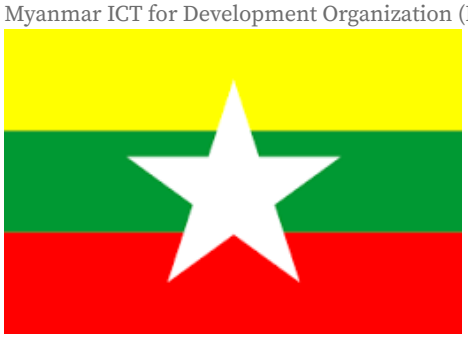
The State of Internet Censorship in Myanmar

Kay Yen Wong (Sinar Project), Maria Xynou (OONI), Arturo Filastò (OONI), Khairil Yusof (Sinar Project),Tan Sze Ming (Sinar Project), Myanmar ICT for Development Organization (MIDO), 2017-03-29 13:31 UTC



A research study by the Open Observatory of Network Interference (OONI), Sinar Project, and the Myanmar ICT for Development Organization (MIDO).

Table of contents

Country: Myanmar

Probed ISPs: FMG Company Limited (AS63852), Global Technology Co., Ldt (AS133524), OOREDOO Myanmar (AS132167), Telenor Myanmar (AS133385), Myanma Posts & Telecommunications (AS9988), Yatanarpon Teleport Company Limited (AS18399).

Testing period: 25th October 2016 - 28th February 2017

OONI tests: Web Connectivity, HTTP Invalid Request Line, HTTP Header Field Manipulation, WhatsApp test, Facebook Messenger test, Vanilla Tor test.

Censorship method: Signs of TCP/IP blocking and HTTP blocking.

Key Findings

Out of 1,927 sites that were tested for censorship in six local vantage points in Myanmar, only five sites presented signs of TCP/IP and HTTP blocking, including the sites of the U.S. embassy in Myanmar and of the Organization of American States (OAS). The motivation and justification behind the potential blocking of these sites remains unclear. No block pages were detected as part of this study that can confirm cases of censorship.

Similarly, no middle boxes were detected as part of this study. Blue Coat software (some types of which can potentially be used for internet censorship and surveillance) was previously detected in Myanmar by OONI in late 2012. Extensive tests though performed across six different networks in Myanmar show that Blue Coat software didn't appear to be present during the testing period (25th October 2016 to 28th February 2017), indicating that it may have been removed.

WhatsApp, Facebook Messenger, and the Tor network appeared to be accessible across all six networks in Myanmar where OONI tests were run.

Introduction

In an attempt to examine the current state of internet censorship in Myanmar, the Open Observatory of Network Interference (OONI), Sinar Project and Myanmar ICT for Development Organization (MIDO) collaborated on a joint study to examine whether internet censorship events were persisting in the country through the collection and analysis of network measurements.

The aim of this study is to increase transparency of internet controls in Myanmar and to collect data that can potentially corroborate rumours and reports of internet censorship events. The following sections of this report provide information about Myanmar's network landscape and internet penetration levels, its legal environment with respect to freedom of expression, access to information and privacy, as well as about cases of censorship and surveillance that have previously been reported in the country. The remainder of the report documents the methodology and key findings of this study.

Background

Myanmar is a sovereign state with a population of around 51 million in South East Asia, bordering the Andaman Sea and the Bay of Bengal, between Bangladesh and Thailand. It is a parliamentary republic with 7 regions, 7 states, and 1 union territory.

Its population is comprised of 135 distinct officially recognised ethnic groups, with the majority Burman ethnic group making up 68% of the population and dominating the military and government. The minority ethnic groups includes the Shans (9%), Karens (7%), Rakhines (4%), Chinese (3%), Indians (2%) and Mon (2%), with the other ethnic groups consisting the remaining 5%.

According to Myanmar's 2014 census, a large majority of Myanmar's population practices Buddhism, with 87.9% identifying as Buddhists, 6.2% as Christians, 4.3% Muslims, 0.8% Animists, 0.5% Hindus, 0.2% as 'other' and the remaining 0.1% as 'none'. Non-Buddhist minorities face widespread persecution and prejudice, with the Rohingya minority having continued to suffer from human rights violation under the military junta since 1978, with continued criticism by human rights organisations on the government's treatment of the Rohingya minority. The government has been actively accused of forced or pressured religious conversions of non-Buddhist minorities. Adherence to Buddhism was an unwritten prerequisite for promotions within the government and army, with nearly all senior level officers of the armed forces and the ruling State Peace Development Council (SPDC) identifying as Buddhists.

Civil wars and rampant ethnic and religious strife have been a constant feature of Myanmar's socio-political landscape for most of its independent years as ethnic minorities struggle for ethnic and sub-national autonomy. Human rights violations and systematic denial of basic rights such as freedom of expression, association, and assembly, occurred with regularity during the military junta's rule of the country from 1962 till 2011. The ruling State Peace and Development Council (SPDC) regularly arrested activists and opposition party members sentenced by unfair trials in closed courts, in addition to

imposing systematic restrictions of information control to limit social mobilisation around key political events.

From 1962, the country was ruled by the military junta up until 2011 when it was officially dissolved and replaced with a nominally civilian government following the 2010 general election. Although the 2010 election was criticised for declaring the National League for Democracy (NLD) illegal, and only allowing government sanctioned political parties to contest in it, it marked the transition of the military's movement towards more openness, with the government's political reforms which included ending the house arrest of NLD's pro-democracy leader Aung San Suu Kyi, the release of 200 political prisoners as part of a general amnesty, relaxation of press censorship, and institution of new labour laws.

Drastic reforms in September 2011 marked the military government's transition to more openness, with significant relaxations of the country's censorship policies. Censorship tests conducted by ONI in 2012 found reductions in the scope and depth of content filtered in 2012 compared to in 2005, with a majority of previously censored political content ranging from independent news sites, the websites of opposition parties, and critical political content made accessible. Despite that, a culture of self-censorship remains, with many media organisations taking precaution to avoid accusations of libel and state security charges. With the new transition towards a free democratic system following the win of the opposition party, National League for Democracy in the most recent 2015 election, it is imperative to continue the questioning of the true breadth and depth of the current state of censorship in Myanmar.

Myanmar's transition to a civilian government in 2011 began an economic overhaul aimed at attracting foreign investors, and integrating Myanmar into the global economy. This, along with the easing of most Western sanctions has led to its accelerated growth in 2013 and 2014, with a GDP growth of 8.7%. Despite this, due to the former military government's isolationist policies and economic mismanagement, Myanmar's income gap is among the widest in the world, as a large proportion of the economy remains under the control of supporters of the previous military government.

Myanmar ranks as a corrupt nation, with a Corruption Perceptions Index rank of 136 out of 176, and a rating of 28 out of 100 as of 2016.

Network landscape and internet penetration

As of 2016, internet penetration rates in Myanmar are at 19.3%, quickly growing due to the sharp increase in its mobile penetration rate with the emergence of cheap mobile internet and improved telecommunication infrastructure. Despite the strong growth in Myanmar's mobile penetration rate from 7% in 2013 to 85% by 2016, fixed line telephone penetration remains low at just under 1%.

Prior to September 2011, a combination of government censorship, deliberate infrastructure and technical constraints, deliberately controlled internet speeds with proxy-caching servers, and government restrictions on pricing limited the internet penetration rates in Myanmar, with it being as low as 0.2% in 2010.

The government's expansive control over the internet was largely facilitated by the fact that users were limited to only two ISPs, Myanmar Posts and Telecom (MPT) and Bagan Cybertech (currently Yatanarpon Telecom), both of which were state-controlled by the Myanmar government. With low computer ownership, most users relied on internet cafés, promoted as "Public Access Centres" (PAC) for internet access, with many internet cafés utilising proxy sites and circumvention tools to bypass government restrictions.

Following the enactment of the Information Technology Law, the government began the issuing of ISP licenses to new operators in 2013 in an effort to open up Myanmar's telecommunications market. With the entry of two foreign operators Ooredoo and Telenor in the local mobile market leading to the emergence of cheap mobile internet and improved telecommunication infrastructure, internet penetration rates skyrocketed to 12.6% in 2015, with it currently growing at 19.3% in 2016.

The table below illustrates some of the main providers in Myanmar.

Mobile Operators/ISPs	Fixed Internet	Mobile Internet
Myanmar Posts and Telecom (MPT)	X	X
Yatanarpon Telecom Company	X	X
Telenor Myanmar Limited		X
Ooredoo Myanmar Limited		X
Global Technology Co., Ltd	X	
Fiber Link Myanmar Co., Ltd	X	
Fortune Broadband	X	
Elite Tech	X	
WeLink	X	
Amara Communications Co., Ltd		X
Bluewave	X	
AGB	X	
Spectrum Life Net Core	X	
Myanmar Net	X	

Legal environment

Freedom of expression

Telecommunications Law 2013

The 2013 Telecommunications Law restricts speech via telecommunications equipment. Section 66D prohibits the "extortion, coercion, wrongful restrainment, defamation, undue influence or threatening of any person" using any telecommunications networks. The use of such subjective terms imposes on the criminal liability of the speech of any telecommunications user.

The Research Team for Telecommunication Law, as established by the Committee for Amending the Telecommunication Law, has analyzed the Telecommunication Law from various aspects, particularly from the view of the legal system and IT technology. According to the findings, this law has resulted in seven cases under section 66(d) and five charges under the former President U Thein Sein administration. Under the present National League for Democracy government, there have been forty-two 66(d) cases, with five resulting in charges, and eight people being held in custody. The rest are ongoing cases.

Many of these cases may result from the vague terminology and definitions used as part of Myanmar's Telecommunication Law. The Research Team for Telecommunication Law pointed out, for example, that Section 68(a) of the Law ("Connecting, receiving, transmitting, distributing or handing out false information dishonestly or participating in such activity") is vague, confusing, and does not specify the types of online activities that could potentially result in prosecution.

Myanmar Penal Code

Section 124A [Sedition] of the Myanmar Penal Code prohibits any words, either spoken or written, signs, or visible representations that bring into hatred, contempt, attempts to excite, or disaffection towards the government, and can be punished by life imprisonment or imprisonment of a shorter term to which a fine may be added.

Sections 499-502 [Defamation] allow the state to prosecute an individual for defamation, defined as making or publishing any imputation concerning a person intending to harm the reputation of such a person, with a penalty of imprisonment of up to 2 years.

Section 505B [Public Tranquility] punishes the creation, publication or circulation of any statement or rumour with the intent to cause fear or alarm to the public which may induce them to commit an offence against the State or against public tranquility, with the penalty of imprisonment which may extend to two years.

Computer Science Development Law (1996)

Section IX of the 1996 Computer Science Development Law requires prior permission and registration for the importing, keeping, or utilization of computers or related equipment in addition to the setting up of computer networks. Failure to comply with the stipulations of the Ministry of Communications, Posts and Telegraphs is punishable by imprisonment of up to 15 years, and may also be liable to a fine. Despite it being effectively superseded by the 2004 Electronic Transactions Act and subsequently the 2013 Telecommunications Act, it has never been formally repealed and technically remains in force.

Press freedom

End of pre-publication censorship 2012

In 2012, as part of Myanmar's reform process, the country's Ministry of Information abolished pre-publication censorship practices, no longer requiring media organisations to submit their content to a censorship board prior to publication. However, a culture of self-censorship remains, with many media organisations taking precaution to avoid accusations of libel and state security charges.

Broadcast Law 2015

The Broadcast Law lifted the ban on private ownership of daily newspapers for the first time, with broadcast licenses to public service, commercial and community broadcasters authorized and revoked by

a Broadcast Council. However, the law maintains government control over the broadcasting sector– members of the Broadcast Council are appointed by its president, leaving it open to political manipulation, and undermining its independence.

Access to information

Official Secrets Act 1923

Myanmar's broadly drawn Official Secrets Act which dates back to 1923 penalizes the receival and dissemination of a broadly defined range of documents, especially government documents. Section 3(1)(a) of the Official Secrets Act provides penalties of up to 14 years of imprisonment for anyone approaching or entering a broad range of prohibited places. Section 5 of the Act severely limits the disclosure of information of any kind by anyone within or with connections to the government, in addition to making it an offense to receive such information, with both offenses carrying providing penalties of up to 2 years of imprisonment.

Electronic Transactions Law 2004

The 2004 Electronic Transaction Law forbids the sending or distribution of "information relating to secrets of the security of the state" through the internet. Due to the broadness of this definition, this applies to communications about cultural or economic affairs, and has been used to imprison journalists, bloggers or activists. The law, along with the Television and Video Law was applied by closed courts (mostly operating out of Insein prison) to deliver sentences of up to 65 years to activists, bloggers and members of the 88 Generation Students Group.

Privacy

Section 357 of the Constitution of Burma 2008 states that "the Union must protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of the Constitution". Certain data privacy requirements exist as part of Myanmar's 2004 Electronic Transactions Law. Some ISPs such as Telenor have adopted their own policies in regards to the privacy of their customers. The company stated in their policy that they hold a public commitment to protecting their subscribers' freedom of expression and privacy in accordance with local legislation.

In mid-December 2016, Myanmar ICT for Development Organization (MIDO) organized the Myanmar Digital Rights Forum, together with Phandeeyar, Myanmar Centre for Responsible Business and EngagedMedia.org, with support from the Embassy of Sweden. The two-day Forum brought together about 90 representatives from organizations of the private sector and civil society, as well as government and media, to discuss concerns to digital rights.

The participants discussed the (then) draft Citizens' Privacy and Security Protection Bill and raised a number of concerns about its impact and practical implementation. Many of the concerns pertained to the flaws and vague definitions included in the Bill, as well as to its limited compliance with international human rights standards. Some of the participants pointed out that the Bill does not contain a clear process for seeking permission, an order or a warrant that would authorize the circumstances for data collection and retention. As such, representatives from 18 organizations attending the Myanmar Digital Rights Forum released a joint statement urging the Union Parliament and the Government not to expedite the law enacting without having nation-wide public consultation.

Despite the comments and requests made by civil society organizations, the Citizens' Privacy and Security Protection Bill was enacted into law on 8th March 2017. The main changes to the law, compared to the

original draft, include the removal of the bylaw making powers from the Home Ministry, and the insertion of vague wording in Article 8 for "permission from the Union President or a Union-level Government body".

Censorship and surveillance

Telecommunications Law 2013

Articles 75 and 77 of the 2013 Telecommunications Law allows the government to intercept, suspend, or obtain any information that threatens the national security and prevalence of law in the country. The broad provision fails to specify which government agents are authorised to do this, and what sort of information specifically constitutes the general terms such as 'national security'.

Reported cases of internet censorship and surveillance

The internet freedom landscape in Myanmar appears to have taken a relatively positive turn following the 2011 reforms. Nonetheless, some cases of internet censorship and surveillance that have been reported since are included below.

Internet café surveillance

A 2011 report by Reporters Without Borders(RSF) revealed the issuing of a set of expansive directives by the Ministry of Communications Post and Telegraphs (MCPT) requiring owners of internet cafés to collect and share with the authorities the personal data of their patrons including their "names, National Registration Card number, passport number (if the user is a foreigner), contact address", in addition to a log of their internet records.

Internet censorship devices

In 2011, Citizen Lab research uncovered the use of commercial filtering devices manufactured by U.S.-based Blue Coat Systems in Myanmar. Tests of internet filtering conducted within Burma running on Open Net Initiative (ONI) developed software provided evidence that Blue Coat's devices were being used to actively filter internet content in Myanmar. Of the 37 Blue Coat content categories, all URLs from 10 categories on ONI's test list appeared to be blocked entirely, including categories for pornography, LGBT, Hacking, and Proxy Avoidance.

Similarly, a report by Reporters without Borders revealed the acquisition of censorship equipment and hardware from the Chinese subsidiary of Alacatel-Lucent. The offering of a website filtering and surveillance system by Alcatel-Lucent's Chinese subsidiary was confirmed by a spokesman for Hanthawaddy, a state-controlled ISP.

Blue Coat software (some types of which can potentially be used for internet filtering, censorship, and surveillance) was detected in Myanmar through OONI's HTTP Invalid Request Line test in late 2012. It remains unclear, however, if this was a country-wide deployment or if it was only used in the specific network that was tested. Two years later OONI's HTTP Invalid Request Line test was run in the same network, but the presence of Blue Coat systems was not detected (indicating that it was possibly removed from that specific network).

Hacking Team Surveillance Software

Leaked email communications from 2015 revealed a discussion between Hacking Team, an Italian spyware company, and the Myanmar government on establishing domestic surveillance mechanisms, with the earliest communication dating back to 2012. Although Hacking Team's offer 'active IT intrusion services' appears to have failed, the fact that such options were being considered by the Myanmar government is disturbing.

Blocking of Facebook

Following days of unrest and inter-communal violence between Buddhist and Muslim residents of the Mandalay region which left two dead and 14 injured, Facebook went down in Myanmar coinciding with the government-imposed curfew hours in Mandalay, with speculation that the blocked access may have been to prevent online users from posting hate speech and fueling unrest in Mandalay.

Examining internet censorship in Myanmar

The Open Observatory of Network Interference (OONI), in collaboration with Sinar Project and Myanmar ICT for Development Organization (MIDO), performed a study of internet censorship in Myanmar. The aim of this study was to understand whether and to what extent censorship events occurred in Myanmar during the testing period.

The sections below document the methodology and key findings of this study.

Methodology

The methodology of this study, in an attempt to identify potential internet censorship events in Thailand, included the following:

- Review of the Citizen Lab's test list for Myanmar
- OONI network measurements
- Data analysis

A list of URLs that are relevant and commonly accessed in Myanmar was created by the Citizen Lab in 2014 for the purpose of enabling network measurement researchers to examine their accessibility in Myanmar. As part of this study, this list of URLs was reviewed to include additional URLs which - along with other URLs that are commonly accessed around the world - were tested for blocking based on OONI's free software tests. Such tests were run from local vantage points in Myanmar, and they also examined whether systems that are responsible for censorship, surveillance and traffic manipulation were present in the tested network. Once network measurement data was collected from these tests, the data was subsequently processed and analyzed based on a set of heuristics for detecting internet censorship and traffic manipulation.

The testing period for this study started on 25th October 2016 and concluded on 28th February 2017.

Review of the Citizen Lab's test list for Myanmar

An important part of identifying censorship is determining *which* websites to examine for blocking.

OONI's software (called *OONI Probe*) is designed to examine URLs contained in specific lists ("test lists") for censorship. By default, OONI Probe examines the "global test list", which includes a wide range of internationally relevant websites, most of which are in English. These websites fall under 31 categories,

ranging from news media, file sharing and culture, to provocative or objectionable categories, like pornography, political criticism, and hate speech.

These categories help ensure that a wide range of different types of websites are tested, and they enable the examination of the impact of censorship events (for example, if the majority of the websites found to be blocked in a country fall under the "human rights" category, that may have a bigger impact than other types of websites being blocked elsewhere). The main reason why objectionable categories (such as "pornography" and "hate speech") are included for testing is because they are more likely to be blocked due to their nature, enabling the development of heuristics for detecting censorship elsewhere within a country.

In addition to testing the URLs included in the global test list, OONI Probe is also designed to examine a test list which is specifically created for the country that the user is running OONI Probe from, if such a list exists. Unlike the global test list, country-specific test lists include websites that are relevant and commonly accessed within specific countries, and such websites are often in local languages. Similarly to the global test list, country-specific test lists include websites that fall under the same set of 31 categories, as explained previously.

All test lists are hosted by the Citizen Lab on GitHub, supporting OONI and other network measurement projects in the creation and maintenance of lists of URLs to test for censorship. As part of this study, OONI and Sinar Project reviewed the Citizen Lab's test list for Myanmar by adding more URLs to be tested for censorship. Overall, *822 URLs* that are relevant to Myanmar were tested as part of this study. In addition, the URLs included in the Citizen Lab's global list (including 1,105 different URLs) were also tested.

It is important to acknowledge that the findings of this study are only limited to the websites that were tested, and do not necessarily provide a complete view of other censorship events that may have occurred during the testing period.

OONI network measurements

The Open Observatory of Network Interference (OONI) is a *free software* project that aims to increase transparency of internet censorship around the world. Since 2012, OONI has developed multiple free and open source software tests designed to examine the following:

- Blocking of websites.
- Blocking of censorship circumvention tools (such as Tor).
- Blocking of instant messaging apps.
- Detection of systems responsible for censorship, surveillance, and traffic manipulation.

As part of this study, the following OONI software tests were run from six different local vantage points in Myanmar:

- Web connectivity
- HTTP invalid request line
- HTTP header field manipulation
- Vanilla Tor

- WhatsApp
- Facebook Messenger

The Web Connectivity test was run with the aim of examining whether a set of URLs (included in both the "global test list" and the recently updated "Myanmar test list") were blocked during the testing period and if so, how. The Vanilla Tor test was run to examine the reachability of the Tor network, while the WhatsApp and Facebook Messenger tests were run to examine whether these instant messaging apps were blocked in Myanmar during the testing period.

The HTTP invalid request line and HTTP header field manipulation tests were run with the aim of examining whether "middle boxes" (systems placed in the network between the user and a control server) that could potentially be responsible for censorship and/or surveillance were present in the tested network.

The sections below document how each of these tests are designed for the purpose of detecting cases of internet censorship and traffic manipulation.

Web Connectivity test

This test examines whether websites are reachable and if they are not, it attempts to determine whether access to them is blocked through DNS tampering, TCP/IP blocking or by a transparent HTTP proxy. Specifically, this test is designed to perform the following:

- Resolver identification
- DNS lookup
- TCP connect
- HTTP GET request

By default, this test performs the above (excluding the first step, which is performed only over the network of the user) both over a control server and over the network of the user. If the results from both networks match, then there is no clear sign of network interference; but if the results are different, the websites that the user is testing are likely censored.

Further information is provided below, explaining how each step performed under the web connectivity test works.

1. Resolver identification

The domain name system (DNS) is what is responsible for transforming a host name (e.g. torproject.org) into an IP address (e.g. 38.229.72.16). Internet Service Providers (ISPs), amongst others, run DNS resolvers which map IP addresses to hostnames. In some circumstances though, ISPs map the requested host names to the wrong IP addresses, which is a form of tampering.

As a first step, the web connectivity test attempts to identify which DNS resolver is being used by the user. It does so by performing a DNS query to special domains (such as whoami.akamai.com) which will disclose the IP address of the resolver.

2. DNS lookup

Once the Web Connectivity test has identified the DNS resolver of the user, it then attempts to identify which addresses are mapped to the tested host names by the resolver. It does so by performing a DNS lookup, which asks the resolver to disclose which IP addresses are mapped to the tested host names, as well as which other host names are linked to the tested host names under DNS queries.

3. TCP connect

The web connectivity test will then try to connect to the tested websites by attempting to establish a TCP session on port 80 (or port 443 for URLs that begin with HTTPS) for the list of IP addresses that were identified in the previous step (DNS lookup).

4. HTTP GET request

As the web connectivity test connects to tested websites (through the previous step), it sends requests through the HTTP protocol to the servers which are hosting those websites. A server normally responds to an HTTP GET request with the content of the webpage that is requested.

Comparison of results: Identifying censorship

Once the above steps of the web connectivity test are performed *both* over a control server and over the network of the user, the collected results are then compared with the aim of identifying whether and how tested websites are tampered with. If the compared results do *not* match, then there is a sign of network interference.

Below are the conditions under which the following types of blocking are identified:

- **DNS blocking:** If the DNS responses (such as the IP addresses mapped to host names) do *not* match.
- **TCP/IP blocking:** If a TCP session to connect to websites was *not* established over the network of the user.
- **HTTP blocking:** If the HTTP request over the user's network failed, or the HTTP status codes don't match, or all of the following apply:

1. The body length of compared websites (over the control server and the network of the user) differs by some percentage;
2. The HTTP headers names do not match;
3. The HTML title tags do not match.

It's important to note, however, that DNS resolvers, such as Google or a local ISP, often provide users with IP addresses that are closest to them geographically. Often this is *not* done with the intent of network tampering, but merely for the purpose of providing users with localized content or faster access to websites. As a result, some false positives might arise in OONI measurements. Other false positives might occur when tested websites serve different content depending on the country that the user is connecting from, or in the cases when websites return failures even though they are not tampered with.

HTTP Invalid Request Line test

This test tries to detect the presence of network components ("middle box") which could be responsible for censorship and/or traffic manipulation.

Instead of sending a normal HTTP request, this test sends an invalid HTTP request line - containing an invalid HTTP version number, an invalid field count and a huge request method – to an echo service listening on the standard HTTP port. An echo service is a very useful debugging and measurement tool, which simply sends back to the originating source any data it receives. If a middle box is not present in the network between the user and an echo service, then the echo service will send the invalid HTTP request line back to the user, exactly as it received it. In such cases, there is no visible traffic manipulation in the tested network.

If, however, a middle box is present in the tested network, the invalid HTTP request line will be intercepted by the middle box and this may trigger an error and that will subsequently be sent back to OONI's server. Such errors indicate that software for traffic manipulation is likely placed in the tested network, though it's not always clear what that software is. In some cases though, censorship and/or surveillance vendors can be identified through the error messages in the received HTTP response. Based on this technique, OONI has previously detected the use of BlueCoat, Squid and Privoxy proxy technologies in networks across multiple countries around the world.

It's important though to note that a false negative could potentially occur in the hypothetical instance that ISPs are using highly sophisticated censorship and/or surveillance software that is specifically designed to not trigger errors when receiving invalid HTTP request lines like the ones of this test. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

HTTP Header Field Manipulation test

This test also tries to detect the presence of network components ("middle box") which could be responsible for censorship and/or traffic manipulation.

HTTP is a protocol which transfers or exchanges data across the internet. It does so by handling a client's request to connect to a server, and a server's response to a client's request. Every time a user connects to a server, the user (client) sends a request through the HTTP protocol to that server. Such requests include "HTTP headers", which transmit various types of information, including the user's device operating system and the type of browser that is being used. If Firefox is used on Windows, for example, the "user agent header" in the HTTP request will tell the server that a Firefox browser is being used on a Windows operating system.

This test emulates an HTTP request towards a server, but sends HTTP headers that have variations in capitalization. In other words, this test sends HTTP requests which include valid, but non-canonical HTTP headers. Such requests are sent to a backend control server which sends back any data it receives. If OONI receives the HTTP headers exactly as they were sent, then there is no visible presence of a "middle box" in the network that could be responsible for censorship, surveillance and/or traffic manipulation. If, however, such software is present in the tested network, it will likely normalize the invalid headers that are sent or add extra headers.

Depending on whether the HTTP headers that are sent and received from a backend control server are the same or not, OONI is able to evaluate whether software – which could be responsible for traffic manipulation – is present in the tested network.

False negatives, however, could potentially occur in the hypothetical instance that ISPs are using highly sophisticated software that is specifically designed to not interfere with HTTP headers when it receives them. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

Vanilla Tor test

This test examines the reachability of the Tor network, which is designed for online anonymity and censorship circumvention.

The Vanilla Tor test attempts to start a connection to the Tor network. If the test successfully bootstraps a connection within a predefined amount of seconds (300 by default), then Tor is considered to be reachable from the vantage point of the user. But if the test does not manage to establish a connection, then the Tor network is likely blocked within the tested network.

WhatsApp test

This test is designed to examine the reachability of both WhatsApp's app and the WhatsApp web version within a network.

OONI's WhatsApp test attempts to perform an HTTP GET request, TCP connection and DNS lookup to WhatsApp's endpoints, registration service and web version over the vantage point of the user. Based on this methodology, WhatsApp's *app* is likely blocked if any of the following apply:

- TCP connections to WhatsApp's endpoints fail;
- TCP connections to WhatsApp's registration service fail;
- DNS lookups resolve to IP addresses that are *not* allocated to WhatsApp;
- HTTP requests to WhatsApp's registration service do *not* send back a response to OONI's servers.

WhatsApp's web interface (web.whatsapp.com) is likely if any of the following apply:

- TCP connections to web.whatsapp.com fail;
- DNS lookups illustrate that a different IP address has been allocated to web.whatsapp.com;
- HTTP requests to web.whatsapp.com do *not* send back a consistent response to OONI's servers.

Facebook Messenger test

This test is designed to examine the reachability of Facebook Messenger within a tested network.

OONI's Facebook Messenger test attempts to perform a TCP connection and DNS lookup to Facebook's endpoints over the vantage point of the user. Based on this methodology, Facebook Messenger is likely blocked if one or both of the following apply:

- TCP connections to Facebook's endpoints fail;
- DNS lookups to domains associated to Facebook do *not* resolve to IP addresses allocated to Facebook.

Data analysis

Through its data pipeline, OONI processes all network measurements that it collects, including the following types of data:

Country code

OONI by default collects the code which corresponds to the country from which the user is running OONI Probe tests from, by automatically searching for it based on the user's IP address through the MaxMind GeoIP database. The collection of country codes is an important part of OONI's research, as it enables OONI to map out global network measurements and to identify where network interferences take place.

Autonomous System Number (ASN)

OONI by default collects the Autonomous System Number (ASN) which corresponds to the network that a user is running OONI Probe tests from. The collection of the ASN is useful to OONI's research because it reveals the specific network provider (such as Vodafone) of a user. Such information can increase transparency in regards to which network providers are implementing censorship or other forms of network interference.

Date and time of measurements

OONI by default collects the time and date of when tests were run. This information helps OONI evaluate when network interferences occur and to compare them across time.

IP addresses and other information

OONI does *not* deliberately collect or store users' IP addresses. In fact, OONI takes measures to remove users' IP addresses from the collected measurements, to protect its users from potential risks.

However, OONI might *unintentionally* collect users' IP addresses and other potentially personally-identifiable information, if such information is included in the HTTP headers or other metadata of measurements. This, for example, 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.

OONI processes the above types of data with the aim of deriving meaning from the collected measurements and, specifically, in an attempt to answer the following types of questions:

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

- How did network interference occur?

To answer such questions, OONI's pipeline is designed to process data which is automatically sent to OONI's measurement collector by default. The initial processing of network measurements enables 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" (such as Blue Coat) within tested networks.

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

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

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

OONI's methodology for detecting the presence of "middle boxes" - systems that could be responsible for censorship, surveillance and traffic manipulation - can also present false negatives, if ISPs are using highly sophisticated software that is specifically designed to *not* interfere with HTTP headers when it receives them, or to *not* trigger error messages when receiving invalid HTTP request lines. It remains unclear though if such software is being used. Moreover, it's important to note that the presence of a middle box is not necessarily indicative of censorship or traffic manipulation, as such systems are often used in networks for caching purposes.

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

Findings

As part of this study, network measurements were collected through OONI Probe software tests performed across six local vantage points in Myanmar between 25th October 2016 to 28th February 2017.

Upon analysis of the collected data, no block pages were detected that could confirm cases of censorship. WhatsApp, Facebook Messenger, and the Tor network appeared to be accessible in all networks where tests were run. While OONI tests had *previously detected the presence of Blue Coat software* (some types of which can potentially be used for internet censorship and surveillance) in Myanmar in late 2012, the presence of Blue Coat was *not* detected as part of this study (and neither were any other middle boxes).

Certain sites, however, presented a high amount of network anomalies are part of our testing, indicating that connections to them might have been tampered with. The findings pertaining to these sites are summarized in the table below.

Sites	TCP/IP blocking	HTTP failure	HTTP diff	DNS blocking	Control failure	Not blocked
http://burma.usembassy.gov	0	9	0	0	32	0
http://realdoll.com	0	41	0	0	0	0
http://www.sportingbet.com	40	0	0	0	1	0
http://www.cidh.org	9	0	0	0	32	0
http://www.vibe.com	0	0	7	0	32	2

The values under the “Control failure” column in the table above pertain to measurements where we are unable to determine whether access to those sites was blocked or not, because the control request failed. It’s useful to cross-reference this information with whether connections to the site in question were confirmed to *not* be blocked. The fact that connections to vibe.com, for example, were *not* blocked twice indicates that the site is *least likely* to have been tampered with, in comparison to the other sites included in the table above. Access to realdoll.com, on the other hand, which presented HTTP failures every time it was tested is more likely to have been blocked. Similarly, gambling site sportingbet.com which presented signs of TCP/IP blocking almost every time it was tested is also likely to have been censored.

The website of the Organization of American States (OAS), which is responsible for the promotion and protection of human rights in America, presented signs of TCP/IP blocking. The testing of this site *also* presented signs of TCP/IP blocking in a previous OONI study on internet censorship in Zambia in October 2016. While this inevitably raises the question of whether such measurements are false positives, it’s worth noting that the failure rate from a control vantage point is less than 1%. The motivation behind the potential blocking of this site though remains unclear.

Finally, the testing of the site of the U.S. embassy in Myanmar presented signs of HTTP blocking, indicating that access to it may have been tampered with. The testing of multiple other sites also presented network anomalies, but those were ruled out as false positives based on our heuristics.

Acknowledgement of limitations

The findings of this study present various limitations and do not necessarily reflect a comprehensive view of internet censorship in Myanmar.

The first limitation is associated with the testing period. While OONI network measurements have been collected from Myanmar since 2012 and continue to be collected on the day of the publication of this report, this study only takes into account and analyzes network measurements that were collected between 25th October 2016 to 28th February 2017. This study is limited to this time frame because we aim to examine the most recent censorship events and because there was a significant increase in the collection of network measurements during this period, in comparison to previous months and years. As such, censorship events which may have occurred before and/or after the testing period are not examined as part of this study.

Another limitation to this study is associated to the amount and types of URLs that were tested for censorship. As mentioned in the methodology section of this report ("Review of the Citizen Lab's test list for Myanmar"), OONI's Web Connectivity test was run to examine the accessibility of 822 URLs that are more relevant to the Myanmar context and of 1,105 internationally relevant sites. While a total of 1,927 URLs were tested for censorship as part of this study, we did not test all of the URLs on the internet, indicating the possibility that other websites not included in tests lists might have been blocked.

Finally, while network measurements were collected from *six* different local vantage points in Myanmar, OONI's software tests were not run consistently across all networks. Stable measurements were collected from certain vantage points throughout the testing period, but less stable measurements were also collected from a number of other vantage points following the launch of OONI's mobile app on 9th February 2017. In other words, once OONI Probe became easier to install and run via its mobile version for Android and iOS, we received an increased amount of sporadic measurements from various new networks. Since tests were not always run consistently, our ability to evaluate whether censorship cases were persistent was limited.

Conclusion

Signs of TCP/IP and HTTP blocking pertaining to fives sites, including the sites of the U.S. embassy in Myanmar and of the Organization of American States (OAS), were detected as part of this study. It remains unclear though why those sites might be blocked. Overall, 1,927 URLs were tested for censorship. No block pages were detected that could confirm cases of internet censorship.

Similarly, no middle boxes were detected as part of this study. Blue Coat software (some types of which can potentially be used for internet censorship and surveillance) was detected in Myanmar by OONI in late 2012. It's unclear, however, if this was a countrywide deployment or if it was only used in the specific network that was tested. Two years later, the presence of Blue Coat software was not detected in the same network, indicating that it may have been removed. Our recent study, covering the same network plus five additional networks, does *not* show the presence of Blue Coat software in tested networks.

WhatsApp, Facebook Messenger, and the Tor network appeared to be accessible across all six networks in Myanmar where OONI tests were run.

Acknowledgements

We thank the Open Technology Fund (OTF) and Access Now for funding this research. We also thank all the anonymous volunteers in Myanmar who have run and continue to run OONI Probe, thus making this research possible.

Global community measuring internet censorship around the world.

About

OONI

Data Policy

Data License

Contact

OONI Probe

Install

Tests

Source code

API

Updates

Blog

Mailing list

Slack