Myanmar: Data on internet blocks and internet outages following military coup

Maria Xynou (OONI), Ramakrishna Padmanabhan (CAIDA, UC San Diego), Phyu Kyaw, Myanmar ICT for Development Organization (MIDO), Arturo Filastò (OONI),
2021-03-09

On 1st February 2021, the military in Myanmar carried out a coup d'etat, seizing power and detaining the country's State Counsellor (equivalent to a prime minister) and other democratically elected leaders.

A few days after the coup, ISPs in Myanmar started blocking access to Facebook services. On 5th February 2021, they started blocking access to Twitter and Instagram as well. On 6th February 2021, access to the internet was shut down entirely for nearly 30 hours. When internet connectivity was restored, social media blocks remained in place and they are currently ongoing. Since 15th February 2021, access to the internet has been shut down every night (between around 1am to 9am local time) in Myanmar. More recently, some ISPs in Myanmar appear to have started blocking access to Wikipedia as well.

In this report, we share OONI data on the blocking of social media, Wikipedia, and circumvention tool sites in Myanmar following the military coup. To demonstrate the internet outages that Myanmar experienced every night over the past weeks, we share IODA data (and other public data sources monitoring internet traffic).

Background

In November 2020, the National League for Democracy (NLD) party won the majority in Myanmar's 2020 general election. The NLD governed Myanmar since winning the 2015 general election, with Aung San Suu Kyi serving as the country's State Counsellor (equivalent to a prime minister). Aung San Suu Kyi was once seen as a beacon for human rights, having won the Nobel Peace Prize in 1991 amid 15 years in detention for her pro-democracy struggle. But her inaction in response to the genocide of the Muslim Rohingya people in Rakhine State (which started in October 2016) and her refusal to acknowledge that Myanmar's military had committed masacres drew international criticism.

Observers questioned the credibility of the November 2020 election because of the disenfranchisement of the Rohingya, particularly since Myanmar's electoral commission cancelled voting in large parts of Rakhine State and other conflict-hit states. Nonetheless, the NLD reported that the latest election was a "landslide" victory and announced that it would be inviting ethnic minority parties to work with it.

However, the military-backed opposition disputed the election results, accusing the government of irregularities, and demanding a rerun of the election. The country's Union Election Commission determined that the election was done "fairly and free", and that there would *not* be an election re-run.

In response, military leaders in Myanmar seized power in a coup on 1st February 2021, detaining Aung San Suu Kyi and other elected leaders. A night-time curfew has been imposed by the military, and a one-year state of emergency has been declared. Following the coup, the military instructed local Internet Service Providers (ISPs) to block access to social media services, and to shut down the internet every night (starting from around 1am local time on 15th February 2021). They have also amended the Electronic Transactions Law, making the spread of "fake news or disinformation" online punishable by up to 3 years in prison. The amended Electronic Transactions Law also includes provisions that the military initially tried to introduce in a new cybersecurity bill drafted shortly after it seized power (but that bill was rejected by stakeholders in Myanmar). These amendments reportedly raise concerns with respect to media freedom, access to information, and online freedom of expression in Myanmar.

Methods

To investigate the blocking of online platforms, we analyzed OONI measurements collected from Myanmar (similarly to our previous studies in 2020 and 2017). OONI measurements are regularly collected and contributed by users of the OONI Probe app, which is free and open source, designed to measure various forms of internet censorship and network interference.

More specifically, we limited our analysis to OONI measurements collected from Myanmar between **1st February 2021 to 25th February 2021** in order to examine how internet censorship has changed in the country following the military coup. We further limited our analysis to OONI measurements pertaining to the testing of social media websites and apps, as well as to the testing of `www.wikipedia.org`, circumvention tool websites, news media websites (which we reported to be blocked last year),

`www.justiceformyanmar.org` and `coronavirus.app` (which we found blocked as part of recent OONI data analysis).

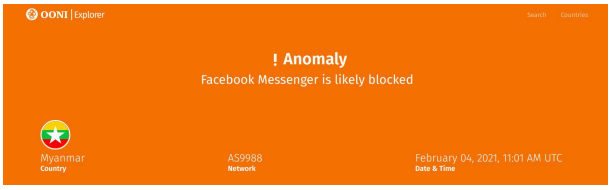
While a wide range of websites can be tested through OONI's Web Connectivity test (designed to measure the TCP/IP, DNS, and HTTP blocking of websites), the OONI Probe app currently only includes tests for the following social media apps: WhatsApp, Facebook Messenger, and Telegram. Our analysis was therefore limited to the testing of these specific apps.

Our findings are also limited by the type and volume of measurements contributed by volunteer OONI Probe users in Myanmar (i.e. if a blocked service was not tested in Myanmar in the analysis period, relevant measurement findings will not be available).

To explore the internet outages (i.e. when access to the internet was shut down entirely) in Myanmar, we referred to the following public data sources: Internet Outage Detection and Analysis (IODA), Oracle's Internet Intelligence Map, and Google traffic data. Our goal was to check whether the signals and timing of the internet outages in Myanmar can be verified and corroborated by all three separate public data sources.

Findings

Blocking of social media

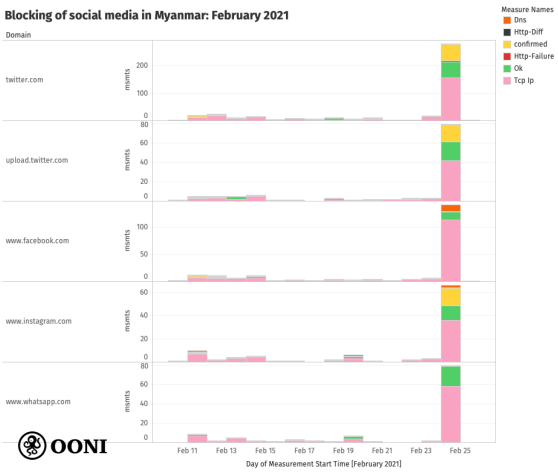


Merely three days after the military coup, ISPs in Myanmar started blocking access to Facebook services.

On 4th February 2021, OONI data showed that access to facebook.com, Facebook Messenger, and WhatsApp was blocked on several networks in Myanmar. This was also disclosed by Telenor, who shared that they received a directive from Myanmar's Ministry of Transport and Communications on 3rd February 2021 to temporarily block Facebook. This directive was reportedly motivated by concerns over the spread of misinformation on Facebook. Quite similarly, Facebook reportedly restricted the distribution of content by profiles and accounts run by Myanmar's military in an attempt to limit the spread of misinformation. While it was initially reported that Facebook would remain blocked until 7th February 2021, OONI data shows that access to Facebook services remains blocked on several networks in Myanmar.

On 5th February 2021, ISPs in Myanmar appear to have started blocking access to Twitter as well. Many OONI measurements collected thereafter suggest the ongoing blocking of `twitter.com` on several networks in Myanmar. OONI measurements also suggest the blocking of `www.instagram.com` from 10th February 2021 onwards (though it's possible that the blocking may have started earlier, as very few measurements testing `www.instagram.com` are available from the previous days).

The following chart illustrates the blocking of social media in Myanmar in February 2021 (following the military coup) based on OONI data.



Source: OONI measurements collected from Myanmar between 1st February 2021 to 25th February 2021, https://explorer.ooni.org/search?since=2021-02-01&probe_cc=MM&until=2021-02-25

The above chart aggregates the OONI Probe measurement coverage that each social media domain received (across networks in Myanmar) between 1st February 2021 to 25th February 2021. The measurements are colour-coded based on the Web Connectivity test results; it is evident that most measurements presented TCP/IP anomalies, suggesting the IP blocking of Twitter, Facebook, WhatsApp, and Instagram on most tested networks in Myanmar.

In some cases though (on the following 6 networks: AS58952, AS133385, AS136255, AS63852, AS18399, AS136783), we see these social media sites blocked in different ways. Measurements that are annotated as `confirmed` in the above chart pertain to cases where we were able to *automatically confirm* blocking based on the detection of block pages. We were able to confirm blocking because OONI network measurement data shows that those ISPs implemented DNS based interference which returned IP addresses (59.153.90.11, 167.172.4.60) that host block pages, such as the following:

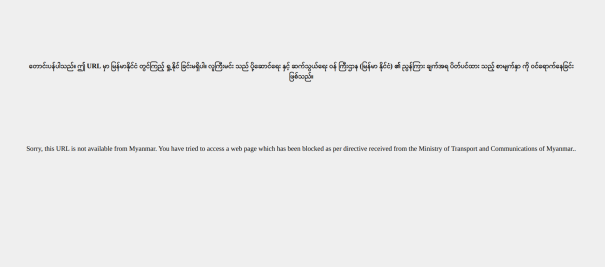


Image: Block page served in Myanmar.

It's worth noting though that the same ISPs which served block pages through DNS based interference were also found to implement IP based blocking as well. In other words, OONI data shows that ISPs in Myanmar adopt a mixture of censorship techniques – in some cases serving block pages, while in other cases implementing what looks like IP based blocking. More details are available through our analysis.

Overall, from the above chart on social media blocking in Myanmar, we see that:

- There was a significant increase in OONI Probe measurement coverage towards the end of the analysis period;
- Most measurements present TCP/IP level interference, suggesting IP based blocking on most networks;
- Some ISPs blocked a few of these sites by means of DNS interference, returning IP addresses that host block pages

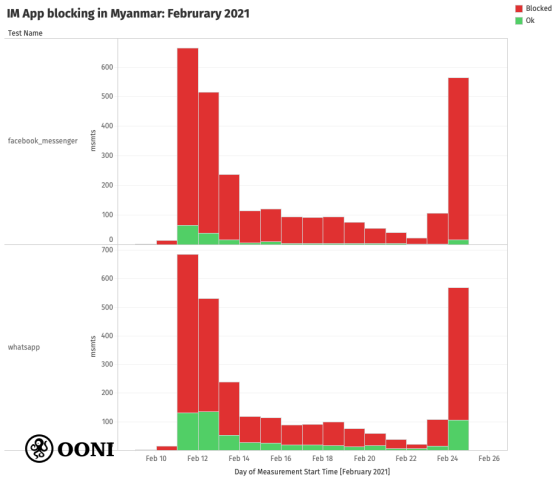
(59.153.90.11, 167.172.4.60) or an address in private IP space (such as 127.0.0.1 or 172.29.8.1);

- Some measurements were successful (i.e. the tested websites were found accessible), showing that the blocks are not implemented deterministically over time on all networks.

While OONI measurements show that Telegram has been reachable in Myanmar, both WhatsApp and Facebook Messenger presented signs of blocking during their testing throughout February 2021. Similarly to the testing of social media websites, we observe both DNS based tampering and IP blocking of WhatsApp and Facebook, which varies from network to network (and in some cases, we observe ISPs adopting a mixture of censorship techniques).

In the testing of Facebook Messenger, there are cases where all attempted TCP connections to Facebook's endpoints failed, and there are other cases where DNS lookups to domains associated with Facebook do not resolve to IP addresses allocated to Facebook. In the testing of WhatsApp, we observe interference with WhatsApp web (`web.whatsapp.com`) and WhatsApp's registration service, though attempted connections to WhatsApp's endpoints are often successful (this is observed on several networks).

The following chart illustrates the testing of WhatsApp and Facebook Messenger (across networks) in Myanmar throughout February 2021, based on OONI data.



Source: OONI measurements collected from Myanmar throughout February 2021, https://explorer.ooni.org/search?until=2021-02-28&since=2021-02-01&probe_cc=MM

As is evident from the above chart, WhatsApp and Facebook Messenger presented signs of blocking most times that they were tested in Myanmar throughout February 2021. The high volume of anomalous measurements (across many different networks) provides a strong signal of blocking, particularly since this is not observed in past measurements (before February 2021). It's worth noting though that some measurements (collected in February 2021) were successful (i.e. the tested apps were reachable), suggesting that the blocks are not deterministic across networks in Myanmar.

Today, OONI data suggests the ongoing blocking of Facebook, Facebook Messenger, WhatsApp, Twitter, and Instagram in Myanmar.

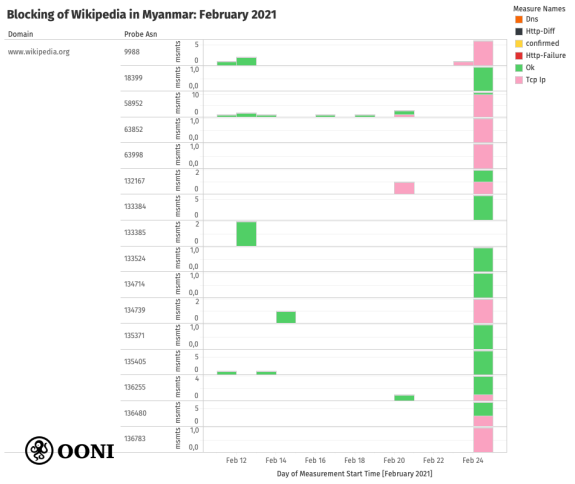
Blocking of Wikipedia

Starting from 20th February 2021, we started to observe the blocking of Wikipedia in Myanmar as well (though the first

measurement that presented signs of IP based blocking of `www.wikipedia.org` was collected on 18th February 2021).

In all anomalous measurements collected thereafter on the testing of `www.wikipedia.org` on several different networks in Myanmar, we consistently observe that attempted TCP connections to the IP address allocated to `www.wikipedia.org` failed, suggesting IP based blocking. This censorship technique would also affect Wikipedia subdomains, which is why we see other Wikipedia language editions (such as `ar.wikipedia.org`) presenting the same signs of IP blocking.

It's worth highlighting though that `www.wikipedia.org` does *not* appear to be blocked on all networks in Myanmar. The following chart aggregates OONI measurements from the testing of `www.wikipedia.org` on multiple networks in Myanmar, illustrating that while `www.wikipedia.org` presents signs of IP blocking (primarily from 20th February 2021 onwards) on some networks, it's accessible on others.

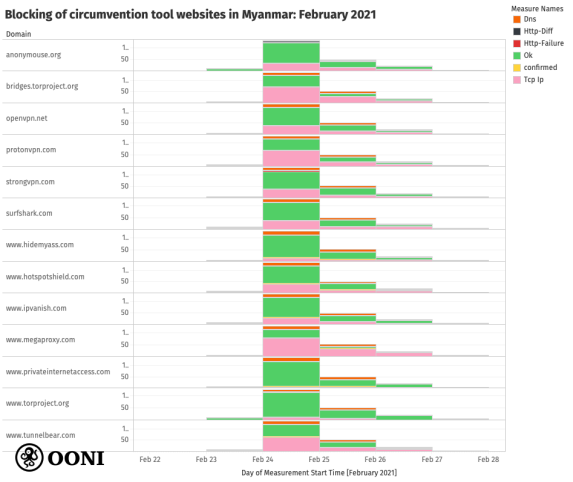


Source: OONI measurements collected from Myanmar testing `www.wikipedia.org` between 1st February 2021 to 25th February 2021, https://explorer.ooni.org/search?since=2021-02-01&probe_cc=MM&test_name=web_connectivity&domain=www.wikipedia.org

The blocking of `www.wikipedia.org` does not appear to be deterministic either. For example, when looking at recent measurements collected from AS136480 (UniLink Myanmar), it is evident that some measurements collected on 24th February 2021 successfully established a TCP connection to Wikipedia's IP address, while other measurements (collected on the same day on the same network) suggest that Wikipedia's IP was blocked. We observe the same non-deterministic pattern in the blocking of social media as well, as it is sometimes possible for connections to go through (even though IP blocks appear to be in place).

Blocking of circumvention tool sites

Circumventing internet censorship over the last month might have been quite challenging in Myanmar, given that a number of censorship circumvention tools appear to have been blocked. In February 2021, a list of VPNs and their associated IP addresses (that ISPs in Myanmar were reportedly required to block access to) circulated on Facebook. The websites of some of these VPNs (such as `protonvpn.com` and `www.tunnelbear.com`) were found blocked in our recent OONI data analysis, as illustrated in the chart below.



Source: OONI measurements collected from Myanmar between 1st February 2021 to 28th February 2021, https://explorer.ooni.org/search?since=2021-02-01&probe_cc=MM&until=2021-02-28

All of the circumvention tool websites listed in the above chart were confirmed blocked at least once, as OONI measurements show DNS based interference returning IP addresses that host block pages (59.153.90.11, 167.172.4.60) or an address in private IP space (such as 127.0.0.1 or 172.29.8.1).

Most anomalous measurements though show IP blocking, which is not only consistent with what we observe in the blocking of social media and Wikipedia, but which also matches reports regarding the IP blocking of circumvention tools. It's worth highlighting though that these circumvention tool sites are *not* blocked on all networks in Myanmar (as illustrated in the above chart), and that the blocking of certain circumvention tool websites does not necessarily mean that the relevant apps are blocked as well (particularly since circumvention tools often rely on a variety of techniques for evading censors).

For example, even though the testing of `www.torproject.org` presented signs of IP blocking on several networks (such as AS18399 and AS135405), the testing of Tor shows that it was reachable on multiple networks (including AS18399 and AS135405) in Myanmar over the last month. As most Tor directory authorities and bridges were reachable when tested from local networks in Myanmar, it was likely possible to use Tor for censorship circumvention.

OONI Probe currently only includes tests for measuring the reachability of the following circumvention tools: Tor, Psiphon, and RiseupVPN. We are therefore unable to evaluate whether the apps of the other circumvention tool websites (listed in the above chart) were blocked in Myanmar as well.

Other ongoing blocks

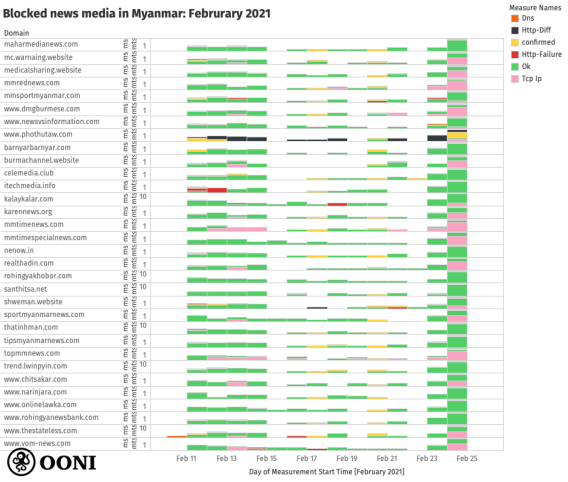
Apart from the recent blocking of social media and Wikipedia (following the recent military coup in Myanmar), we also observe the ongoing blocking of a number of news media websites and of the site of Justice for Myanmar (`justiceformyanmar.org`), the blocking of which started in 2020. As part of our recent OONI data analysis, we found a COVID-19 site (`coronavirus.app`) blocked in Myanmar as well.

News media

Last year, we reported the **DNS based blocking of 174 domains** in Myanmar (following a March 2020 directive issued by Myanmar's Ministry of Transport and Communications), which include 41 news outlets. While they include a few ethnic media websites reporting on the situation in Rakhine, they also include websites

which are not considered credible (as pointed out to us by civil society groups in Myanmar).

Recent OONI measurements show that these news websites currently remain blocked on several networks in Myanmar, as illustrated through the following chart.



Source: OONI measurements collected from Myanmar between 1st February 2021 to 25th February 2021, https://explorer.ooni.org/search?since=2021-02-01&probe_cc=MM&until=2021-02-28&only=anomalies&test_name=web_connectivity

It is evident through the above chart (which aggregates measurements across networks) that the (ongoing) blocking of news media websites in Myanmar varies from network to network, and that different censorship techniques are adopted.

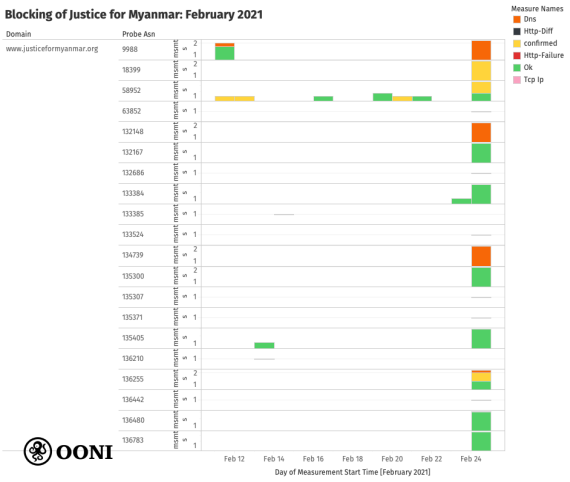
In some cases, we observe DNS based interference which returns IP addresses that host block pages, enabling us to automatically confirm blocking. In other cases, we observe IP based blocking (which we more commonly see in more recent measurements), while some measurements are successful. These censorship patterns are consistent with what we observe in the blocking of social media and Wikipedia, as discussed previously. Further details are available through our analysis (which also provides relevant OONI measurements).

Justice for Myanmar

In August 2020, Telenor Myanmar disclosed that the Myanmar government had issued another directive instructing ISPs to block the website of Justice for Myanmar and 3 associated IP addresses.

Justice for Myanmar is an activist campaign which aims to pressure businesses and investors around the world to divest from Myanmar military businesses. They argue that more than 150 international and domestic companies are engaged with military-owned companies in Myanmar, supporting brutal oppression in the country. Their campaign aims to expose international businesses with ties to Myanmar's military and pressure them to divest.

Their work is even more timely and urgent now that Myanmar is run by the military. However, access to their website remains blocked on several networks in Myanmar, as illustrated through the following chart.



Source: OONI measurements collected from Myanmar between 1st February 2021 to 25th February 2021, https://explorer.ooni.org/search?since=2021-02-01&probe_cc=MM&until=2021-02-28&test_name=web_connectivity&domain=www.justiceformyanmar.org

We were able to confirm the blocking of `www.justiceformyanmar.org` on MyTel (AS136255), Frontiir (AS58952), and Yatanarpon Teleport (AS18399) where we observe DNS based interference returning an IP address (`59.153.90.11`) that hosts a block page or an address in private IP space (`127.0.0.1`). It's worth noting though that the site appears to be accessible on many other networks.

In their statement, Telenor Myanmar highlighted that while authorities in Myanmar have legal basis to order such directives, the practice appears to be incompatible with international human rights law. And so while Telenor Myanmar were required to comply with this directive and block access to `www.justiceformyanmar.org`, they reportedly raised concerns regarding international human rights and the collateral damage that may inadvertently occur from the blocking of IP addresses.

Campaigners from Justice for Myanmar reportedly argued that the February 2021 military coup was not just about preserving Min Aung Hlaing's political influence (who has served as the commander-in-chief of Defense Services since 2011, and who now serves as the country's de facto leader), but also his wealth. Businesses owned by Min Aung Hlaing's children have reportedly profited from access to state resources during his tenure.

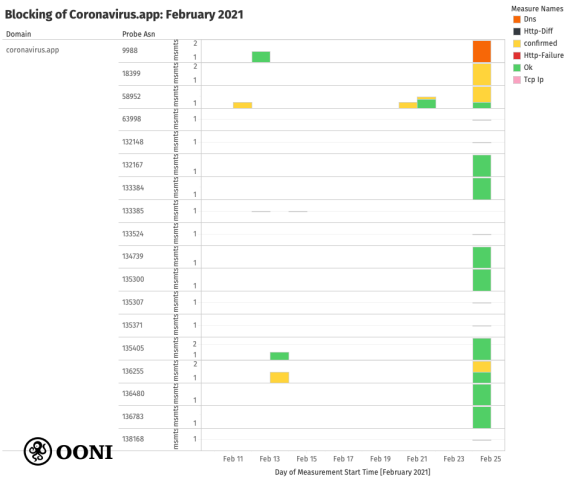
According to Justice for Myanmar:

"If democratization progresses and there is accountability for his criminal conduct, he and his family stand to lose their revenue streams."

COVID-19 site

While analyzing OONI data for this report, we came across the blocking of a COVID-19 site (`coronavirus.app`) as well. This site ("The Coronavirus App") tracks the spread of the ongoing COVID-19 pandemic worldwide, providing users with an interactive map that allows them to view fatality rate and recoveries, and check affected regions in real-time.

The following chart aggregates OONI Probe measurement coverage on the testing of `coronavirus.app` on multiple networks in Myanmar between 1st February 2021 to 25th February 2021.



Source: OONI measurements collected from Myanmar between 1st February 2021 to 25th February 2021, https://explorer.ooni.org/search?since=2021-02-01&probe_cc=MM&until=2021-02-28&test_name=web_connectivity&domain=coronavirus.app

While `coronavirus.app` is accessible on many networks in Myanmar, OONI data shows that it is blocked on at least 3 networks (AS136255, AS58952, AS18399) where we were able to automatically confirm blocking. On these networks, we observe DNS based interference, returning an IP address (`59.153.90.11`) that hosts a block page or an address in private IP space (`127.0.0.1`).

Note: While some of these measurements include an `error` annotation in the OONI Explorer measurement headers, that is due to the fact that the blockpage server was not reachable in the moment that the test was performed (possibly because the blockpage server was offline). We are nonetheless able to fingerprint the blocking because these IP addresses (59.153.90.11, 167.172.4.60) used to host block pages, as documented in our previous study last year. The return of an IP address in private IP space (such as 127.0.0.1 or 172.29.8.1) is consistent with the blocking pattern we observed for other websites.

Internet outages

Since the military coup on 1st February 2021, Myanmar has experienced multiple significant internet outages. These outages are visible through several public data sources: Internet Outage Detection and Analysis (IODA), Oracle's Internet Intelligence Map, and Google traffic data.

The Internet Outage Detection and Analysis (IODA) project of the Center for Applied Internet Data Analysis (CAIDA) measures internet outages worldwide in near real-time. To track and identify internet outages, IODA uses three complementary measurement and inference methods: Routing (BGP) announcements, Active Probing, and Internet Background Radiation (IBR) traffic. Access to IODA measurements is openly available through their Dashboard, which enables users to explore internet outages with country, region, and AS level of granularity.

Outage on 1st February 2021

IODA detected an initial drop in connectivity at around 21:00 UTC on 31st January 2021, followed by a larger drop at around 00:20 UTC on 1st February 2021, as illustrated below. Both of these drops are visible in IODA's Active Probing and BGP signals.

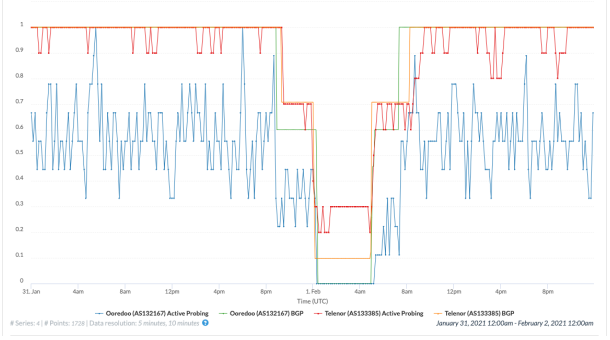
Source: Internet Outage Detection and Analysis (IODA), IODA Signals for Myanmar, https://ioda.caida.org/ioda/dashboard#view=inspect&entity=country/MM&lastView=overview&from=1612051200&

IODA provides data at network-level granularity (in addition to country-level and region-level), enabling us to examine which networks were affected and to what extent. Analyzing network-level data also allows us to uncover outage timing patterns and differences.

This was the first major Internet outage that occurred amid the coup; for this particular outage, we observed significant differences in the extent to which various networks were affected and we also observed timing differences. Some networks experienced almost complete loss of Internet connectivity while others appear to have experienced only small outages. For networks that did experience an outage, there were still timing differences: in some, the outage began at 21:00 (UTC) on 31st January 2021, while on other networks, the outage began only after midnight on 1st February 2021. The graphs below highlight these differences.

Source: Internet Outage Detection and Analysis (IODA), Active Probing and BGP Signals for MPT (AS9988) and Mytel (AS136255). These networks observe steep drops in the BGP signal just after midnight (UTC) on 1st February 2021.
https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/9988&lastView=overview&from=1612051200&unti

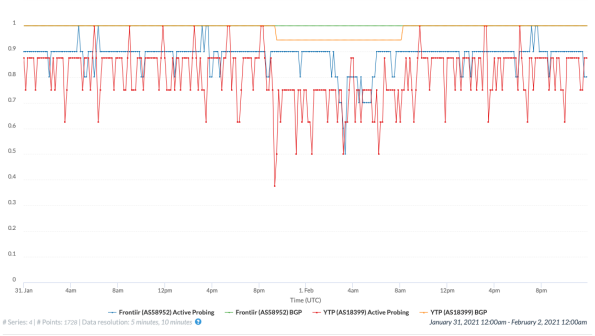
https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/136255&lastView=overview&from=1612051200&u



Source: Internet Outage Detection and Analysis (IODA), Active Probing and BGP Signals for Ooredoo (AS132167) and Telenor (AS133385). These networks first observe drops in the signals at ~ 21:00 (UTC) on 31st January 2021. The signals drop further after midnight (UTC) on 1st February 2021.

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/132167&lastView=overview&from=1612051200&u

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/133385&lastView=overview&from=1612051200&u



Source: Internet Outage Detection and Analysis (IODA), Active Probing and BGP Signals for Frontiir (AS58952) and YTP (AS18399). These networks observe relatively small drops in Internet connectivity according to IODA's signals.

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/18399&lastView=overview&from=1612051200&un

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/58952&lastView=overview&from=1612051200&un

While this outage resulted in significant drops in connectivity across many ASes, the next ones were even more severe.

Outage on 6th February 2021

Myanmar experienced a second (higher impact) internet outage on 6th February 2021. IODA data from the following chart (taken from the IODA dashboard) clearly shows that Myanmar experienced an internet outage, starting from around 02:00 UTC on 6th February 2021 and lasting up until around 08:00 UTC on 7th February 2021.

Source: Internet Outage Detection and Analysis (IODA), IODA Signals for Myanmar, https://ioda.caida.org/ioda/dashboard#view=inspect&entity=country/MM&lastView=overview&from=1612310400&

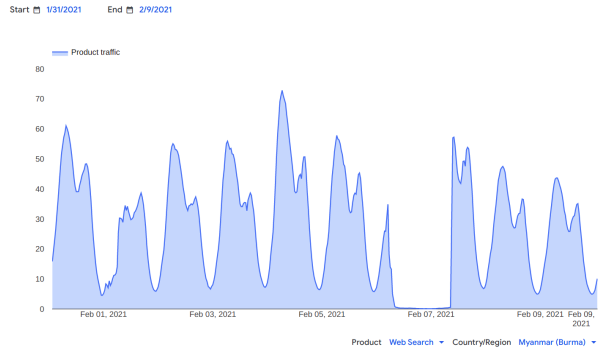
Within this time period, we observe a major drop in both active probing and IBR signals, and also a drop in the BGP signal correlating in time with the drop in the other signals, strongly suggesting that Myanmar experienced a widespread internet outage. This is further indicated by the fact that we see these signals resume to their previous levels thereafter.

Quite similarly, Oracle's Internet Intelligence Map tracks internet disruptions worldwide based on three signals: Traceroute completion ratio, BGP routes, and DNS query rate. On 6th February 2021, Oracle's Internet Intelligence Map records the same internet outage in Myanmar as IODA data (with almost identical timings in the drop of signals). We also observe the same drop in connectivity on 1st February 2021, as previously seen in IODA data.

Source: Oracle Internet Intelligence Map, Myanmar (February 2021), https://map.internetintel.oracle.com/?

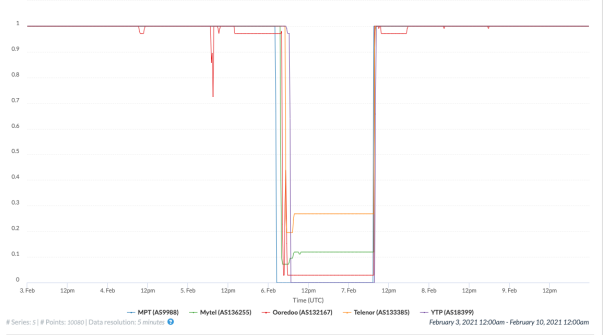
root=national&country=MM

Myanmar's internet outage (on 6th February 2021) is further corroborated by Google traffic data, which very visibly shows that almost no Google traffic originated from Myanmar during the same time period.



Source: Google Transparency Report, Traffic and disruptions to Google: Myanmar (February 2021), https://transparencyreport.google.com/traffic/overview?hl=en&fraction_traffic=start:1612051200000;end:1612915199999;product:19;region:MM&lu=fraction_traffic

Investigating IODA's network-level signals for the outage that began on 6th February 2021, we observe fewer timing differences among major networks compared to the first outage that occurred amid the coup on 1st February 2021. The end-times of the outage, in particular, are nearly identical across most major networks. This level of synchronization suggests that networks were able to plan and execute the enforcement and relaxation of this shutdown.



Source: Internet Outage Detection and Analysis (IODA), BGP Signals for MPT (AS9988), Mytel (AS136255), Ooredoo (AS132167), Telenor (AS133385), and YTP (AS18399). While the outage begins at slightly different times, Internet connectivity appears to be restored almost simultaneously across these networks.

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/9988&lastView=overview&from=1612310400&unti

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/136255&lastView=overview&from=1612310400&u

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/132167&lastView=overview&from=1612310400&u

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/133385&lastView=overview&from=1612310400&u

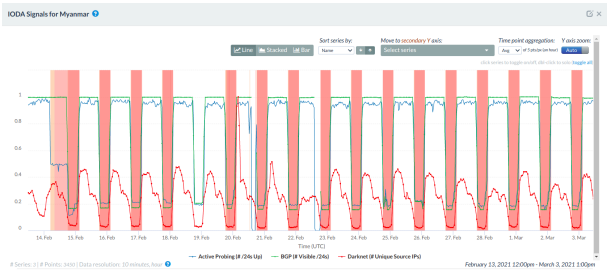
https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/18399&lastView=overview&from=1612310400&un

Ongoing nightly outages

Starting from 15th February 2021, Myanmar began to experience internet outages every night.

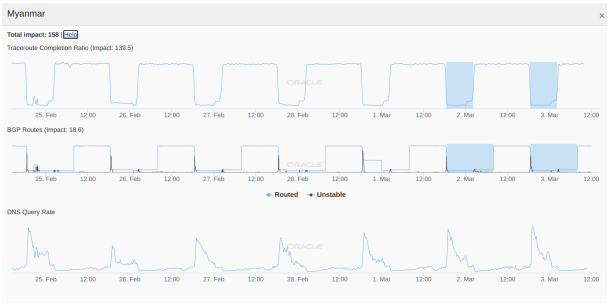
Like clockwork, access to the internet has been shut down completely on a national level every night (for around 8 hours) between 01:00 to 09:00 local time (which corresponds to 18:30 UTC to 02:30 UTC). And the nightly internet curfews in Myanmar appear to be ongoing.

This is evident through IODA data, which shows that all signals consistently drop between 01:00 to 09:00 local time every night from 15th February 2021 onwards.



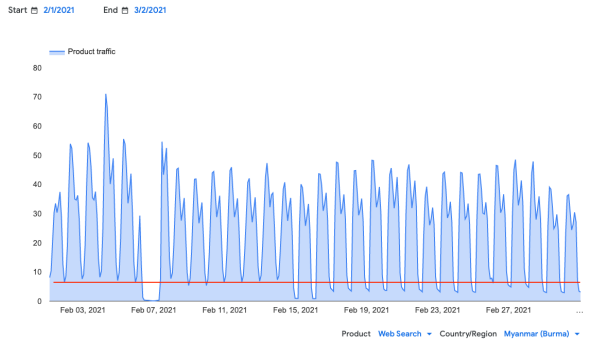
Source: Internet Outage Detection and Analysis (IODA), IODA Signals for Myanmar, https://ioda.caida.org/ioda/dashboard#view=inspect&entity=country/MM&lastView=overview&from=1613217600&

The nightly internet outages in Myanmar are also visible through Oracle's Internet Intelligence Map, which shows the same timings in the drop of signals as IODA data.



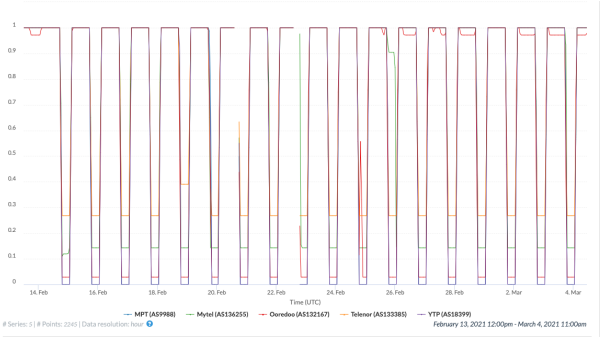
Source: Oracle Internet Intelligence Map, Myanmar (February 2021), https://map.internetintel.oracle.com/?root=national&country=MM

Myanmar's nightly internet outages are further suggested by Google traffic data, which shows a drop in Google traffic from 15th February 2021 onwards (in comparison to previous dates), quite similarly to IODA and Oracle Internet Intelligence data.



Source: Google Transparency Report, Traffic and disruptions to Google: Myanmar (February 2021), https://transparencyreport.google.com/traffic/overview?hl=en&fraction_traffic=start:1612137600000;end:1614729599999;product:19;region:MM&lu=fraction_traffic

When investigating IODA's network-level signals, we observe that most major networks in Myanmar now experience highly synchronized outages, that each begin at 18:30 UTC and end at 02:30 UTC. This synchronization is in stark contrast to the first Internet outage that occurred during the coup on 1st February 2021; in the time since, it appears that ISPs have developed and honed techniques to enforce and relax Internet connectivity shutdowns according to pre-planned schedules.



Source: Internet Outage Detection and Analysis (IODA), BGP Signals for MPT (AS9988), Mytel (AS136255), Ooredoo (AS132167), Telenor (AS133385), and YTP (AS18399). The nightly Internet outages begin at 18:30 UTC and end at 02:30 UTC for all these networks, suggesting high levels of coordination and automation.

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/9988&lastView=overview&from=1613217600&unti

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/136255&lastView=overview&from=1613217600&u

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/132167&lastView=overview&from=1613217600&u

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/133385&lastView=overview&from=1613217600&u

https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/18399&lastView=overview&from=1613217600&un

All of these data sources on the nightly internet outages corroborate what locals in Myanmar have been reporting, as well as what has already been reported quite extensively by the international media.

Conclusion

As the political environment in Myanmar changed (following the military coup on 1st February 2021), internet controls in the country increased.

Last year, multiple websites (including a few ethnic media websites reporting on the situation in Rakhine) were blocked, and their blocking appears to be ongoing. We also observe the ongoing blocking of `www.justiceformyanmar.org` (an activist campaign which aims to pressure businesses and investors around the world to divest from Myanmar military businesses), and we recently detected the blocking of COVID-19 site (`coronavirus.app`) as well.

But following the February 2021 military coup, the scale of internet censorship in Myanmar has become quite unprecedented.

In summary, we now see:

- **Social media blocks.** Access to Facebook, Facebook Messenger, WhatsApp, Instagram, and Twitter appears to be blocked on multiple networks in Myanmar since early February 2021.
- **Wikipedia block.** Access to `www.wikipedia.org` appears to have been blocked on several networks in Myanmar (primarily seen from 20th February 2021 onwards).
- **Circumvention tool sites blocked.** Access to several circumvention tool websites (such as `protonvpn.com` and `www.tunnelbear.com`) appears to have been blocked on some networks in Myanmar in February 2021.
- **Nightly internet outages.** The first internet disruption was observed in the early hours of 1st February 2021 (on the day of the military coup), followed by a second, higher impact internet outage on 6th February 2021 (which lasted for almost 30 hours). As of 15th February 2021, Myanmar

has been experiencing complete internet outages every night (between around 1am to 9am local time).

Through OONI data (on the blocking of Wikipedia and social media services), we observe the following:

- **Censorship variance across networks.** Internet censorship appears to vary across networks in Myanmar, as we observe different sites being blocked on different networks (and the blocks are not implemented on all networks).
- **Variance in censorship techniques.** ISPs in Myanmar are primarily seen to block sites and apps by means of IP blocking and/or DNS based interference.
    - **IP blocking.** In many cases, we observe the IP blocking of websites and apps across networks in Myanmar.
    - **DNS based interference.** In some cases, ISPs in Myanmar block sites by means of DNS based interference, returning IP addresses that host block pages (59.153.90.11, 167.172.4.60) or an address in private IP space (such as 127.0.0.1 or 172.29.8.1). We were able to automatically confirm these censorship cases.
- **Non-deterministic censorship.** Not all IP blocks appear to be effective. OONI data shows that it is sometimes possible for connections to go through (even though IP blocks appear to be in place), which is likely why we observe inconsistent measurements (in terms of accessibility and blocking).

The findings of this study suggest an **alarming shift in Myanmar's internet censorship landscape**. In our 2017 study (which examined internet censorship in Myanmar based on the analysis of all OONI measurements collected between 2016-2017), we barely found any internet censorship in the country. Now, the ongoing social media blocks and nightly internet outages raise major human rights concerns, particularly in light of the current political environment.

Acknowledgements

We thank OONI Probe users in Myanmar for contributing measurements, making this study possible.