipment in [the] telecommunication sector, if these acts lead to national insecurity, shall be punished by sentences from 7 to 15 years imprisonment.” The lack of clarity over types of telecommunication activity could heavily punish legitimate expression disseminated via radio shows, television, and online, and even through private messages and phone conversations between individuals, should the authorities determine it to be a threat.¹³

Cybercrime Law (Draft) 2020

Proposed in 2012, the law is subject to further changes in response to critical backlash, and as of August 2021, there was no specific date for the completion of the drafting nor for the implementation of the Law. Articles 8 and 12 state that service providers must “preserve

¹¹ IFJ. (2022, July 1). *Cambodia: Government needs to pass Access to Information Law*. <https://www.ifj.org/media-centre/news/detail/category/press-releases/article/cambodia-government-needs-to-pass-access-to-information-law.html>

traffic data for at least 180 days (about 6 months)", to be shared with "competent authorities" upon their request.

Articles 32 and 33 criminalise the "unauthorised access" to a computer system or the transferring of data from one system to another without permission. Those charged face imprisonment of up to 10 years. These Articles also pose concerns to whistleblowers and HRDs who access such information to expose rights violations by the state, as they are not provided adequate safeguards.

Article 40 criminalises the use of computers to initiate "interruptions, fear, threats, abuses, [and] intimidation". Individuals charged under this Article face a maximum of six months imprisonment. Article 45 criminalises "any person who knowingly and intentionally makes a false statement or material misrepresentation through information technology" that could be detrimental to "public safety" and "national security".

Freedom from Interference

Press freedom and internet freedom in Cambodia are increasingly under threat. In the 2022 [Freedom in the World](#) Report by Freedom House, Cambodia was classified as "Not Free". People are afraid to express their views or opinions online, especially those which are critical of the government. The Cambodian government has used the existing laws and legal regulations and developed new ones to increase interference. It was noted that the Criminal Code has been used in cases involving journalists and the COVID-19 Law has been used in cases involving journalists and human rights defenders.

In 2022, journalists in Cambodia were increasingly being subjected to various forms of harassment and pressure, as well as violence, amid growing restrictions on civic space and press freedoms in the country. As part of the report, 65 journalists were interviewed and surveyed. All respondents to the survey stated they had faced some form of interference in the course of their work, while more than 80% of those surveyed said they had experienced surveillance and disproportionate or unnecessary restrictions, including in relation to access to information¹⁴.

Freedom from Censorship

During recent years, censorship in its different forms has dramatically increased in Cambodia . The forceful imposition of legal and non-legal measures by the Cambodian government against targeted groups or individuals has negatively restricted the freedom of expression and internet freedoms.

[OHCHR](#) argued that while neither Prakas 170 nor the Sub-Decree on the National Internet Gateway are specifically targeted at the media, the potential impact of these instruments on freedom of expression more broadly and press freedom is profound. Both instruments vest broad powers in government to censor expression in a manner that appears to go well beyond what is permitted by Article 19(3) of ICCPR, giving rise to situations where government agencies will be empowered to censor expression and reporting that they deem inconvenient. During the previous national election in 2018, the Ministry of Information ordered ISPs to block the services of 15 independent media outlets or news websites.

Therefore, it is argued that Prakas 170 and the Sub-Decree on the National Internet Gateway threaten to provide a more formal legislative basis for the closure of websites. This includes websites of news outlets, giving rise to fears of routing and shutting down of critical voices and reporting.

In general, the Cambodian people are afraid to speak up against the ruling regime. According to a recent study done by the [Asiacenter](#), individuals have taken a step back from sharing their own political opinions online or participating in political events; instead, they prefer to simply read or listen to such content as they are afraid of getting into trouble with the Cambodian authorities, who have ramped up their control of the online sphere.

Recently, in 2022, a report from [OHCHR](#) that interviewed 15 men and six women journalists showed that 60% of them had faced verbal threats in connection with their work. Another study noted that Facebook was the most surveilled online platform, with 46 cases of restrictions on freedom of expression reported, followed by TikTok (8) and YouTube (7).¹⁵

Free Access to Information

In line with international human rights standards and principles concerning access to information, several laws and legal regulations of Cambodia have guaranteed access to information (A2I). Three provisions in the current Cambodian Constitution provide the constitutional underpinnings of a protected right of “timely and effective access to high quality and accurate information held by the Cambodian government and other public institutions”. Article 5 of the Press Law recognizes the “right of access to information in government-held records. Article 13 of the 2005 Archive Law states: Public archives, which are published documents, are permitted to be used by the public for research and consultations as unrestricted information. Other public activities shall be permitted for free research 20 years thereafter the date of the documents or thereafter the end of the proceeding, or in special cases as stipulated in Article 14 of this Law.¹⁶ The Information Law remains in the draft version till late 2021 since its initiative version was drafted in 2007.

However, free access to information remains a great challenge. A recent [study](#) by [OHCHR](#) on journalists suggested that journalists are working in an increasingly difficult environment, one that is particularly fraught with difficulties when it comes to accessing information from public sources. While the authorities have adopted laws that seem to curtail the right to freedom of expression, they have delayed finalising a promised new law that will permit journalists and media personnel to access official information.

Inter-Ministerial Prakas (Proclamation) No. 17017

This Prakas was implemented amidst an environment of stricter controls on online platforms during the elections, such as blocking of pro-democracy websites. The Prakas’ initial proclamation enables close collaboration between the Ministry of Information, Ministry of Interior, and MPTC to monitor social media usage. The regulation directly targets website publications and social media networks within the Cambodian Internet space. Under Clause 6, the Ministry of Information is authorised to manage published online information through electronic systems and “take action” against illegal publications.

While the Inter-Ministerial Prakas was often called Cambodia's "fake news" law, it has rarely been used to criminalise the act of disseminating disinformation. Rather, it has been used as a justification for governmental digital surveillance.

National Internet Gateway¹⁸

This Sub-Decree significantly enhances monitoring capacities over user activity, as gateway operators will report their observations on internet usage to the Ministry of Telecommunications. Similar to the Inter-Ministerial Prakas, this law is geared towards online state surveillance rather than criminalising online activities. Therefore, this new policy is a highly potent tool against online expression and the right to privacy.

Article 6 of the document describes the functions and duties of the NIG operator. These include the management of access to connections and internet services. Due to vague and overly broad provisions, the Article allows for the government to block access to sites that propagate critical views against the state, by branding it as information that threatens social order or safety.

Article 12 (revenue collection, safety, and public order protection) also requires NIG operators to "[assure] safety, public order, dignity, culture, tradition and custom of the society, as well as preventing and cracking down on crimes". Vague definitions and unclear assessments of what constitutes a crime, or what actions threaten "social order, dignity, culture, traditions, and customs" potentially allows for continued politically motivated prosecution of online activists and internet users. Service providers must also urge users to complete online forms and verify their identities: the collection of such data, with no existing safeguards on data privacy, may result in its use to surveil and monitor internet activity. As such monitoring is already commonplace in Cambodia, the NIG only serves to worsen the situation of internet freedoms and self-censorship.

Under Article 14, gateway operators are required to store data and provide routine status reports to the authorities. Through the storage of technical records, IP addresses, and identification of the route of traffic through the NIG for 12 months, operators can monitor user activities.

The Sub-Decree on Management and Use of National Domain Names on the Internet has restricted freedom of expression and freedom of information, with any domain names that the government considered unregistrable and can not re-registered after deletion. In Article 8, it states that registration of national domain names shall adhere to the principle of first come first served. National domain names that are unregistrable include domain names that harm morality, tradition, and religion, and contravene the laws and applicable regulations. Under Article 11, registrants shall have obligations as follows: shall not use national domain name to promote activities or trades or other information, and communicate on the internet that affect culture, morality, traditions, customs, individual rights, consumer rights, public legal interests, national security, or social order.

Draft Law on Cybersecurity

The Ministry of Posts and Telecommunications is currently developing a Law on Cybersecurity to establish a regulatory body for the governance of digital security and to extend police powers. An early draft of the law fails to ensure the independence of the regulatory body and includes insufficient avenues of appeal. Further, it grants wide-ranging search and seizure powers during loosely defined cybersecurity incidents, and it also permits the prosecution of those who fail to comply. The law imposes strict liability offences subject to criminal penalties, including for failing to comply with technical conditions for maintaining cybersecurity, failing to report a cybersecurity incident, and providing cybersecurity services without a licence. The draft includes a classic catch-all provision — quickly becoming a trade mark of Cambodian laws — which would permit the Ministry of Posts and Telecommunications to perform any “necessary duties related to cybersecurity”. Such opaque language undermines the fundamental requirement of legality and adds to the government’s armoury of broad laws, which it can weaponise against critics at its will.

Domain Name Registration Sub-Decree

On 31 December 2021, the government of Cambodia issued a new sub-decree governing domain names, the Sub-Decree on the Management and Use of National Domain Names on the Internet Domain Name Sub-Decree. It mandates the use of national domain names (.kh) by all entities registered to operate in Cambodia. In February 2023, the Ministry of Posts and Telecommunications launched a website through which official domain names could be purchased. While States have a wide discretion to manage their national domain names, requiring the use of national domain names could limit freedom of expression in violation of international human rights standards. There is also a concern that the Domain Name Sub-Decree could be used in conjunction with other restrictive laws on online expression and digital governance to censor online content and enhance surveillance.

Reported Cases of Internet Censorship

The government has ordered internet service providers to block the websites and social media pages of several independent media outlets and a public database¹².

On 9 February 2023, the online news outlet VOD issued an article that Prime Minister Hun Sen’s son, Hun Manet, had signed an agreement providing financial assistance to Turkey, as claimed by the government spokesperson Phay Siphon. Hun Sen then announced on his Facebook page that VOD has to apologise to his son within 72 hours or else the Ministry of Information will revoke its licence. On 12 February 2023, VOD sent a letter to Prime Minister Hun Sen, expressing regret and requesting forgiveness for unintentional wrongdoing. However, the Prime Minister rejected the apology in the early hours of 13 February 2023, and the Khmer and English websites of VOD were blocked by ISPs.¹³ On 13 February 2023,

¹²

<https://cambojanews.com/government-orders-internet-providers-to-block-media-outlets-kamnotra-data-base/>

¹³ <https://www.licadho-cambodia.org/articles/20230213/180/index.html>

the Ministry of Information revoked the VOD'S licence, which was overseen by the Cambodian Centre for Independent Media (CCIM).¹⁴

According to the Bangkok Post, "The Oversight Board, whose decisions are binding, on Thursday recommended Hun Sen's Facebook and Instagram accounts be suspended for six months due to the video filmed in January, in which he told opponents they would face legal action or a beating with sticks if they accused his party of vote theft in July's national polls." and "The Cambodian premier now uses the Telegram app to relay his political messages to supporters, and TikTok to engage with youth."¹⁵

In addition, the Information Ministry revoked the licences of three media outlets following reports on the involvement of a senior official in land fraud. These outlets were the [Federation of Cambodia-ASEAN Journalists](#), [Raksmei Kampong Cham](#), and [Dumnong Knong](#).¹⁶

Network Landscape

Through its strong relationships with and influence over the ISPs, the government has expanded its control over the internet. As implied, internet freedom in Cambodia is increasingly under threat. The five major telecommunication firms that provide both land-based and mobile internet services in Cambodia — Viettel, Smart Axiata, CamGSM, Xinwei Telecom, and Southeast Asia Telecom — are closely affiliated with the Royal Government of Cambodia (RGC) and its officials, and they are likely to provide cover for each other.

Three prominent communication tools in Cambodia are mobile phone, fixed phone, and internet. According to the newly functioning Telecommunication Regulators of Cambodia (TRC), [the numbers of subscribers for these services](#) are as follows:

¹⁴ Sochan, R. (2023, February 13). VOD's media licence revoked. VOD's Media Licence Revoked | Phnom Penh Post. <https://phnompenhpost.com/national/vods-media-licence-revoked>

¹⁵ Public Company Limited, B. P. (n.d.). *Cambodia's Hun Sen threatens to block Facebook access*.

<https://www.bangkokpost.com>.

<https://www.bangkokpost.com/world/2602683/cambodias-hun-sen-threatens-to-block-facebook-access>

¹⁶ *Information Ministry Revokes Three Media Licenses Following Reports on Senior Official's Role in Land Fraud* | *CamboJA News*. (2023, March 18). Information Ministry Revokes Three Media Licenses Following Reports on Senior Official's Role in Land Fraud | *CamboJA News*. <https://cambojanews.com/information-ministry-revokes-three-media-licenses-following-reports-on-senior-officials-role-in-land-fraud/>

Mobile Phone Subscriptions

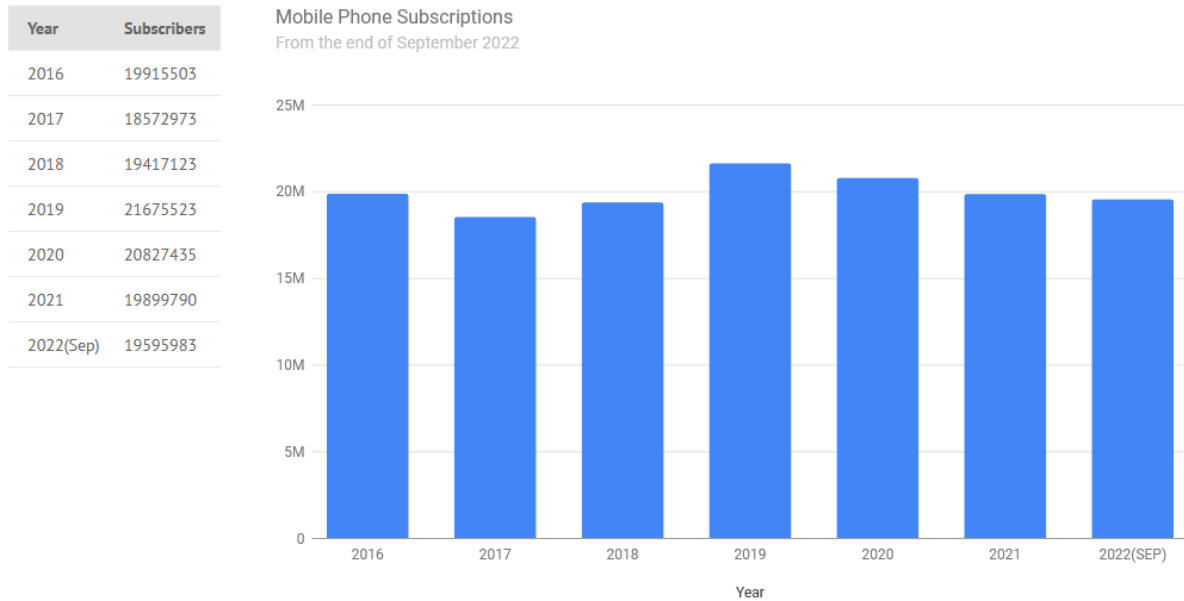


Chart 1: The chart shows the number of mobile phone subscribers by year. During the COVID-19 pandemic in 2020, the number of users sharply increased to 20,827,435 subscriptions. When the COVID-19 situation got better, the users slightly decreased in 2021 (19,899,790 subscription) and in September 2022 (19,595,983 subscription).

Source: [Telecommunication Regulators of Cambodia](#)

Fixed Phone Subscriptions

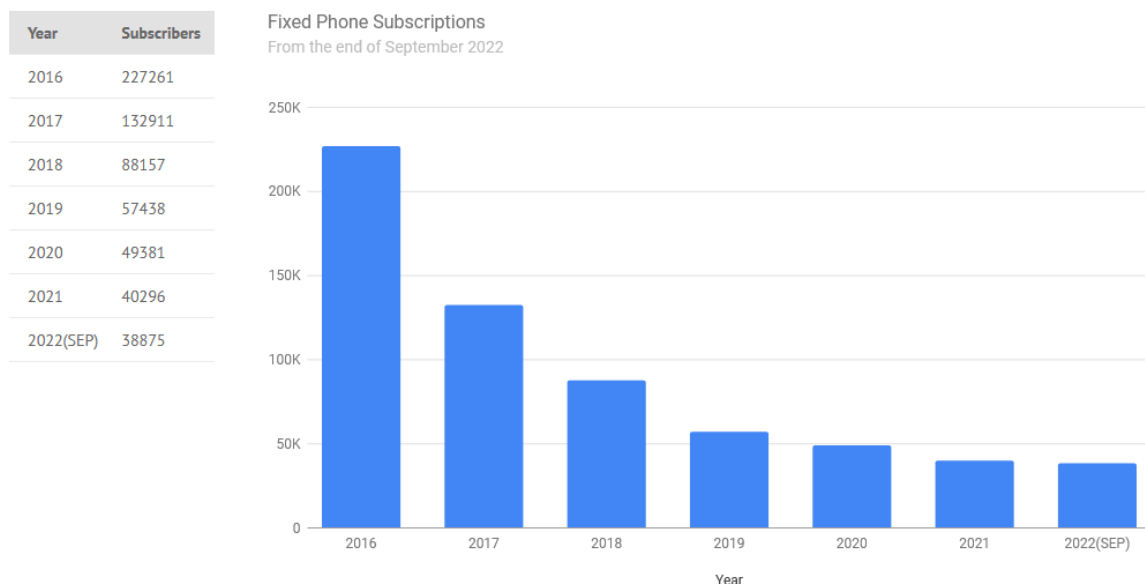


Chart 2: The fixed phone subscriptions in Cambodia dropped every year from 2016 (227261 subscriptions) to September 2022 (38875 subscriptions). The number of subscriptions in 2017 (132911 subscriptions) dropped to nearly half of 2016 (227261 subscriptions). The lowest decline was between 2021 (40296) and 2022 (38875).

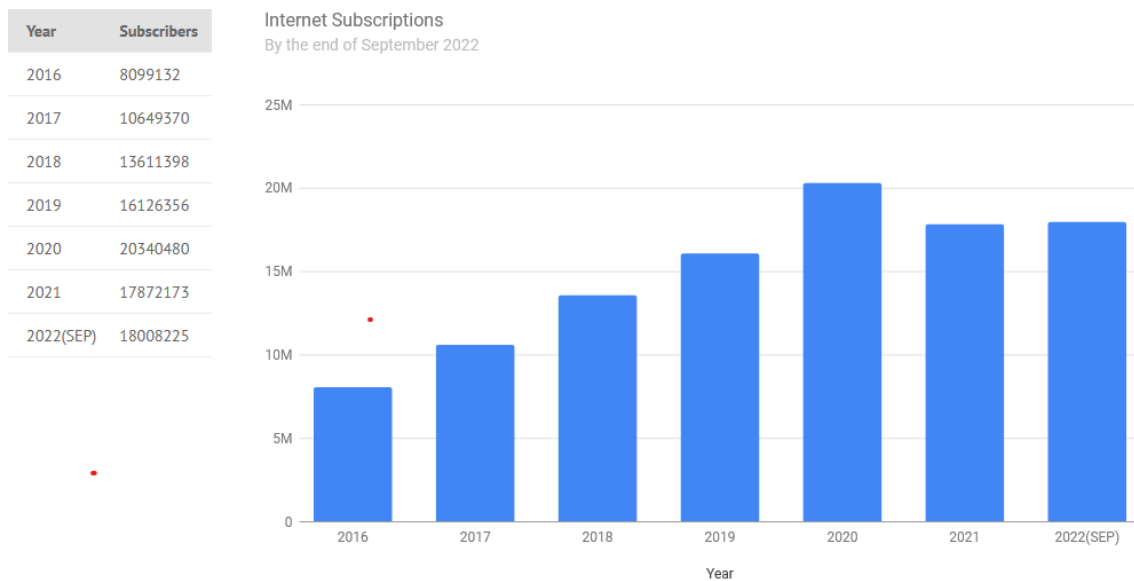


Chart 3: The number of internet subscribers in September 2022 (18,008,225 subscriptions) had increased by more than double compared to 2016 (8,099,132 subscriptions). The highest number of internet subscriptions was in 2020 (20,340,480 subscriptions) during the covid pedomic. It then decreased slightly in 2021 (17,872,173 subscriptions) and increased slightly in 2022 (18,008,225 subscriptions).

Source: [Telecommunication Regulators of Cambodia](#)

Licences

No	Licences	Total
1	International Gateway	2
2	Mobile Phone	5
3	Fixed Phone	6
4	VoIP	9
5	ISP	42
6	Satellite	1
7	Telecom Tower Sharing	4
8	Submarine Cable	2
9	Optical Cable Network	5
10	Value Added Network	1
11	Toll Free	1

Table 2: These licences have worked together in order to provide internet services and phone calls to users.

Source: [Telecommunication Regulators of Cambodia](#)

Mobile Companies

No.	Network	Company
1	Smart	Smart Axiata Co., Ltd
2	Mobitel/ CellCard	CamGSM Co., Ltd.
3	CooTel	Xinwei (Cambodia) Telecom Co., Ltd
4	SEATEL	Southeast Asia Telecom (Cambodia) Co., Ltd.
5	Metfone	Viettel (Cambodia) Pte., Ltd.

Table 3: According to TRC, three (Metfone, Cellcard, and Smart) of the five telecommunication companies account for 90% of users. Metfone has the widest coverage on mobile data and internet usage, but Cellcard has won the Ookla Speed Test Award for four years from 2017 to 2020. Smart got its reputation by promoting tech startups among youth and teenagers. Cellcard and Smart, in particular, offer many promotions, e-sports, and e-games that have gained the interest of young audiences.

Source: [Telecommunication Regulators of Cambodia](#)

Internet Service Providers

Around 42 ISPs have operated in Cambodia with licences from MPTC. Among these, five major telecommunication firms provide both land-based and mobile internet services: Viettel, Smart Axiata, CamGSM, Xinwei Telecom, and Southeast Asia Telecom, all originating from countries with authoritarian leanings. Viettel, a Vietnamese company run by Vietnam's Ministry of Defense, operates in Cambodia under the name Metfone.

CamGSM was originally known as Mobitel before rebranding itself as Cellcard in 2005.

Viettel, Smart Axiata, and local CamGSM account for around 90% of the market share of mobile subscriptions. Smart Axiata enjoyed a market share of almost 60%, while Viettel and CamGSM enjoyed 26% and 11% of the market share, respectively. Xinwei Telecom from China, which operates under the name CooTel, and Southeast Asia Telecom from Singapore account for 2.67% and 0.65% of the market share, respectively.¹⁷ In particular, Metfone provides all types of services (Internet access, leased lines, private leased circuits, mobile phone voice and messaging services, and ADSL), while the other ISPs also provide some of these other services.

The detailed names of the 42 internet service providers are listed in Annex III.

¹⁷ Asia Centre. (2021). Internet Freedoms in Cambodia: A Gateway To Control. <https://asiacentre.org/wp-content/uploads/Internet-Freedoms-in-Cambodia-A-Gateway-to-Control.pdf>

Certificates

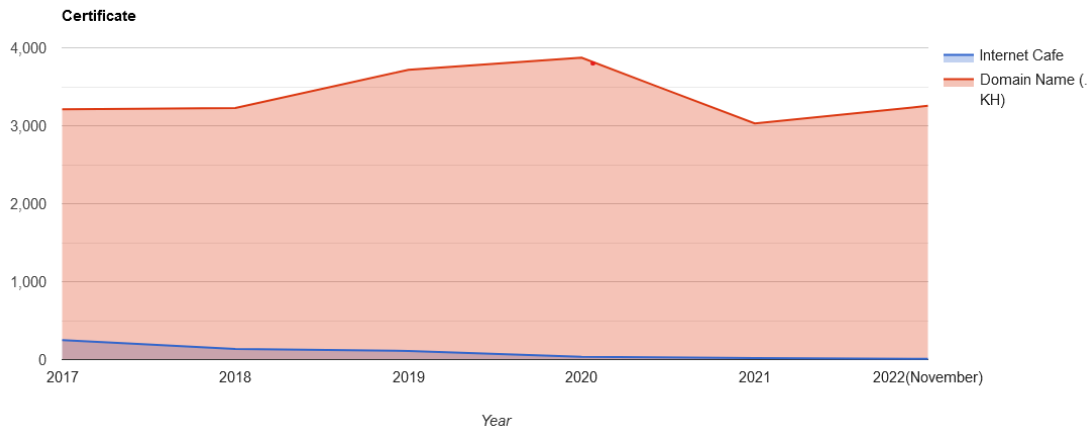


Chart 4: The total number of local domain registration from 2017 to 2022 was 20,310 domains. The highest number (3,872 domains) was in 2020. The total number of internet cafe registration was 562 internet cafes and the highest number (251 internet cafes) was in 2017.

Certificate			
No	Year	Internet Café	Domain Name (.KH)
1	2017	251	3210
2	2018	135	3226
3	2019	111	3718
4	2020	36	3872
5	2021	20	3029
6	2022(November)	9	3255

Table4: The Internet Cafe and local Domain Name (.KH) registered yearly.

Source: [Telecommunication Regulators of Cambodia](#)

Instant Messaging

Year (mil.)	Facebook User	Instagram	TikTok	LinkedIn
Jan 2023	11.75 million	1.84 million	7.4 million	0.50 million
Increase	0.91%	0.91%	1.21%	1.12%

Table 5: The social media platform Tiktok had a higher increase (1.21%) than other social media sites such as Facebook (0.91%), Instagram (0.91%), and LinkedIn (1.12%).¹⁸

Findings on Internet Censorship in Cambodia

The Open Observatory of Network Interference (OONI), in collaboration with Sinar Project and the Advocacy and Policy Institute (API), Cambodian Center for Independent Media (CCIM), and About CamboJA Journalist Alliance Association (CamboJA) performed a study of internet censorship in Cambodia. The aim of this study was to understand whether and to what extent censorship events occurred in Cambodia during the testing period from 1 July 2022 to 30 June 2023.

Blocking of websites

Throughout the one-year period, we tested 2.5 million measurements from 2,201 websites on OONI. As of 30 June 2023, the test list contained 1,629 websites in the Global Test List and 83 websites in the Cambodia Test List. Based on OONI measurements, we will generally use the terms as follows in this report:

- **Measured or Measurement Counts:** Refers to the total number of measurements collected through the OONI Probe.
- **Blocked:** Refers to “Confirmed Blocked” in OONI measurements, which are measurements from automatically confirmed blocked websites (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).
- **Input:** the number of websites that were tested.
- **Autonomous System Number (ASN):** A unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems. The Internet Service Provider (ISP) needs to register the identity of Autonomous System Number (ASN) to identify the network.

	Jul-Sep 2022	Oct-Dec 2022	Jan-Mar 2023	Apr-Jun 2023	Total
Measured	405,134	563,309	773,357	788,627	2,530,427
Blocked	0	0	243	964	1,236
Block rate	0.00%	0.00%	0.03%	0.12%	0.05%

¹⁸ *Social Media in Cambodia - 2023 Stats & Platform Trends* - OOSGA. (n.d.). OOSGA. <https://oosga.com/social-media/khm/>

	Jul-Sep 2022	Oct-Dec 2022	Jan-Mar 2023	Apr-Jun 2023	Total
Input (Website)	1,886	1,798	1,837	1,870	2,201
ASNs (Internet Service Providers)	14	19	18	22	24

Table 6: Summary of OONI web connectivity measurements for Cambodia from 1 July 2022 to 30 June 2023

From July 2022 to June 2023, there were 2201 websites measured by the OONI Probe. The results showed that in Cambodia, 37 (22 global websites and 15 Khmer websites) out of 2,201 websites were blocked or censored by DNS Blocking from the Internet Service Providers (Viettel, Ezecom, Wicam, CamSIM, Private Company (iSEEK)) by using the blocked method of DNS tampering, whereby the website would be redirected to a timed out IP address belonging to an ISP or the bogon IP address of 127.0.0.1. Several popular news outlets were also found to be censored, including Voice of Democracy (VOD), Radio Free Asian (RFA), and Cambodia Daily.

Of the 37 blocked or censored websites, it was found that some of the domains or websites are still active (12 websites), down/inaccessible (18 websites), or up for sale (7 websites). The blocked and reseller domains continued to be blocked, even though these would be active if the internet service providers (ISP) wouldn't remove them from the censored list.

Some popular websites and sub domains that have been abandoned for many years are still censored by Internet Service Providers.

- <http://khmer.cambodiadaily.com/> and <https://khmer.cambodiadaily.com/> were the former subdomains of the Cambodia Daily News Outlet, and the current official one is <https://www.cambodiadaily.com/>.

These measurements were analysed using the heuristics mentioned in Annex IV. It was found that there were 37 confirmed blocked websites of which 23 were confirmed by OONI and 14 were confirmed by heuristics and news reports together with OONI measurements. Annex 1 specifies detailed information about the blocked websites:

- Website name
- Name of Internet Service Provider
- Method of blocking
- Period of blocking
- Status of the website
- Origin (whether it is a global or Khmer websites)

Category	Category description	OONI Probe Measurements	Number of blocked and likely blocked measurements	Percentage of blocked and likely blocked measurements
ALDR	Alcohol & Drugs	27,589	451	1.6%
ANON	Anonymization and circumvention tools	155,093	8,510	5.5%
COMM	E-commerce	14,984	275	1.8%
COMT	Communication Tools	169,321	3,240	1.9%
CTRL	Control content	17,254	66	0.4%
CULTR	Culture	65,725	1,007	1.5%
DATE	Online Dating	18,985	1,939	10.2%
ECON	Economics	28,461	1,834	6.4%
ENV	Environment	54,612	705	1.3%
FILE	File-sharing	57,932	2,718	4.7%
GAME	Gaming	18,059	110	0.6%
GMB	Gambling	24,211	1,700	7.0%
GOVT	Government	28,656	3,018	10.5%
GRP	Social Networking	238,831	3,486	1.5%
HACK	Hacking Tools	28,958	2,486	8.6%
HATE	Hate Speech	6,906	194	2.8%
HOST	Hosting and Blogging Platforms	139,097	5,114	3.7%
HUMR	Human Rights Issues	274,649	10,251	3.7%
IGO	Intergovernmental Organizations	7,230	46	0.6%
LGBT	LGBT	123,863	3,732	3.0%
MILX	Terrorism and Militants	3,487	61	1.7%
MISC	Miscellaneous content	4,005	20	0.5%
MMED	Media sharing	110,189	2,729	2.5%
NEWS	News Media	570,739	26,182	4.6%
POLR	Political Criticism	54,409	3,691	6.8%
PORN	Pornography	15,187	1,159	7.6%
PROV	Provocative Attire	12,764	120	0.9%
PUBH	Public Health	68,650	1,423	2.1%
REL	Religion	60,415	3,344	5.5%
SRCH	Search Engines	44,909	1,812	4.0%
XED	Sex Education	32,889	1,291	3.9%

Table 7: Summary of OONI web connectivity measurements for Cambodia from 1 July 2022 to 30 June 2023 by category

Confirmed blocked websites by category

The numbers and percentages for the 37 blocked websites are shown by category. The red value is the percentage of blocked websites, and the black value is the number of blocked websites by category.

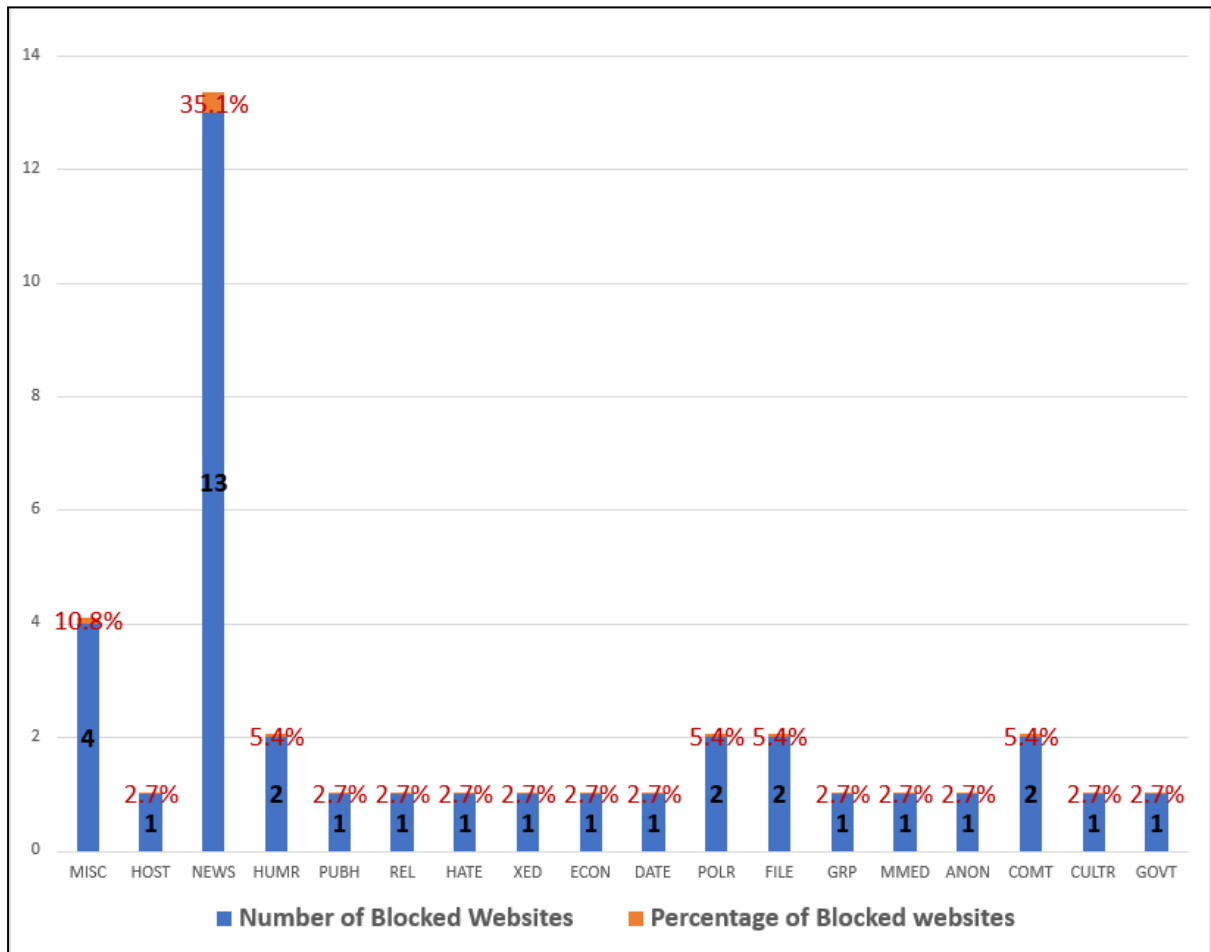


Chart 5: The highest percentage of the blocked category was News (13 websites or 35.1%) and the second one was Miscellaneous (4 websites or 10.8%)

Blocking of news websites

On 13 February 2023, [a number of independent news websites were reportedly blocked](#), particularly Voice of Democracy's (VOD) website after the news publication was shut down, Free Radio Asia, and Cambodia Daily.

In total, seven domains were found blocked based on OONI measurements. The most common blocking method was DNS tampering, whereby the website would be redirected to a bogon IP address of 127.0.0.1.

Web Connectivity Test

Cambodia

OK Confirmed Anomaly Failure

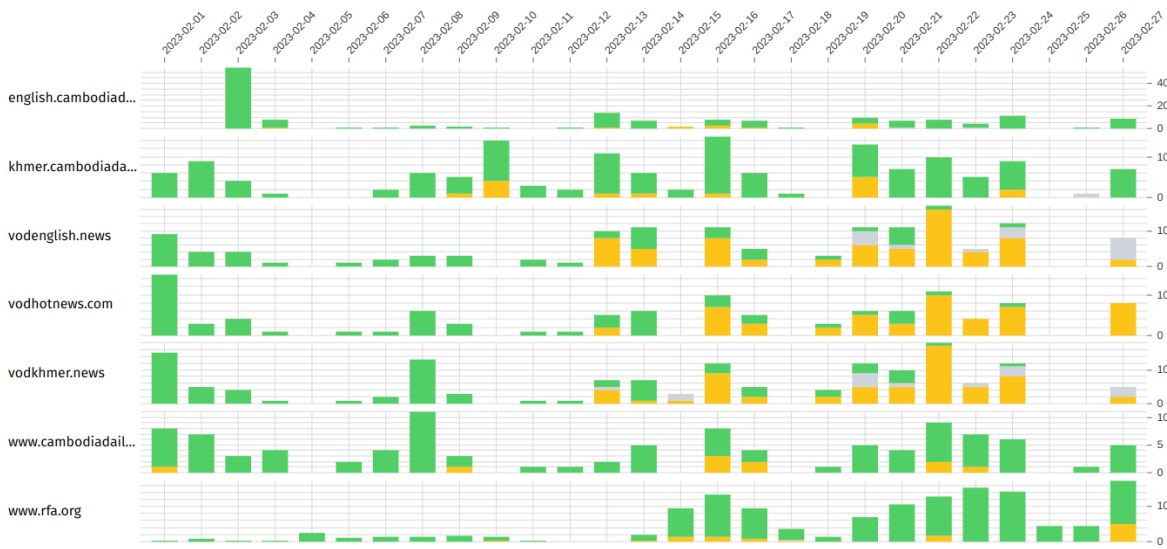


Chart 6: Blocking of news websites in Cambodia in February 2023 (Source: [OONI Explorer](#))

Blocking of instant messaging apps

	Facebook Messenger	Signal	Telegram	Whatsapp
Total Measurements	25,314	16,721	25,281	25,323
Percentage of blocked and likely blocked	0.8%	0.6%	0.5%	0.3%

Table 8: OONI measurements on instant messaging apps in Cambodia from July 2022 to June 2023

Notes:

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

Blocking of circumvention tools

	PSIPHON	Tor	Tor Snowflake	Vanilla Tor
Total Measurements	25,372	25,068	18,280	18,071
Percentage of blocked and likely blocked	0.7%	2.2%	13.6%	0.0%

Table 9: OONI measurements on circumvention tools in Cambodia from July 2022 to 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 24 vantage points in Cambodia, testing using the OONI software was not run consistently across all networks. Due to this, the findings in this report, particularly the confirmed blockings, may not show all the blockings done by the ISPs in the country.

- **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 the reason 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. Hence, 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 to 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 Cambodia.

- **Inactive websites**

For Cambodia in particular, a large number of websites found blocked have been inactive. In these cases, they may have remained in ISPs' block lists even though the domain is no longer in use or replaced.

Conclusion and recommendations

Online news sites and other websites have been found to be periodically blocked in Cambodia. Our findings show that 36 out of 2,202 websites in 2022 and 2023 were blocked, particularly those that disseminate information that could be perceived as a threat to the ruling government. Therefore, it can be concluded that press freedom and internet freedom in Cambodia are continuously under threat. In 2022 and 2023, Cambodia was classified as “Not Free”, and people are afraid to express their views or opinions online, especially those which are critical of the government.

According to the findings, 35.1% of blocked websites are news websites. Several cases of internet censorship and surveillance have been reported in Cambodia over the last decade.¹⁹ Furthermore, the Cambodian government has used the existing laws and legal regulations and developed new ones to increase interference. The forceful imposition of legal and non-legal measures by the Cambodian government against targeted groups or individuals have negatively restricted the exercise of freedom of expression and internet freedoms.

These websites include those for news and media, and thus it raises concerns about press freedom, internet freedom, and censorship in Cambodia. However, as the current data from Cambodia does not show any blocked pages, more measurements may be needed in the next round of reporting to make more substantial conclusions.

However, between the January 2022 to June 2022 and July 2022 to June 2023 reporting periods, a slight decrease was found from 43 websites to 36 websites, although this does not directly indicate reduction in censorship as the websites tested are different. It is highly likely that they were blocked by DNS and confirmed by internet service providers (Viettel, Wicam, CamSIM, Ezecom, Private Company (iSEEK)). The 36 blocked websites were censored by DNS, mainly by VIETTEL (CAMBODIA) PTE., LTD. (AS38623), S.I Group (AS38623), and CAMGSM Company Ltd (AS17976) in 2022. We consider press freedom and internet freedom in Cambodia to be continuously under threat.

Based on the analysis and findings of the report, we reiterate the recommendations made by the OHCHR. It is recommended that the State (Cambodia) review and revise its current and pending legislation, including the Sub-Decree on National Internet Gateway and the amendments to the Press Law, the leaked draft cyber security law, and the draft laws on cybercrimes. We also recommend that the draft access to information law be passed in order to ensure that vague terminology and overly broad restrictions are not used. The UN Human Rights Committee further recommends that the state ensures that in the formulation and enforcement of its legislation, including Ministerial Sub-Decrees, any restrictions on the exercise of freedom of expression and association comply with the strict requirements of articles 19 (3) and 22 of the covenant on civil and political rights and convention on human rights.

To sum it up, the government should review and reconsider uplifting blocked websites that exercise the rights and freedom of expression and internet freedoms.

¹⁹ The letter from Ministry of Information issued on 13th February 2023 ordered to shutdown VOD.

Registration of Domain Name System (.kh)

The Cambodia Post and Telecommunication department required companies to register their Local Domain Name System (.kh) to their website and email in January 2023, even though this deadline does not appear to have been strictly enforced.²⁰ There were 3255 domains that were already registered.²¹ In addition, it wasn't compulsory for The Civil Society Organization to register their domain (.kh).

We are concerned that the new draft law/regulation would make it compulsory for local CSOs, companies, and even individuals to register domain .kh. It contributes to greater control of the government over internet access and may limit freedom of information. Therefore, we are requesting that the government lift such provisions that lead to the restriction of freedom of expression on the internet.

The government should implement the Consumer Protection Law effectively and apply the law and principle of fair competitiveness amongst service providers related to digital products and services. When viewed from both a social justice perspective and economic efficiency perspective, the issues of digital rights have several implications. From a social justice perspective, everyone is entitled to the right to social, political, and economic freedom as stated in the International Covenant on Economic, Social and Cultural Rights of 1966. From an economic efficiency perspective, it shines a light on the limitations of digital rights to have a “potential impact” on the competition on two sides of the same coin. On one side of the coin, it would inhibit the principle of fair competitiveness amongst service providers related to digitally related products and services given, if the decision to block or restrict one business's websites, mostly commercial ones, is made without a property arbitration procedure. On the other side of the coin, small and medium enterprises (SMEs) might not have enough capacity and knowledge to ensure their commercial practices without high risk of restriction, blocks, or censorship. For this reason, fair arbitration or judicial procedures are needed for such a digital transformation.

Contribute to the study

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

- 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](#).

²⁰ Ogden, J. (2023, January 29). *Register .kh Domain Names in Cambodia - Cambodia Begins at 40*. Cambodia Begins at 40. <https://www.cambodiabeginsat40.com/?p=41005>

²¹ *Internet Subscriptions* | Telecommunication Regulator of Cambodia. (n.d.). Internet Subscriptions | Telecommunication Regulator of Cambodia. <https://trc.gov.kh/en/internet-subscriptions/>

- Translation: Translate the OONI Probe to your local language [here](#).
- Join the community: Participate in community discussions on [OONI's Slack channel](#).

Acknowledgements

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

Annex I: List of confirmed blockings

No.	Websites/ URL	Category	Internet Service Providers that implemented blocking	Method of Blocking	Explorer Link	Country	Remark
1	https://securevpn.im/	ANON	Viettel (Metfone)	DNS	Link	Global	Active
2	https://www.icconnectthere.com/	COMT	Viettel (Metfone)	DNS	Link	Global	Active
3	https://www.epa.gov/	GOVT	Viettel (Metfone), CamGSM, Ezecom, Wicam	DNS	Link	Global	Active
4	http://www.qhtyzx.com/	NEWS	Viettel (Metfone)	DNS	Link	Khmer	Active
5	https://vodenglish.news/	NEWS	Ezecom	DNS	Link	Khmer	Active
6	https://vodkhmer.news/	NEWS	Ezecom	DNS	Link	Khmer	Active
7	https://www.rfa.org/	NEWS	SINET, WICAM	DNS	Link	Khmer	Active

No.	Websites/ URL	Category	Internet Service Providers that implemented blocking	Method of Blocking	Explorer Link	Country	Remark
8	https://english.cambodiadaily.com/	NEWS	SINET	DNS	Link	Khmer	Active
9	https://vodhotnews.com	NEWS	WiCAM Corporation Ltd., Viettel (Metfone), EZECOM limited, KingCorp Inc, COGETEL Co., Ltd, S.I Group, Smart Axiata, Co., Ltd., CAMGSM Company Ltd	DNS	Link	Khmer	Active
10	https://dailystormer.name/	POLR	Viettel (Metfone)	DNS	Link	Khmer	Active
11	https://occupystreams.org/	POLR	Ezecom,Wicam	DNS	Link	Khmer	Active
12	http://www.teenhealthfx.com/	XED	Viettel (Metfone)	DNS	Link	Global	Active
13	https://www.cipl-organization.org/	CULTR	Viettel (Metfone)	DNS	Link	Khmer	Domain on sale

No.	Websites/ URL	Category	Internet Service Providers that implemented blocking	Method of Blocking	Explorer Link	Country	Remark
14	http://www.adhoc-cambodia.org/	HUMR	Viettel (Metfone)	DNS	Link	Global	Domain on sale
15	http://stubes.info/onlain/italbGdoRW1hS2JrOGc	NEWS	Viettel (Metfone)	DNS	Link	Global	Domain on sale
16	http://www.kirivong.com/	NEWS	Viettel (Metfone), private companies (iSeek)	DNS	Link	Global	Domain on sale
17	http://www.ksn-news.com/	NEWS	Viettel (Metfone)	DNS	Link	Global	Domain on sale
18	https://www.monorom.info/	NEWS	Viettel (Metfone), private companies (iSeek)	DNS	Link	Khmer	Domain on sale
19	http://www.healthcambodia.org/	PUBH	Viettel (Metfone), private companies (iSeek)	DNS	Link	Global	Domain on sale
20	https://site.voicepulse.com/	COMT	Viettel (Metfone), private companies (iSeek), Wicam	DNS	Link	Global	Inactive
21	https://cambodian.dating/	DATE	Viettel (Metfone)	DNS	Link	Global	Inactive

No.	Websites/ URL	Category	Internet Service Providers that implemented blocking	Method of Blocking	Explorer Link	Country	Remark
22	https://bitcoin-mix.org/	ECON	Viettel (Metfone)	DNS	Link	Global	Inactive
23	https://sci-hub.se/	FILE	Viettel (Metfone)	DNS	Link	Khmer	Inactive
24	https://www.libgen.tw/	FILE	Viettel (Metfone)	DNS	Link	Global	Inactive
25	https://scontent-frt3-2.cdninstagram.com/favicon.ico	GRP	Viettel (Metfone), private companies (iSeeK), CamGSM	DNS	Link	Global	Inactive
26	http://www.nazi-lauck-nsdapao.com/	HATE	Viettel (Metfone)	DNS	Link	Global	Inactive
27	http://ocsp.int-x3.letsencrypt.org/	HOST	Viettel(Metfone)	DNS	Link	Global	Inactive
28	http://www.ycc.org.kh/	HUMR	Viettel (Metfone), private companies (iSeeK), CamGSM	DNS	Link	Khmer	Inactive
29	http://hdhdhdgd.com	MISC	Viettel (Metfone)	DNS	Link	Global	Inactive

No.	Websites/ URL	Category	Internet Service Providers that implemented blocking	Method of Blocking	Explorer Link	Country	Remark
30	https://secure.flickr.com/	MMED	Viettel (Metfone), private companies (iSeeK), Wicam	DNS	Link	Global	Inactive
31	http://www.repubblica.com/	NEWS	Viettel (Metfone), private companies (iSeeK)	DNS	Link	Khmer	Inactive
32	http://www.ruf-ch.org/	NEWS	Viettel (Metfone), private companies (iSeeK)	DNS	Link	Global	Inactive
33	https://khmer.cambodiadaily.com/	NEWS	Viettel (Metfone), private companies (iSeeK)	DNS	Link	Khmer	Inactive
34	http://www.islamdoor.com/	REL	Viettel (Metfone)	DNS	Link	Global	Inactive
35	http://khmer.cambodiadaily.com/	NEWS	Viettel (Metfone), private companies (iSeeK), SINET,	DNS	Link	Global	Inactive
36	http://www.cannabis.info/	MSC	Viettel (Metfone)	DNS	Link	Global	Inactive
37	http://www.hrcr.org/	HUMR	Viettel (Metfone)	DNS	Link	Khmer	Inactive

Annex II: List of Internet Service Providers (ISPs)

No.	ASNs	ASN Name	ASN Registration Country
1	AS23673 AS24325	Cogetel Online	KH
2	AS24478	AngkorNet	KH
3	AS38901	EZECOM	KH
4	AS38623	Viettel (Metfone)	KH
5	AS38893	Clicknet	KH
6	AS17976	TeleSURF / Mobitel	KH
7	AS24492	WiCam	KH
8	AS17726	CamNet	KH
9	AS45348	Chuan Wei	KH
10	AS18014 AS24441	City Link	KH
11	AS38209	Camintel	KH
12	AS131186 AS131203	MekongNet	KH
13	AS45498	Smart Mobile	KH
14	AS38235	MekongNet IXP	KH
15	AS24567	WirelessIP	KH
16	AS45339	BeyondTel	KH
17	AS7712	CIDC IT	KH
18	AS17981	Cambo Technology	KH
19	AS45429	DTV Star	KH
20	AS38600 AS45281	Hello	KH
21	AS9902 AS23868	NeocomISP	KH
22	AS38286	PPCTV	KH
23	AS45124	Finder IXP	KH
24	AS38723	Star-Cell	KH
25	AS45465	Flash Tech	KH
26	AS131178	Opennet	KH
27	AS131207	S.I Net	KH
28	AS38579	CB	KH

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 here.</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&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, to provide users with faster access to websites, and for a number of other networking purposes.</p> <p>Middleboxes are sometimes 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 a 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 https://www.facebook.com/), 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 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 affected the implementation of internet censorship in the country.

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

How are the network measurements gathered?

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

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

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

How are the network measurements analysed?

OONI processes the following types of data through its [data pipeline](#):

Country code

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

Autonomous System Number (ASN)

By default, OONI collects the Autonomous System Number (ASN) of the network used to run 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 to evaluate when network interferences occur and to allow 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 organizations. 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. 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.
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.

No.	Category Description	Code	Description
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. To protect its users from potential risks, OONI takes measures to remove them 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 [OONI Explorer](#) or through [OONI's measurement API](#).

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

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

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

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

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

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

Since 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, heuristics as 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
				
		False positive	Confirmed blocking	Sampled measurement is analyzed 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 would 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 available measurements on OONI. For this study, 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.