



ARTICLE 19



## Unplugged in Myanmar

Internet restrictions following the military coup

9 July 2021

## ARTICLE 19

**E:** info@article19.org

**W:** www.article19.org

**Tw:** @article19org

**Fb:** facebook.com/article19org

First published by ARTICLE 19, 9 July 2021

Copyright ARTICLE 19, 2021 (Creative Commons License 3.0)

### © ARTICLE 19, 2021

ARTICLE 19 works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We do this by working on two interlocking freedoms, which set the foundation for all our work. The Freedom to Speak concerns everyone's right to express and disseminate opinions, ideas and information through any means, as well as to disagree from, and question power-holders. The Freedom to Know concerns the right to demand and receive information by power-holders for transparency good governance and sustainable development. When either of these freedoms comes under threat, by the failure of power-holders to adequately protect them, ARTICLE 19 speaks with one voice, through courts of law, through global and regional organisations, and through civil society wherever we are present.

About Creative Commons License 3.0: This work is provided under the Creative Commons Attribution-Non-Commercial-ShareAlike 2.5 license. You are free to copy, distribute and display this work and to make derivative works, provided you: 1) give credit to ARTICLE 19; 2) do not use this work for commercial purposes; 3) distribute any works derived from this publication under a license identical to this one. To access the full legal text of this license, please visit: <http://creativecommons.org/licenses/by-nc-sa/2.5/legalcode>.

## SUMMARY

On 1 February 2021, the Myanmar military seized power from the democratically elected government led by Aung San Suu Kyi's National League for Democracy (NLD). While quashing anti-military protests with unlawful force, enacting draconian legal changes, and arresting hundreds of anti-military activists, the military put in place severe internet restrictions that deny people in Myanmar the full enjoyment of their human rights.

In the months since the coup, the military has enacted increasingly sophisticated restrictions on internet access. In the immediate aftermath of the events of 1 February, the military often imposed blanket, but time-bound, restrictions on internet access. The military has recently moved to an approach of 'whitelisting', in which all mobile internet access is blocked save for pre-approved websites and applications. However, the degree to which this policy is being implemented is unclear, and internet users continue to be able to access a wide range of websites. By making internet access the exception rather than the norm, the government has violated the right to freedom of expression and access to information, which may only be restricted under limited conditions defined by international law.

While the internet restrictions themselves violate human rights, they have also exacerbated other human rights concerns in the country. Internet restrictions have hindered the organisation of anti-junta protests, obstructed efforts to assist individuals threatened by the junta, and restricted the flow of information about human rights abuses. The restrictions have also deepened the economic crisis brought on by the COVID-19 pandemic.

While imposing internet restrictions, the military enacted changes to Myanmar's Penal Code—many of which target expression, including online expression. New or amended crimes carry severe penalties for, among other things, expressing opinions critical of the government. Internet restrictions and the threat of criminal sanction have severely constricted the operating environment and forced many civil society organisations to limit their work or shut down entirely. Internet service providers (ISPs) have come under increased pressure to implement policies that would provide expansive surveillance powers to authorities.<sup>1</sup>

This briefing paper first explains internet restrictions that the NLD-led government put in place before the coup. It then sets out a timeline of the implementation of internet restrictions since 1 February. It further describes the domestic legal framework enabling the internet restrictions and the new changes to Myanmar law that have increased repression of the right to freedom of expression. This briefing paper concludes by providing recommendations to States, the UN, and private sector actors.

---

<sup>1</sup> Fanny Potkin, 'After pressuring telecom firms, Myanmar's junta bans executives from leaving', *Reuters*, 5 July 2021, available at: <https://www.reuters.com/world/asia-pacific/exclusive-after-pressuring-telecom-firms-myanmars-junta-bans-executives-leaving-2021-07-05/> and *Frontier Myanmar*, 'Junta steps up phone, internet surveillance – with help from MPT and Mytel', 5 July 2021, available at: <https://www.frontiermyanmar.net/en/junta-steps-up-phone-internet-surveillance-with-help-from-mpt-and-mytel/>.

## TABLE OF CONTENTS

Summary .....	3
Background: Pre-Coup Internet Restrictions .....	5
Internet Restrictions Post-Coup .....	7
Impact of Internet Restrictions.....	15
Domestic Legal Framework.....	17
International Law .....	20
Recommendations .....	24

## BACKGROUND: PRE-COUP INTERNET RESTRICTIONS

The efforts of Myanmar's military to suppress digital rights did not emerge in a vacuum. Rather, many of the Tatmadaw's actions have built on the policies and initiatives of the NLD-led government and prior governments. While the military has now gone much further than the NLD-led government ever did in suppressing dissent and restricting internet access, the military's abuses and human rights violations are a continuation of rights-abusing practices that began long before the 1 February coup.

### Internet shutdowns

The first major internet restrictions enacted by the NLD-led government lasted more than a year-and-a-half. On 20 June 2019, Myanmar's Ministry of Transport and Communications (MOTC) ordered mobile telecommunications operators to 'stop mobile internet traffic' in nine townships in Rakhine and Chin States due to 'disturbances of peace and use of internet services to coordinate illegal activities'.<sup>2</sup> The area affected by the internet shutdown was the site of armed conflict between the Myanmar military and the Arakan Army, an ethnic armed group. The military has committed grave human rights violations against Rakhine and Rohingya populations in the area. In making the order, the MOTC stated it was exercising authority granted by Section 77 of the Telecommunications Law. In September 2019, the MOTC lifted the ban in five of the townships, but on 3 February 2020, the ban was re-imposed in those townships.<sup>3</sup> In May 2020, the government lifted the shutdown in Rakhine State's Maungdaw Township but kept it in place in the other eight townships.<sup>4</sup>

In August 2020, the government of Myanmar restored 2G network access to all townships affected by the shutdown. Nevertheless, because 3G and 4G network access were still unavailable, internet speeds were reportedly so slow that mobile users were unable to load webpages or open applications.<sup>5</sup> On 3 February 2021, the MOTC lifted the restrictions imposed in Rakhine and Chin States, only to implement nationwide restrictions.<sup>6</sup>

The 19-month internet shutdown in Rakhine and Chin States exacerbated challenges caused by the COVID-19 pandemic. The NLD-led government used the internet to disseminate information about COVID-19 and official efforts to mitigate its effects. Government restrictions on mobile internet access prevented individuals from receiving health guidance, assessing risks, and learning what actions the government was taking to protect them. Due in part to the internet shutdown, humanitarian groups and local politicians in the region reported that, in the areas affected by the internet restrictions, many people

<sup>2</sup> Telenor, 'Network shutdown in Myanmar, 21 June 2019', 21 June 2019, available at: <https://www.telenor.com/network-shutdown-in-myanmar-21-june-2019/>.

<sup>3</sup> *Ibid.*

<sup>4</sup> See, ARTICLE 19, 'Myanmar: One year on, Internet shutdown imperils human rights in Myanmar', 19 June 2020, available at: <https://www.article19.org/resources/myanmar-one-year-on-internet-shutdown-imperils-human-rights-in-myanmar/>.

<sup>5</sup> Lei Lei, 'Myanmar Govt Restores internet in Rakhine, Locals Complain of Weak Signal', *Irrawaddy*, 5 August 2020, available at: <https://www.irrawaddy.com/news/burma/myanmar-govt-restores-internet-rakhine-locals-complain-weaksignal.html>; Four special rapporteurs on freedom of expression have stated that 'cutting off access to the internet, or parts of the internet, for whole populations or segments of the public (shutting down the internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the internet or parts of the internet'. UN Special Rapporteur on Freedom of Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and the Internet', 1 June 2011, para. 6(b), available at: <https://www.osce.org/fom/78309>.

<sup>6</sup> Telenor, 'Network restored in eight townships in Myanmar', 3 February 2021, available at: <https://www.telenor.com/network-restored-in-eight-townships-in-myanmar/>.

were not aware of the COVID-19 pandemic, let alone what actions they should take to best mitigate the risks it poses.<sup>7</sup>

## SIM card registration

Myanmar authorities also took action to expand the power of the state to monitor internet communications during the NLD's term. In February 2020, the MOTC launched an effort requiring the real-name registration of all SIM cards issued in the country. On 30 June 2020, the MOTC deactivated all SIM cards that remained unregistered. According to an MOTC official, more than 34 million SIM cards were deactivated.<sup>8</sup> To register their SIMs, mobile phone users had to present their identification card. However, eleven million people in Myanmar lack an identification card, making registration impossible.<sup>9</sup> The registration requirements have proved another obstacle to internet access in the country, with a disproportionate effect on Myanmar's most vulnerable populations.

The NLD-led government also announced that it was preparing to develop a biometric database linked to all SIM cards. On 3 December 2020, Telenor Myanmar released a statement that claimed that Myanmar authorities were attempting to gain direct access to the personal data of Telenor subscribers.<sup>10</sup> However, Myanmar lacks comprehensive data protection legislation to safeguard the data that would be collected under the system, an issue that has become all the more pressing since the coup.<sup>11</sup>

## Restrictions on access to websites

Beginning in early 2020, the NLD-led government took action to block websites that reported news unfavourable to those in power. In March 2020, the MOTC invoked Section 77 of the Telecommunications Law to direct ISPs to block access to 2,147 websites. Director General of the Directorate of Communications U Myo Swe stated that the directive was issued in part in response to 'fake news' about COVID-19. Several of the websites that were banned, however, were ethnic media outlets such as *Development Media Group*, *Narinjara*, and *Karen News*, as well as several Rohingya news sites. At the time of blocking, these media outlets had not reported about the COVID-19 pandemic. They had, however, reported extensively on the conduct of the Myanmar military, armed conflict, and human rights concerns.<sup>12</sup>

On 27 August 2020, ISPs again received a directive to block a website on the basis that the website spread 'fake news' and 'rumours'.<sup>13</sup> The order required companies to block the website of *Justice for Myanmar*, a human rights campaign that has extensively documented

<sup>7</sup> Isobel Asher Hamilton, 'Myanmar has had an internet blackout for a year. Some of its citizens still don't know there's a pandemic', *Business Insider*, 25 June 2020, available at: <https://www.businessinsider.com/myanmar-internet-shutdownpeople-unaware-coronavirus-pandemic-2020-6>.

<sup>8</sup> Naing Lin Aung, 'Telecoms ministry says it has deactivated more than 34 million SIM cards', *Myanmar Now*, 27 October 2020, available at: <https://myanmar-now.org/en/news/telecoms-ministry-says-it-has-deactivated-more-than-34-million-sim-cards>.

<sup>9</sup> Thale Solnordal Jensen, 'Half a million identities', *Norwegian Refugee Council*, 8 June 2017, available at: <https://www.nrc.no/news/2017/june/half-a-million-identities/>.

<sup>10</sup> Naing Lin Aung, 'Telenor says government is seeking direct access to customers' personal data', *Myanmar Now*, 12 December 2020, available at: <https://www.myanmar-now.org/en/news/telenor-says-government-is-seeking-direct-access-to-customers-personal-data>.

<sup>11</sup> Chris Burt, 'Myanmar closes delayed biometrics tender amid funding confusion, data protection laws still absent', *Biometric Update*, 11 June 2020, available at: <https://www.biometricupdate.com/202006/myanmar-closes-delayed-biometrics-tender-amid-funding-confusion-data-protection-laws-still-absent>.

<sup>12</sup> ARTICLE 19, 'Myanmar: Immediately lift ban on ethnic news websites', 1 April 2020, available at: <https://www.article19.org/resources/myanmar-immediately-lift-ban-on-ethnic-news-websites/>.

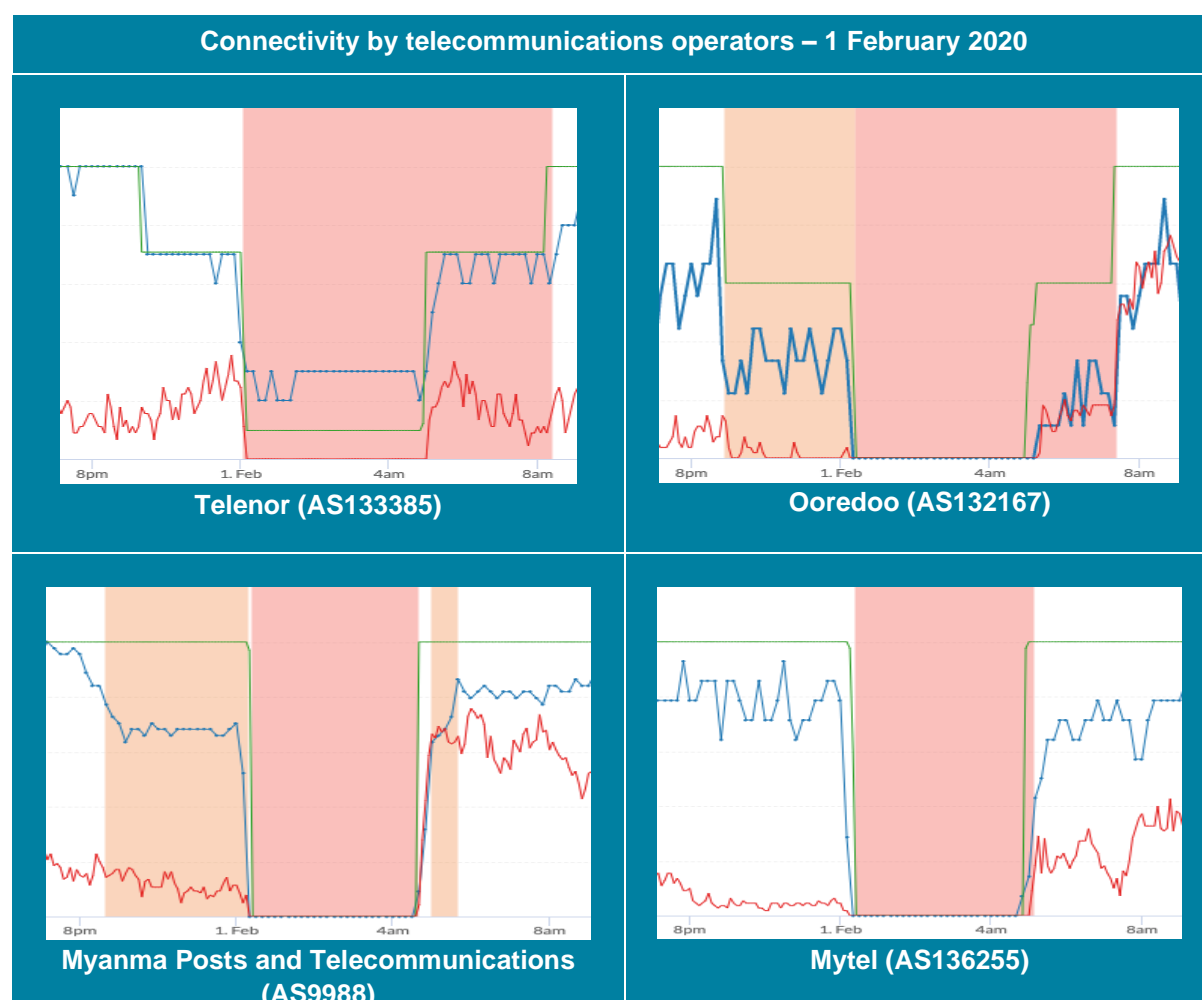
<sup>13</sup> Telenor, 'Directive to block website and 3 IP addresses', 29 August 2020, available at: <https://web.archive.org/web/20210226031418/https://www.telenor.com.mm/en/article/directive-block-website-and-3-ip-addresses>.

the Myanmar military's economic interests and exposed the corruption and covert deals that funnel resources to the military.<sup>14</sup>

## INTERNET RESTRICTIONS POST-COUP

In the early morning of **1 February 2021**, the Myanmar military seized power from the democratically elected government, justifying the coup based on allegations of fraud in the November 2020 general election. Since then, the military has implemented a range of measures to restrict internet access.

From around 3:00 am, residents across the country reported intermittent interruptions in internet connections. According to internet monitor NetBlocks, national internet connectivity levels decreased to 50 per cent by 8:00 am and only returned to around 75 per cent of ordinary levels by the late afternoon, in an apparent 'centrally issued telecoms blackout order'.<sup>15</sup> Data concerning network access through telecommunications providers shows an almost complete shutdown of connections starting soon after midnight.



<sup>14</sup> The website for Justice for Myanmar can be found at: <https://www.justiceformyanmar.org/>.

<sup>15</sup> Netblocks, 'Internet disrupted in Myanmar amid apparent military uprising', 31 January 2021, <https://netblocks.org/reports/internet-disrupted-in-myanmar-amid-apparent-military-uprising-JBZrmlB6>.

The above figures, using network data sources from Internet Outage Detection and Analysis (IODA), illustrate how four leading telecommunications providers implemented internet restrictions—presumably at the direction of military authorities—on the night of the coup.

The blue line represents active probing, which involves sending network pings to various destinations in the world and measuring the rate of returned responses. Active probing measurements use very small packets of data, so even with limited bandwidth, destinations would yield responses. A reduction in responses would therefore indicate quite severe internet throttling and/or complete disconnection. The green line represents global internet routing data, which is a feature of network operators around the world constantly exchanging routing information. It is possible for routing information to be exchanged between operators and for there still to be no local network connectivity when a firewall is in use. However, when global routing data drops significantly, it is usually a sign of total outage as caused by a physical obstruction or an internet shutdown. The red line represents unassigned network activity, essentially garbage traffic bouncing around the internet; fewer networked computers leads to a reduction in garbage traffic.

Internet connections for the four providers shown—Telenor Myanmar, Ooredoo, Myanma Posts and Telecommunications (MPT), and Mytel—slowed at varying times and to different extents. Whereas for both Telenor and Ooredoo, network restrictions started around 8:30 pm UTC (3:00 am Myanmar time), MPT and Mytel network restrictions did not begin until just after midnight UTC (6:30 am Myanmar time). Ooredoo, MPT, and Mytel users experienced a near-total network shutdown, while Telenor users retained limited network connectivity. A third variance between networks demonstrated in the above figure is the time of network connectivity resumption based on provider. While Telenor and Ooredoo network disruptions lasted longer, gradually resuming around 8:00 am UTC (around 2:00 pm Myanmar time), network connectivity for MPT and Mytel resumed sooner, at around 4:00 am UTC (10:00 am Myanmar time). Both Telenor and Ooredoo gradually restored internet connectivity, while MPT and Mytel lifted restrictions quickly.<sup>16</sup>

The variance in implementing and lifting the initial internet restrictions suggests the possibility of unclear directives from authorities, the lack of capacity to oversee a uniform application of said orders, and a different approach to implementation taken by different telecommunications providers. Further, the different times and rates of network interference exhibited by the providers indicates that, although the order was likely issued centrally, the military lacks a centralised internet kill switch.

On **3 February**, the MOTC ordered all ISPs to block access to Facebook.<sup>17</sup> The order was issued under Section 77 of the Telecommunications Law and stated that the action had been taken to stop the spread of misinformation and ‘agitation’ impacting the state’s stability.<sup>18</sup>

<sup>16</sup> IODA, Telenor network data, available at: <https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/133385&lastView=overview&from=1612073531&until=1612246331>; and IODA, Ooredoo network data, available at: <https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/132167&lastView=overview&from=1612073531&until=1612246331>; and IODA, MPT network data, available at: <https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/9988&lastView=overview&from=1612073531&until=1612246331>; and IODA, Mytel network data, available at: <https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/136255&lastView=overview&from=1612073531&until=1612246331>.

<sup>17</sup> Reuters, ‘Myanmar internet providers block Facebook services after government order’, 4 February 2021, available at: <https://www.reuters.com/article/us-myanmar-politics-facebook/myanmar-internet-providers-block-facebook-services-after-government-order-idUSKBN2A32ZE>.

<sup>18</sup> ARTICLE 19, ‘Myanmar: Military’s targeting of Facebook ratchets up post-coup assault on freedom of expression’, 4 February 2021, available at: <https://www.article19.org/resources/myanmar-militarys-targeting-of-facebook-ratchets-up-post-coup-assault-on-freedom-of-expression/>.



Internet monitor NetBlocks observed that state-owned MPT had extended the restrictions to include WhatsApp and Instagram.<sup>19</sup> Initially, the order was set to expire on 7 February.<sup>20</sup>

In response, Norwegian mobile service provider Telenor issued a statement asserting that it did not believe the order was 'based on necessity and proportionality, in accordance with international human rights law', but said it would comply with the order.<sup>21</sup> Other major telecommunications providers did not issue formal statements, nor did the military.

Following the initial order targeting Facebook, on 5 February the MOTC further directed all ISPs to temporarily extend the block on social media platforms to include Twitter and Instagram.<sup>22</sup>

From early February onward, the Open Observatory of Network Interference (OONI) has reported that a number of virtual private networks (VPNs) and related circumvention tools have been blocked in whole or in part, including ProtonVPN and TunnelBear. The blocking, OONI explained, has involved both domain name server (DNS) tampering and IP blocking but has not been consistent across all networks.<sup>23</sup> In early April, OONI noted that Psiphon VPN was also likely blocked.<sup>24</sup>

### Virtual private networks (VPNs)

A VPN is a crucial tool for preserving privacy and protecting freedom of expression and access to information online. A VPN creates a secure 'tunnel' by encrypting data sent from a user's device to a VPN server. Most VPNs are able to re-route a user's connection through a third country, allowing for evasion of geographic content restrictions. Without a VPN, a user's location is easily identified through the device's IP address. Identification of the IP address also allows governments to conduct digital surveillance more easily. Hence, using a VPN allows for the circumvention of location-specific internet restrictions while also offering a degree of privacy protection against surveillance and tracking. While VPNs can assist in evading censorship, they only function with internet access.

On **6 February**, the MOTC directed all mobile operators to temporarily block mobile internet—the second nationwide internet restriction imposed after the coup.<sup>25</sup> The order coincided with increasing anti-military protests in the country. Voice and SMS services were reportedly not impacted.<sup>26</sup> Again, the MOTC cited the Telecommunications Law as a legal basis for the shutdown and claimed that the action was meant to target circulation of 'fake

<sup>19</sup> NetBlocks, 'Confirmed: Facebook, Instagram, Messenger and WhatsApp servers are now restricted in #Myanmar on state-owned internet provider MPT; real-time metrics show selective filtering in place even as basic connectivity is restored following military coup', Twitter, 4 February 2021, available at: <https://twitter.com/netblocks/status/1357078197989474305?s=20>.

<sup>20</sup> Christopher Giles, 'Myanmar coup: How the military disrupted the internet', *BBC*, 4 February 2021, available at: <https://www.bbc.com/news/world-asia-55889565>; and Access Now, 'BREAKING: Myanmar's government is now blocking Facebook (including Instagram, WhatsApp, and Messenger) until Feb 7 at midnight. Over 22 million people use Facebook in Myanmar, and it's a critical tool for citizens to share information and organize. #KeepitOn', Twitter, 4 February 2021, available at: <https://twitter.com/accessnow/status/1357083712316440577?s=20>.

<sup>21</sup> Telenor, 'Directive to block social media service', 3 February 2021, available at: <https://www.telenor.com/directive-to-block-social-media-service/>.

<sup>22</sup> Telenor, 'Directive to block social media services Twitter and Instagram in Myanmar', 5 February 2021, available at: <https://www.telenor.com/directive-to-block-social-media-services-twitter-and-instagram-in-myanmar/>.

<sup>23</sup> OONI, 'Myanmar: Data on internet blocks and internet outages following military coup', 9 March 2021, available at: <https://ooni.org/post/2021-myanmar-internet-blocks-and-outages/#blocking-of-circumvention-tool-sites>. DNS tampering involves blocking the website URL, for example, 'protonvpn.com' or 'openvpn.net'. IP blocking involves blocking the IP address associated with a URL. While domain names do not often change, in order to respond to efforts to block their operation, most VPNs maintain multiple IP addresses and change them often.

<sup>24</sup> OONI, '! Anomaly: Psiphon is likely blocked', 4 April 2021, available at: [https://explorer.ooni.org/measurement/20210404T071321Z\\_psiphon\\_MM\\_135300\\_n1\\_q8iCSOO7EuU4H4I](https://explorer.ooni.org/measurement/20210404T071321Z_psiphon_MM_135300_n1_q8iCSOO7EuU4H4I).

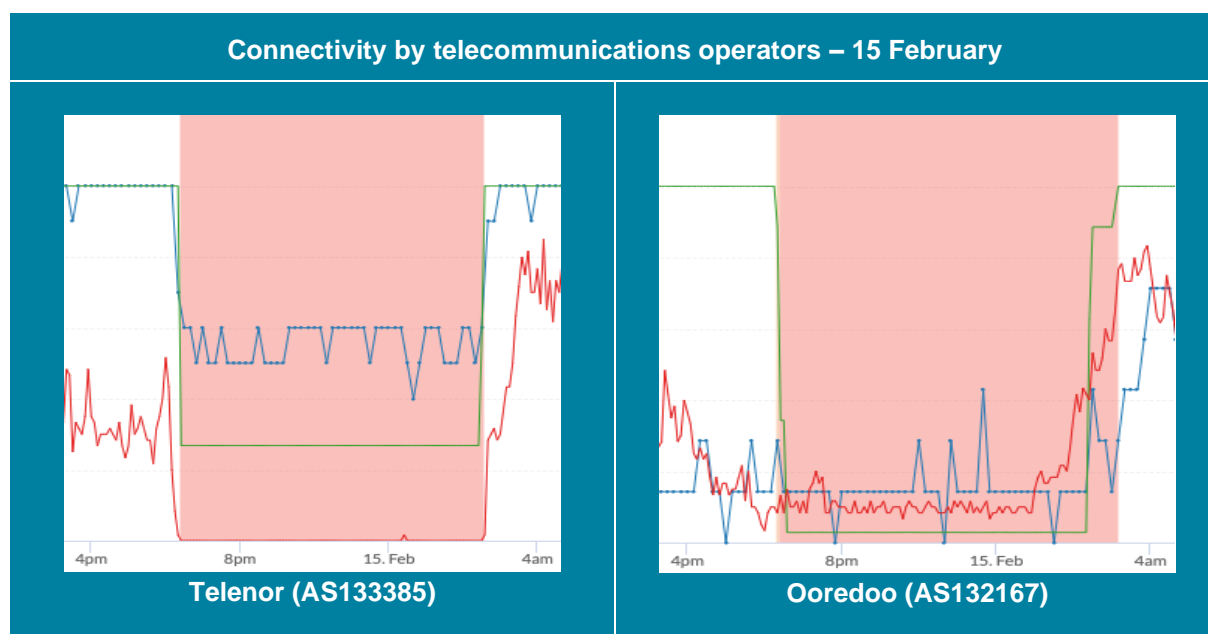
<sup>25</sup> Telenor, 'Data network restored in Myanmar', 6 February 2021, available at: <https://www.telenor.com/media/press-release/myanmar-authorities-orders-nationwide-shutdown-of-the-data-network>.

<sup>26</sup> *Ibid.*

news' and threats to national stability. Telenor stated that it had decided to comply with the order because of its obligations under local law and to protect the safety of its employees,<sup>27</sup> but no other telecommunications providers released statements. According to IODA, connectivity began deteriorating after 9:00 am and from 2:00 pm onwards hovered at just 20 per cent of ordinary connectivity levels for another 24 hours before slowly returning to normal levels on 7 February.<sup>28</sup> Social media platforms, however, remained blocked despite the earlier indication that the block on Facebook would be lifted on 7 February.<sup>29</sup>

On **14 February**, Telenor wrote on its website that it was no longer possible to disclose the directives it received from Myanmar authorities. From 1 to 14 February, Telenor had publicly acknowledged 12 directives regarding network and targeted URL or IP address blocking.<sup>30</sup> Telenor had been the only telecommunications provider in Myanmar publicly disclosing the existence of the directives.

**15 February** marked the beginning of nightly internet shutdowns, which continued for 72 consecutive nights. Beginning at 1:00 am, internet connectivity levels sharply dropped and remained around 16 per cent of normal levels before returning to normal after 9:00 am.<sup>31</sup> Social media remained inaccessible without a VPN. Every night from 15 February to 28 April, all forms of the internet in the country were shut down.



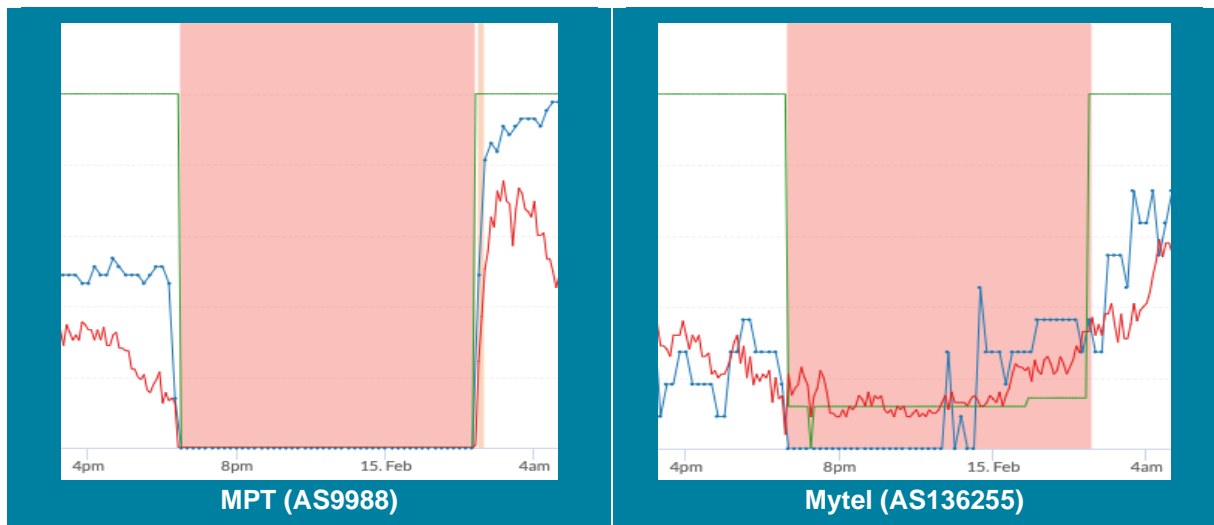
<sup>27</sup> Telenor, 'Data network restored in Myanmar', 6 February 2021, available at: <https://www.telenor.com/media/press-release/myanmar-authorities-orders-nationwide-shutdown-of-the-data-network>.

<sup>28</sup> IODA, Signals for Myanmar, 4 February to 8 February 2021, available at: <https://ioda.caida.org/ioda/dashboard#view=inspect&entity=country/MM&lastView=overview&from=1612437274&until=1612782874>.

<sup>29</sup> Philip Heijmans, 'Myanmar blocks Facebook as protests gain traction', *Bloomberg*, 4 February 2021, available at: <https://www.bloomberquint.com/politics/myanmar-orders-facebook-blocked-as-protests-emerge-after-coup>.

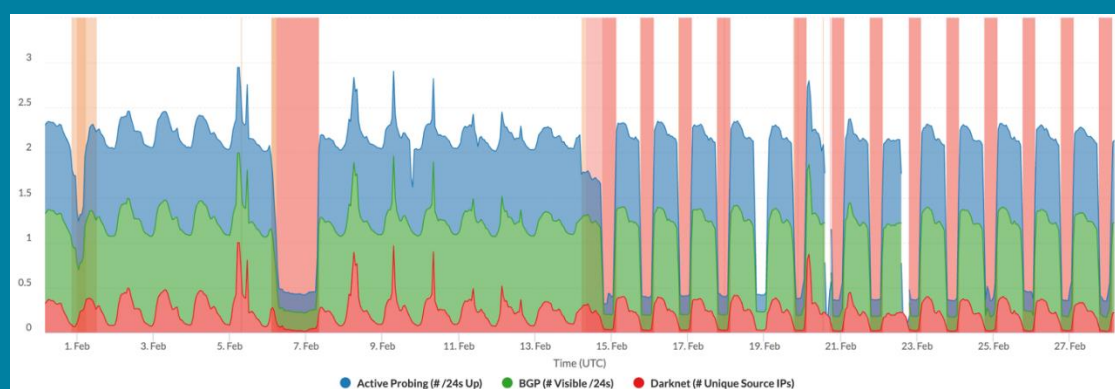
<sup>30</sup> Telenor, 'Directives from authorities in Myanmar – February-April 2021', available at: <https://www.telenor.com/sustainability/responsible-business/human-rights/mitigate/human-rights-in-myanmar/directives-from-authorities-in-myanmar-february-2021/>.

<sup>31</sup> IODA, Signals for Myanmar, 4 February to 8 February 2021, available at: <https://ioda.caida.org/ioda/dashboard#view=inspect&entity=country/MM&lastView=overview&from=1613387674&until=1613474074>.



The above figures, using network data sources from IODA, illustrate the difference in the 15 February night time internet shutdown from the first post-coup shutdown on 1 February. The figures include network data from the same four leading telecommunications providers compared in the figures above. In contrast to the first night of the coup, the four providers (Telenor Myanmar, Ooredoo, MPT, and Mytel) implemented the 15 February shutdown at nearly the same time (around 7:00 pm UTC or 1:00 am Myanmar time) and resumed service at around 3:00 am UTC (9:00 am Myanmar time). MPT imposed the most complete internet shutdown, with a near-total drop in network activity, while Telenor network activity remained at around 50 percent.<sup>32</sup> The relatively sudden cut in network connectivity and resumption of service at the designated times suggests greater coordination and pressure from the authorities, greater understanding of network restriction expectations from telecommunications providers, or a combination thereof.

### Network connectivity – February 2021



Network activity for February 2021, source: IODA <https://ioda.caida.org/>.

<sup>32</sup> IODA, Telenor network data, available at:

<https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/133385&lastView=overview&from=1613283131&until=1613455931>; and IODA, Ooredoo network data, available at:

<https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/132167&lastView=overview&from=1613283131&until=1613455931>; and IODA, MPT network data, available at:

<https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/9988&lastView=overview&from=1613283131&until=1613455931>; and IODA, Mytel network data, available at:

<https://ioda.caida.org/ioda/dashboard#view=inspect&entity=asn/136255&lastView=overview&from=1613283131&until=1613455931>.

The above figure shows network connectivity outages over the first month following the coup. It represents the first three near-total nationwide shutdowns on 1 February, 7 February, and 15 February, following thereon by nightly internet shutdowns where nearly all network activity is seen dropping significantly every night, as shown by the red vertical alert areas. The nightly outages are demonstrated by all three data collection sources.

On the morning of **15 March**, as the public expected mobile internet to be reinstated for the day, mobile data networks remained disabled around the country.<sup>33</sup> This marked the beginning of a nationwide mobile internet ban at all hours of the day.

**Mobile internet:** Mobile internet works by connecting via the cellular network associated with a SIM card and subscription service. The mobile device sends and receives a network internet connection via cell towers.

**Public Wi-Fi:** Public access Wi-Fi may be accessible for free by the general public or may be provided to customers by a particular ISP through a login password.

**Fixed wireless:** Fixed wireless internet works by connecting fixed locations via base stations or wireless routers, delivering direct internet connectivity that is often faster than 4G.<sup>34</sup>

**Fixed line:** With a fixed line connection, the internet is provided through a physical connection either delivered via a phone line (ADSL) or cable (such as a fibreoptic cable) installed by the ISP. While MPT, Telenor, and others provide fibre to the home (FTTH) service, state-owned Mytel is reportedly the largest operator of FTTH in Myanmar.

On **17 March**, the military broadened the internet restrictions to include blocking public Wi-Fi access, affecting public Wi-Fi hotspots in shopping centres, and other public areas.<sup>35</sup> The order also affected Wi-Fi services provided by ISPs like Myanmar Net, which provide limited login passwords for their customers to be able to connect to Myanmar Net Wi-Fi routers in public places. The move was widely interpreted as an effort to limit the ability of the protesters to organise.

On **30 March**, the Bago City Development Corporation, without providing a legal justification, issued an order directing ISPs to begin reporting the home addresses of wireless internet users.<sup>36</sup> There are no reports that similar directives were issued elsewhere in the country.

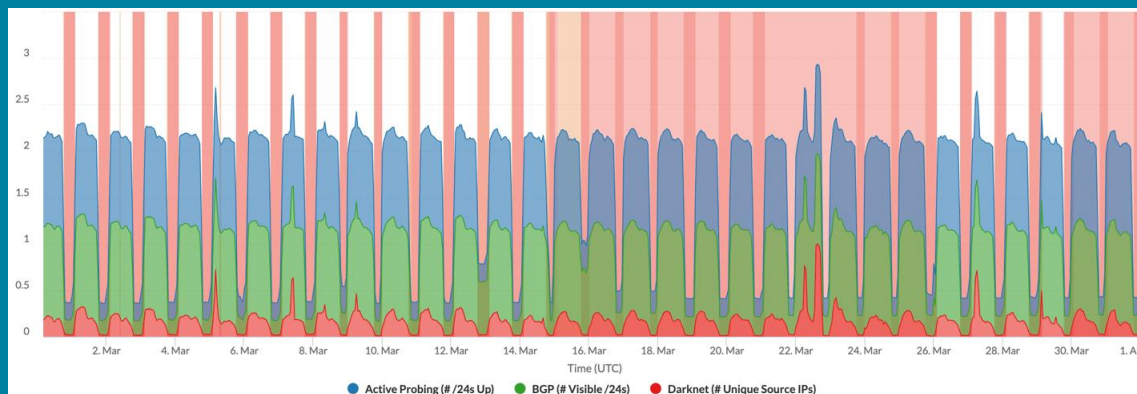
<sup>33</sup> NetBlocks, 'Confirmed: Internet has been cut in #Myanmar for the 29th consecutive night, exactly one month after the military junta introduced the cycle of nightly internet blackouts. Network data show connectivity collapsing to 13% of ordinary levels from 1 am', Twitter, 15 March 2021, available at: <https://twitter.com/netblocks/status/1371277902633971715?s=20>.

<sup>34</sup> High Speed Internet, 'Fixed Wireless. Mobile Broadband. What's the Difference Anyway?', 15 September 2016, available at: <https://www.highspeedinternet.com/resources/fixed-wireless-vs-mobile-broadband-internet>.

<sup>35</sup> *Jurist*, 'Myanmar: internet cutoff looms as junta flexes martial law muscle in Yangon townships', 17 March 2021, available at: <https://www.jurist.org/news/2021/03/myanmar-internet-cutoff-looms-as-junta-flexes-martial-law-muscle-in-yangon-townships/>.

<sup>36</sup> Pyaezone, 'In Bago, Min Aung Hlaing's people demand telecom companies to provide confidential information of customers who setup #Wifi service at home, by 1st April 2021 latest. -Khit Thit', Twitter, 30 March 2021, available at: <https://twitter.com/pyaezone/status/1376847044405469188?s=21>.

## Network connectivity – March 2021



Network Activity for March 2021, source: IODA <https://ioda.caida.org/>.

The above figure represents the consistent network interruptions caused by the nightly internet shutdowns shown in the repeating vertical red bands. The figure also illustrates the broader significant network connectivity reduction beginning first on 15 March with the ongoing blockage of mobile data networks and further intensifying on 17 March with the blockage of public Wi-Fi, represented by the extended vertical red field.

On **1 April**, Myanmar authorities expanded the internet restrictions to include a block on all fixed wireless internet services. The directive to block fixed wireless internet was reportedly emailed to at least one telecommunications provider and did not state the reason or legal basis for the restriction.<sup>37</sup> This left fixed line internet (including FTTH and ADSL services) as the only remaining form of internet access in Myanmar. According to *Nikkei Asia*, there are only approximately 600,000 FTTH connections in Myanmar, with most households instead relying on fixed wireless connections.<sup>38</sup> In a country with a population of approximately 54 million people, this means that less than one per cent of the population had internet access after the 1 April restrictions.

The shutdown of all other types of internet connection has reportedly sparked a scramble to expand fixed line services. However, many people in Myanmar have reported wait times of one to two weeks to over a month to install new fixed line internet connections. The delays are not only a result of the rise in demand. ISPs have also reported that their engineers are concerned for their lives in light of increasing cases of random killings by security forces, especially since the 2 April death of Su Su Kyi, an employee of Shihan Bank who was shot in the head while riding in a company vehicle.<sup>39</sup>

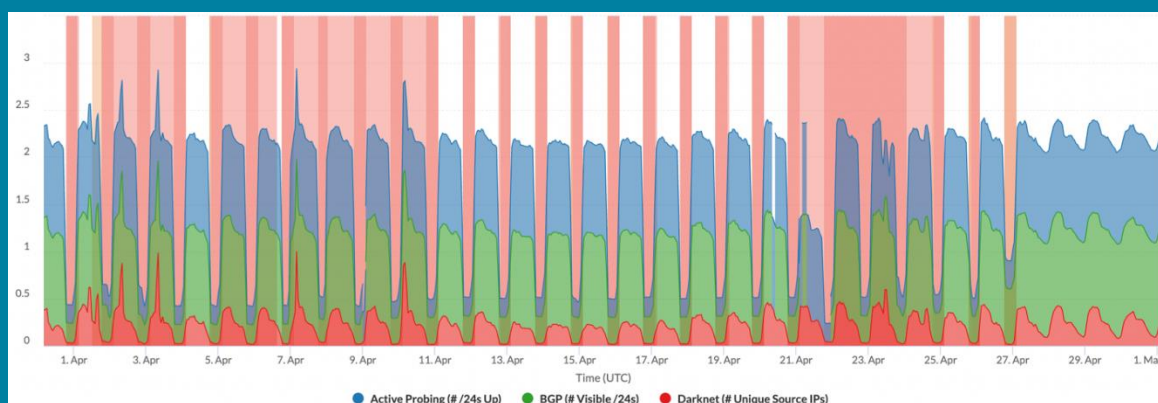
<sup>37</sup> *Reuters*, 'Myanmar orders wireless internet shutdown until further notice: telecoms sources', 1 April 2021, available at: <https://www.reuters.com/article/us-myanmar-politics-internet/myanmar-orders-wireless-internet-shutdown-until-further-notice-telecoms-sources-idUSKBN2BO5H2>.

<sup>38</sup> Gwen Robinson and Rory Wallace, 'Myanmar shutdown of wireless internet fuels fears of news blackout', *Nikkei Asia*, 2 April 2021, available at: <https://asia.nikkei.com/Spotlight/Myanmar-Coup/Myanmar-shutdown-of-wireless-internet-fuels-fears-of-news-blackout>.

<sup>39</sup> *Myanmar Now*, 'Bank staffer dies two days after being shot by junta's troops on her way home from work', 2 April 2021, available at: <https://myanmar-now.org/en/news/bank-staffer-dies-two-days-after-being-shot-by-juntas-troops-on-her-way-home-from-work>.

On **28 April**, the nightly ban on fixed line internet services was lifted.<sup>40</sup> Afterwards, those with fixed line connections were again able to access the internet 24 hours a day, although the censorship of websites and circumvention tools remained in place.

### Network connectivity – April 2021



Network Activity for April 2021, source: IODA <https://ioda.caida.org/>.

The above figure illustrates the consistent nightly internet shutdowns of fixed line internet, which finally ended on 28 April.

According to media reports, in late April, the government relaxed restrictions on certain online banking and business applications, allowing customers to regain access to those platforms.<sup>41</sup> In May, the MOTC sent ISPs a ‘whitelist’ of apps and websites that customers were permitted to access.<sup>42</sup> The Ministry ordered the companies to restrict access to all other apps and websites. Whitelisted websites and services included social media platforms such as Tinder and China’s WeChat as well as online services such as Grab. Twitter and Facebook were not on the list, but Facebook-owned Instagram and WhatsApp were whitelisted. The extent to which ISPs have implemented the orders—and whether the orders are still in effect—is not clear at the time of writing. Internet users experience varying levels of access to a wide range of websites, including those presumably not on the whitelist.<sup>43</sup> Access to websites has changed over time and has differed significantly depending on the network used.

**Whitelisting:** A whitelist (also sometimes called a walled garden or an intranet) is a network access control system that allows users to access a limited number of pre-approved websites or other online services, with others being blocked. A whitelist may be based on the pre-approval of a URL, IP address, domain name, or another element.

<sup>40</sup> *Coconuts Yangon*, ‘Myanmar’s Junta has lifted the overnight internet ban, and no one’s really sure why’, 28 April 2021, available at: <https://coconuts.co/yanmar/news/myanmars-junta-has-lifted-the-overnight-internet-ban-and-no-ones-really-sure-why/>.

<sup>41</sup> Rory Wallace, ‘Myanmar junta builds ‘walled garden’ of internet services’, *Nikkei Asia*, 28 April 2021, available at: <https://asia.nikkei.com/Spotlight/Myanmar-Coup/Myanmar-junta-builds-walled-garden-of-internet-services>.

<sup>42</sup> *Nikkei Asia*, ‘Myanmar allows Tinder but axes dissent havens Twitter, Facebook’, 25 May 2021, available at: <https://asia.nikkei.com/Spotlight/Myanmar-Coup/Myanmar-allows-Tinder-but-axes-dissent-havens-Twitter-Facebook>; and *Frontier Myanmar*, ‘Whitelisted internet takes Myanmar back to a “dark age”’, 30 June 2021, available at: <https://www.frontiermyanmar.net/en/whitelisted-internet-takes-myanmar-back-to-a-dark-age/>.

<sup>43</sup> See, data collected by censorship monitor OONI, available at: [https://explorer.ooni.org/search?until=2021-07-09&since=2021-06-09&probe\\_cc=MM](https://explorer.ooni.org/search?until=2021-07-09&since=2021-06-09&probe_cc=MM).

On **4 June**, the junta ordered a shutdown of all internet sources for one hour,<sup>44</sup> coinciding with a press conference held by the National Unity Government.

On **8 July**, Telenor announced the sale of its mobile operations in Myanmar to M1 Group.<sup>45</sup> As described above, Telenor was the only telecommunications company that publicly reported government orders imposing internet restrictions in the wake of the coup. Telenor's departure from the market will further obscure the military's efforts to obstruct internet access. M1 Group has been added by Burma Campaign UK, a human rights watchdog, to its 'Dirty List' of international companies doing business with the Myanmar Military.<sup>46</sup>

## IMPACT OF INTERNET RESTRICTIONS

The vast majority of Myanmar citizens rely on smartphones and mobile data to access the internet, read and share information, and upload multimedia. Many people in Myanmar have multiple devices, as described in a 2019 industry report noting a 124 per cent mobile connection penetration.<sup>47</sup> In the middle of the pandemic and military coup, online connectivity has become ever-more important. Many civilians are at risk because they lack access to vital information. Given the reliance on mobile internet in Myanmar, the mobile internet restrictions and blocking of social media platforms such as Facebook have severely impacted daily life for many people. The junta's measures to restrict public Wi-Fi and fixed wireless have exacerbated these effects.

### Stymying accountability efforts

The UN Special Rapporteur on the situation of human rights in Myanmar has noted that the shutdowns provide impunity for 'security forces carrying out arrests and violent crackdowns throughout the night'.<sup>48</sup> The government has been able to prevent people from promptly uploading photos and videos showing abuse by the military and police. Myanmar authorities shut down mobile data just as killings of protesters increased dramatically.<sup>49</sup>

More generally, the internet restrictions have had a severe impact on the ability of human rights defenders and media organisations—who are crucial to accountability efforts—to operate inside the country. While by no means the sole factor influencing the flight of individuals and organisations outside of the country, internet restrictions have made it nearly impossible for civil society actors to carry out their essential work. This is especially true of individuals and organisations forced into hiding, many of whom do not have access to fixed line internet service.

<sup>44</sup> Martin Petty, 'Myanmar junta opponents say no faith in ASEAN as envoys visit', *Reuters*, 4 June 2021, available at: <https://www.reuters.com/article/myanmar-politics/internet-outages-across-myanmar-witnesses-idUSP9N2HC02Q>.

<sup>45</sup> Telenor, 'Telenor Group sells Telenor Myanmar to M1 Group', 8 July 2021, available at: <https://www.telenor.com/media/press-release/telenor-group-sells-telenor-myanmar-to-m1-group%e2%80%af>.

<sup>46</sup> Burma Campaign UK, 'M1 Group', 20 August 2019, available at: <https://burmacampaign.org.uk/take-action/m1-group/>.

<sup>47</sup> Mobile World Live, 'Intelligence Brief: Where does Myanmar stand today?', 4 Dec 2019, <https://www.mobileworldlive.com/blog/intelligence-brief-where-does-myanmar-stand-today>.

<sup>48</sup> Human Rights Council, 'Report of the Special Rapporteur on the situation of human rights in Myanmar, Thomas H. Andrews', A/HRC/46/56, 4 March 2021, available at: [https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session46/Documents/A\\_HRC\\_46\\_56.pdf](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session46/Documents/A_HRC_46_56.pdf).

<sup>49</sup> Assistance Association Political Prisoners, 'Daily Briefing in Relation to the Military Coup', 6 July 2021, available at: <https://aappb.org/?p=16352>.

## Surveillance

Myanmar authorities' attacks on the internet have also made it easier for the government to surveil dissidents. As stated above, the government has throttled internet speeds since the coup. 2G networks are not secure. 2G relies on weak encryption that makes it easy for traffic between the device and the cell tower to be intercepted.<sup>50</sup> Communicating without a mobile internet connection has the same effect. Without an internet connection, people can only use voice calls or SMS and MMS messaging, which are much easier for the government to intercept. Without encrypted messaging applications like Signal that require internet connectivity, there are few options for secure communication. In the meantime, the military has reportedly been increasing efforts to force ISPs to install technologies that would allow them to intercept calls, messages, and web traffic.<sup>51</sup>

## Preventing the organisation of protests

Since early February, Facebook and many other social media and messaging platforms have been officially banned in Myanmar. Facebook is the primary way many people in Myanmar access information online and has been an important platform for organising demonstrations and documenting and exposing abuses by the military. Moreover, the blocking of mobile data and public Wi-Fi has severely curtailed the ability of activists to organise, join protests, and report on abuses by the government.

## Economic effects

The internet shutdown has also had a profound effect on Myanmar's economy. Although many users are still able to access the internet using VPNs, the disruption to trade and banking has been significant. Since the coup, disruptions to banking activities have prevented the payment of salaries and have made transferring funds in and out of the country exceedingly difficult. The lack of mobile internet access has prevented people from using online banking, increasing the reliance on cash and cash-based transfers. Every day, hundreds of people line up in front of ATMs for the chance to withdraw between 200,000 to 300,000 kyats (120-180 USD). Before the coup, mobile transfers were more convenient, efficient, and secure and helped facilitate the transfer of funds from family members living abroad. Recent internet restrictions have impeded such transfers.

Business operations have also become extremely challenging because of the lack of reliable internet access. The COVID-19 lockdown has resulted in most people relying on the internet to communicate, interact, and continue with their job responsibilities from home. Amid the internet blackouts, people who work remotely have missed work activities and meetings. Moreover, many online delivery drivers have lost their jobs due to the shutdown.<sup>52</sup> Finally, the shutdowns, combined with the pandemic, have made it difficult for friends and families to communicate with each other.

<sup>50</sup> For more on 2G security flaws see: Electronic Frontiers Foundation, 'Your Phone Is Vulnerable Because of 2G, But it Doesn't Have to Be', 29 June 2020, available at: <https://www.eff.org/deeplinks/2020/06/your-phone-vulnerable-because-2g-it-doesnt-have-be>; and Tech Republic, 'Security holes in 2G and 3G networks will pose a risk for next several years', 19 February 2020, available at: <https://www.techrepublic.com/article/security-holes-in-2g-and-3g-networks-will-pose-a-risk-for-next-several-years/>.

<sup>51</sup> Fanny Potkin, 'After pressuring telecom firms, Myanmar's junta bans executives from leaving', *Reuters*, 5 July 2021, available at: <https://www.reuters.com/world/asia-pacific/exclusive-after-pressuring-telecom-firms-myanmars-junta-bans-executives-leaving-2021-07-05/>.

<sup>52</sup> KRAsia, 'Myanmar's coup nearly put food delivery drivers out of business', 22 May 2021, available at: <https://kr-asia.com/myanmars-coup-nearly-put-food-delivery-drivers-out-of-business-tech-in-culture>.



Thousands of small internet businesses operating over Facebook have had their businesses damaged by the internet restrictions. Before the coup, Myanmar experienced a surge in entrepreneurship and had a burgeoning start-up ecosystem, with many new internet-based small and medium-sized enterprises being formed. However, many businesses have been forced to shutter due to the shutdown, depriving Myanmar people of necessary services. NetBlocks, an organisation that monitors network connectivity and the effects of the shutdown, estimates that the economic cost of the nationwide internet shutdown is approximately USD 24 million per day. As of early July, Top 10 VPN put the cost of the shutdown at USD 2.1 billion.<sup>53</sup>

## DOMESTIC LEGAL FRAMEWORK

### Authority to restrict access to parts or all of the internet

While the military junta has amended legal provisions, enacted new crimes, and imposed martial law on parts of the country, it has done little to alter the existing legal basis for internet access restrictions. This may be because the pre-coup legal framework was already excessively broad and open to abuse.

Section 77 of the Telecommunications Law provides that the MOTC:

[M]ay, when an emergency situation arises to operate for public interest, direct the licensee to suspend a Telecommunications Service, to intercept, not to operate any specific form of communication, to obtain necessary information and communications, and to temporarily control the Telecommunications Service and Telecommunications Equipments.

As noted above, pre-coup, Myanmar authorities repeatedly invoked Section 77 of the Telecommunications Law to restrict mobile data<sup>54</sup> and block access to specific websites.<sup>55</sup> Post-coup, authorities have failed to publicly explain the legal basis for the ongoing internet restrictions. However, it is likely that in directing ISPs to block internet access, including access to specific sites, authorities have continued to rely on Section 77 of the Telecommunications Law.

### Draft Cyber Security Law and Electronic Transactions Law amendments

In early February, the Myanmar military published a draft Cyber Security Law and requested comments from corporate stakeholders by 15 February.<sup>56</sup> Shortly thereafter, the military enacted amendments to the Electronic Transactions Law that incorporated some of the provisions contained in the proposed Cyber Security Law. These included several provisions

<sup>53</sup> Roland Oliphant, Thompson Chau and Samaan Lateef, "When the internet goes down the night raids start": Inside the deadly phenomenon of web shutdowns', *The Telegraph*, 28 February 2021, available at: <https://www.telegraph.co.uk/news/2021/02/28/internet-goes-night-raids-start-inside-deadly-phenomenon-web/#navigation>; and Top 10 VPN, 'The Global Cost of internet Shutdowns', 4 January 2021, available at: <https://www.top10vpn.com/cost-of-internet-shutdowns/>.

<sup>54</sup> ARTICLE 19, 'Myanmar: Internet shutdown in Rakhine and Chin States', 2 August 2019, available at: <https://www.article19.org/resources/briefing-myanmars-internet-shutdown-in-rakhine-and-chin-states/>.

<sup>55</sup> ARTICLE 19, 'Myanmar: Immediately lift ban on ethnic news websites', 1 April 2020, available at: <https://www.article19.org/resources/myanmar-immediately-lift-ban-on-ethnic-news-websites/>.

<sup>56</sup> ARTICLE 19, 'Myanmar: Scrap Cyber Security Draft Law and Restore Full Internet Connectivity', 12 February 2021, available at: <https://www.article19.org/resources/myanmar-scrap-cyber-security-draft-law-and-restore-full-internet-connectivity/>.

criminalising online expression, such as spreading misinformation or disinformation. It also incorporated some barebones data protection provisions for the online space.<sup>57</sup>

While the Cyber Security Law has yet to be adopted by the junta, it is reportedly still being considered.<sup>58</sup> The draft Cyber Security Law raises a number of concerns:

- Overall state control:** The draft law envisages a Cyber Security Steering Committee primarily made up of government officials but including some representatives from civil society and cybersecurity professionals. Overall, however, the structure and powers established by the draft Cyber Security Law grant a tremendous amount of unfettered power and control to the government to regulate information flows in Myanmar. This ranges from content restrictions and rules governing data storage and access to the granting of licences and appeals against refusals to grant such licences (Articles 76 and 77) through to the investigation of cybercrimes. This is against a backdrop of unrestricted powers to make up rules and directives to suit the government's needs (e.g., Articles 79 and 87) in the absence of any mechanisms to scrutinise or otherwise hold the government to account. The rules themselves are unspecific, overly broad, and open to abuse.
- Content removal:** Section 29 of the law would provide Myanmar authorities with the ability to force removal of an extremely broad range of online content, including expression that should be protected under international law. Section 29(a) and (b) call for 'prevention, removal, destruction and cessation of content ... causing hate, disrupting the unity, stabilisation and peace' and 'misinformation and disinformation'. However, key terms such as 'unity', 'stability', 'misinformation', or 'disinformation' are left undefined. They are also inherently vague. This provision is overly broad and in breach of the legality principle under international human rights that requires laws to be couched in terms that are sufficiently precise for individuals to know how to regulate their conduct. These concerns are exacerbated by the fact that what is impermissible under the law is decided by the government rather than the courts, in breach of international standards on freedom of expression.
- Internet shutdowns:** Section 50 of the draft law broadens the basis on which authorities can prohibit online service provision, control online service provision, and permanently ban an online service provider. The Section goes further than the current basis for internet shutdowns—Section 77 of the Telecommunications Law—by only requiring that authorities act in the 'public interest' and by allowing ministries to directly control the devices related to online service provision. Internet shutdowns are a grave violation of the right to freedom of expression as they prevent individuals from gaining access to potentially life-saving information, whether in terms of access to public health advice or where to seek refuge in times of serious disruption to civilian life as is currently the case in Myanmar.

<sup>57</sup> Free Expression Myanmar, 'Myanmar's new Electronic Transactions Law Amendment', 18 February 2021, available at: <https://freeexpressionmyanmar.org/myanmars-new-electronic-transactions-law-amendment/>.

<sup>58</sup> Senior General Min Aung Hlaing, 'Chairman of State Administration Council Commander-in-Chief of Defence Services Senior General Min Aung Hlaing delivers address at meeting (9/2021) of State Administration Council', 27 April 2021, available at: <https://www.seniorgeneralminaunghlaing.com.mm/en/25435/chairman-state-administration-council-commander-chief-defence-services-senior-general-min-aung-hlaing-delivers-address-meeting-92021-state-administration-council/>; and Myanmar Centre for Responsible Business, 'Myanmar's Legal Framework For Cybersecurity Needs To Be Built To International Standards', 10 May 2021, available at: <https://www.myanmar-responsiblebusiness.org/news/legal-framework-for-cybersecurity.html>.

- **Data retention:** Article 30 further requires ISPs to retain usernames, IP addresses, national IDs, and other personal data for up to three years and to provide this information (Article 31) to authorities upon request without any safeguards for the protection of the right to privacy.
- **Data localisation:** Section 26 of the law requires that online service providers maintain devices located in the country at a place designated by Myanmar authorities. This provision allows for Myanmar authorities to keep data in a place where they can easily access it.
- **Overbroad offences and disproportionate penalties:** The rights-abusing provisions of the law are backed up by criminal penalties for employees of online service providers.

If enacted, the draft Cyber Security Law would provide an additional basis for restricting internet access with even fewer safeguards than the Telecommunications Law. Given the military's control of all branches of government and disregard for existing law, it could be argued that legal changes have little practical effect on the military's decisions and actions. Nevertheless, the military has made a point of portraying its actions as consistent with Myanmar law, and so degradation of legal restraints on internet controls should be viewed with concern.

### Restrictions that chill expression online

Prior to the coup, ARTICLE 19 and others extensively documented the Myanmar authorities' attacks on freedom of expression using a variety of legal provisions.<sup>59</sup> Section 66(d)<sup>60</sup> of the Telecommunications Law, Section 505 of the Penal Code, and various other provisions were regularly used to arrest, try, and imprison individuals who criticised the government and military or expressed controversial opinions.

Post-coup, the military has sought to expand the range of prohibited expression. In February 2021, the junta enacted amendments to the Penal Code and Criminal Procedure Code that both increased the punishment for existing crimes and created new crimes.<sup>61</sup>

- An amendment to Section 124A extends the scope of the crime of sedition to include expression that attempts to 'bring into hatred or contempt' the Defense Services.
- New offences under Section 124C and 124D cover sabotage and 'disruption' of the Defense Services or government officials. The Section could easily apply to those taking part in the civil disobedience campaign undertaken by civil servants following the coup. The offences are non-bailable and non-compoundable.

<sup>59</sup> ARTICLE 19, 'Myanmar: UN Human Rights Council must urge newly-elected government to prioritise legal reform to guarantee the right to freedom of expression', 23 December 2020, available at: [https://www.article19.org/wp-content/uploads/2020/12/2020\\_12.23-HRC-Briefing-2021-FINAL.pdf](https://www.article19.org/wp-content/uploads/2020/12/2020_12.23-HRC-Briefing-2021-FINAL.pdf); and Human Rights Watch, 'Dashed Hopes: The Criminalization of Peaceful Expression in Myanmar', 31 January 2019, available at: <https://www.hrw.org/report/2019/01/31/dashed-hopes/criminalization-peaceful-expression-myanmar>.

<sup>60</sup> Section 66(d) of the 2013 Telecommunications Law prohibits 'extorting, defaming, disturbing or threatening to any person by using any telecommunications network' and provides sentences of up to two years' imprisonment, a fine, or both. Section 68(a) of the Telecommunications Law makes it a crime to commit 'communications, reception, transmission, distribution or conveyance of incorrect information with dishonesty or participation'. Violations of Section 68(a) are punishable by up to one year's imprisonment, a fine, or both.

<sup>61</sup> Republic of the Union of Myanmar State Administration Council State Administration Council Law No (5/2021) Law Amending the Penal Code, 14 February 2021, available at: [https://cdn.myanmarseo.com/file/client-cdn/gnlm/wp-content/uploads/2021/02/15\\_Feb\\_21\\_gnlm\\_1.pdf](https://cdn.myanmarseo.com/file/client-cdn/gnlm/wp-content/uploads/2021/02/15_Feb_21_gnlm_1.pdf); and Republic of the Union of Myanmar State Administration Council State Administration Council Law No (6/2021) Law Amending the Code of Criminal Procedure, 14 February 2021, available at: [https://cdn.myanmarseo.com/file/client-cdn/gnlm/wp-content/uploads/2021/02/15\\_Feb\\_21\\_gnlm\\_1.pdf](https://cdn.myanmarseo.com/file/client-cdn/gnlm/wp-content/uploads/2021/02/15_Feb_21_gnlm_1.pdf).

- A new Section 505A criminalises causing 'fear', knowingly spreading 'fake news', and agitating to commit an offence against a government employee. Arrests may be made without a warrant, and convictions carry a penalty of up to three years' imprisonment.

Since the coup, the military has prosecuted hundreds of individuals. Many of these cases are linked to online expression.<sup>62</sup>

The military has eroded privacy protections by repealing articles of the Law Protecting the Privacy and Security of Citizens regarding searches and seizures, and reviving provisions of the Ward or Village-Tract Administration Law that require residents to register overnight guests with local officials.<sup>63</sup>

In mid-March, the Myanmar military implemented a series of martial law orders across several townships in Yangon and Mandalay.<sup>64</sup> The martial law orders effectively strip defendants of fair trial rights by transferring jurisdiction for certain crimes to military courts that lack procedural safeguards. The crimes enumerated in the martial law orders include several expression-related offences, for example, Sections 124A, 124C, 124D, 500 and 505A of the Penal Code and cases involving 'press and media law', 'printing and publishing law', and 'electronic communications law'. The third martial law enacts severe penalties for the crimes enumerated, mandating the maximum possible sentence, and in some cases, death.<sup>65</sup> The imposition of martial law exacerbates the already extreme penalties for speech that should be protected, not prosecuted, under international law.

## INTERNATIONAL LAW

The rights to freedom of expression and information are protected by Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). Although Myanmar is not a party to the ICCPR—and the UDHR does not create international law obligations for states—the right to freedom of expression is generally considered customary international law and hence binding on Myanmar. The Human Rights Committee has affirmed that all forms of expression and all means of information dissemination, including the internet, are protected under international law.<sup>66</sup> Likewise, the UN Human Rights Council, Human Rights Committee, and General Assembly have emphasised that the right to freedom of expression applies online.<sup>67</sup> As such, any restrictions on access to the internet are only permitted if they are consistent with international law.<sup>68</sup>

<sup>62</sup> Antonio Prokscha, 'Journalists arrested as protest crackdown intensifies in Myanmar', *International Press Institute*, 3 March 2021, available at: <https://ipi.media/journalists-arrested-as-protest-crackdown-intensifies-in-myanmar/>; and Freemuse, 'Myanmar Actress and Actor arrested for opposition against the military', 23 April 2021, available at: <https://freemuse.org/news/myanmar-actress-and-actor-arrested-for-opposition-against-the-military/>.

<sup>63</sup> Human Rights Watch, 'Myanmar: Post-Coup Legal Changes Erode Human Rights', 2 March 2021, available at: <https://www.hrw.org/news/2021/03/02/myanmar-post-coup-legal-changes-erode-human-rights>.

<sup>64</sup> Martial Law Order 1/2021, Martial Law Order 2/2021, and Martial Law Order 3/2021.

<sup>65</sup> Martial Law Order 3/2021.

<sup>66</sup> ICCPR, Article 19; and Human Rights Committee, General Comment No. 34, UN Doc CCPR/C/GC/34, 12 September 2011, at paras. 11–12 available at: <https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf>; and Manfred Nowak, UN Covenant on Civil and Political Rights - CCPR Commentary, 2<sup>nd</sup> ed, (2005).

<sup>67</sup> See Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet', UN Doc A/HRC/20/L.13, 29 June 2012, para. 1, available at: <https://undocs.org/A/HRC/20/L.13>; and Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue', UN Doc A/HRC/17/27, 16 May 2011, para. 21, available at: [https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf); and General Comment No. 34, at para. 12.

<sup>68</sup> *Ibid.* para. 43; and Human Rights Committee, 'Concluding Observations of the Human Rights Committee: Syrian Arab Republic', UN Doc CCPR/CO/84/SYR, 9 August 2005, para. 13, available at: <https://undocs.org/en/CCPR/CO/84/SYR>.

The UN Human Rights Committee's General Comment No. 34, which elaborates on states' responsibilities under Article 19 of the ICCPR, outlines a three-part test to determine whether a restriction on expression complies with international human rights law. First, the restriction must be provided by law. Second, it must be made in pursuit of one of the purposes laid out in paragraph 3 of Article 19, enumerated exhaustively as: respect of the rights or reputations of others, or protection of national security, public order, public health, or public morals. Third, the restriction must be necessary and proportionate to achieve its protective function.<sup>69</sup>

### Provided by law

Any government action that constitutes a restriction on freedom of expression must be provided by law. This principle is also known as the principle of legality. The restriction must be drafted with objective and precise language so as to avoid granting government authorities arbitrary discretion in enforcing the law.<sup>70</sup> In addition, the law must be precise enough 'to enable an individual to regulate his or her conduct accordingly, and it must be made accessible to the public'.<sup>71</sup>

The internet restrictions enacted by the junta fail to comply with the principle of legality. The Special Rapporteur on the right to freedom of expression has noted that 'Shutdowns ordered pursuant to vaguely formulated laws and regulations ... fail to satisfy the legality requirement'.<sup>72</sup> Section 77 of the Telecommunications Law has been invoked as the basis for the initial restrictions. Section 77 allows for the internet to be restricted 'when an emergency situation arises to operate for public interest'. However, even in cases where the military identified Section 77 as the legal basis for the restrictions, the military has failed to identify the 'emergency situation' that could justify the restrictions, instead stating that blocks occurred for the sake of 'stability'.<sup>73</sup>

The military has failed to publicly disclose the legal basis, if it exists, for subsequent restrictions. Internet shutdowns that do not have an obvious legal basis violate Article 19's requirement of legality. Internet outages in Chad and Gabon in 2016, for example, were deemed presumptively unlawful because in those instances, the internet was blocked repeatedly, and the government did not provide a public explanation for the shutdowns.<sup>74</sup>

Further, the Telecommunications Law itself fails to define what constitutes an 'emergency situation', rendering the legislation impermissibly vague. Attempts by states to 'restrict, control, manipulate and censor content disseminated via the internet', if enacted through vague laws without legal justification, are violations of international law and are dangerous due to the chilling effect these laws have on the right to freedom of expression.<sup>75</sup> Laws that fail to specify under what circumstances authorities may implement internet shutdowns grant

<sup>69</sup> General Comment No. 34, at para. 22.

<sup>70</sup> Alexandre Charles Kiss, 'Permissible Limitations on Rights, in The International Bill of Rights: the Covenant on Civil and Political Rights 290, (Louis Henkin ed, 1981) at 304.

<sup>71</sup> General Comment No. 34, at para. 25.

<sup>72</sup> Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/HRC/35/22, 30 March 2017, para. 10, available at: <https://www.undocs.org/A/HRC/35/22>.

<sup>73</sup> Reuters, 'Myanmar internet providers block Facebook services after government order', 3 February 2021, available at:

<https://www.reuters.com/article/us-myanmar-politics-facebook/myanmar-internet-providers-block-facebook-services-after-government-order-idUSKBN2A32ZE>.

<sup>74</sup> Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/HRC/35/22, 30 March 2017, para. 9, available at: <https://www.undocs.org/A/HRC/35/22>.

<sup>75</sup> *Ibid.*, para. 26.

those authorities unfettered discretion to disrupt internet access. As such, those laws run contrary to international law.

### In pursuit of a legitimate aim

Second, restrictions on expression must be made in pursuance of one of the purposes laid out in Article 19(3) of the ICCPR—that is, to protect the rights or reputations of others, national security, public order (*ordre public*), or public health or morals. The military's repeated instructions to restrict internet access cannot be justified in relation to any legitimate aim. Instead, they have served to exacerbate human rights abuses committed by the military, including murders, enforced disappearances, and arrest and detention of hundreds of civilians, including human rights defenders.

Restrictions on expression are permissible to protect national security only in cases of political or military threat to the territorial integrity or political independence of the entire nation.<sup>76</sup> States may not invoke national security concerns to suppress political debate or criticism of the administration or regime currently in power.<sup>77</sup>

Restrictions are also permissible to maintain the public order (*ordre public*), including restrictions to uphold the public welfare and social order of a state.<sup>78</sup> Because the scope of what could be included within 'public order' is so expansive, legal experts have argued for a strict determination of the necessity and proportionality of any restriction enacted to purportedly maintain the public order.<sup>79</sup> According to the Special Rapporteur on freedom of expression, 'alarm bells ring when States restrict expression relating to matters of the public interest'.<sup>80</sup> The Human Rights Committee has stated that restrictions on expression can never be imposed 'as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets, and human rights'.<sup>81</sup>

Given the context in which they have been implemented, the military's internet restrictions appear designed to violate human rights rather than protect a legitimate interest. The military ramped up internet restrictions as protests were intensifying across the country and in advance of its first uses of violence against protesters. As the weeks since the coup have passed, the military has enacted more granular restrictions that further reveal the true intention behind the restrictions. For example, the military has prioritised 'whitelisting' banking apps and websites that are crucial to the Myanmar economy while continuing to restrict access to social media platforms that facilitate the organisation of protests and news sites that report on the military's human rights violations. Further, the military's restriction of internet access during a press conference put on by the National Unity Government reveals an intent to stop the free flow of political expression in the country.

<sup>76</sup> Alexandre Charles Kiss, 'Permissible Limitations on Rights', at 297.

<sup>77</sup> Manfred Nowak, 'UN Covenant of Civil and Political Rights - CCPR Commentary', at 445.

<sup>78</sup> Alexandre Charles Kiss, 'Permissible Limitations on Rights', at 302.

<sup>79</sup> Manfred Nowak, 'UN Covenant of Civil and Political Rights - CCPR Commentary', at 465–6.

<sup>80</sup> UN General Assembly, 'Promotion and protection of the right to freedom of opinion and expression: Note by the Secretary-General', UN Doc A/71/373, 6 September 2016, para. 26, available at: <https://undocs.org/A/71/373>.

<sup>81</sup> General Comment No. 34, at para. 23; and *Mukong v Cameroon*, Communication No. 458/1991, UN Doc CCPR/C/51/D/458/1991, 10 August 1994, paras. 9.6–7, available at: <https://undocs.org/CCPR/C/51/D/458/1991>.

## Necessary and proportionate

Third, any restriction on expression must be necessary to achieve its protective function, meaning it must be the least intrusive means of achieving the permissible government interest.<sup>82</sup> A restriction is not necessary if the government interest could be achieved in other ways that do not restrict freedom of expression.<sup>83</sup> In addition, the restriction must be proportionate to the interest that is protected by the restriction.

The military's actions to temporarily shut down all access to the internet is intrinsically a violation of human rights law. Internet shutdowns are never necessary or proportionate, and therefore are automatically violations of international law. By their very nature, blanket internet shutdowns do not target specific threats to legitimate government interests and therefore are not necessary or proportionate measures.<sup>84</sup> Moreover, necessity requires a showing that restrictions would achieve the government's purpose. If internet shutdowns disrupt government efforts to maintain public order, they cannot be necessary to uphold public order.

For these reasons, in their 2011 Joint Declaration on Freedom of Expression and the internet, four special rapporteurs on freedom of expression declared, 'Cutting off access to the internet, or parts of the internet, for whole populations or segments of the public (shutting down the internet) can never be justified, including on public order or national security grounds'.<sup>85</sup> In their 2015 Joint Declaration on Freedom of Expression and Responses to Conflict Situations, the same four special rapporteurs stated, 'Filtering of content on the internet, using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law'.<sup>86</sup>

The military's decision to ban a range of websites—from social media platforms to media sites—is likewise not necessary or proportionate. The blocking of websites is an extreme measure. In general, websites should only be blocked by a court or other independent and impartial adjudicatory body that has determined that blocking is necessary and proportionate to a legitimate aim. Those impacted by the blocking, including telecommunications operators, website operators, and civil society organisations should have an opportunity to be heard in court.<sup>87</sup>

The military's move to 'whitelist' certain websites, while generally maintaining restrictions on mobile internet access to all other sites, wholly reverses the legal protections contained in human rights law. This approach represents the most, rather than the least, restrictive method of carrying out the military's goals.

<sup>82</sup> Human Rights Committee, General Comment No. 27, UN Doc CCPR/C/21/Rev.1/Add.9, 1999, Annex VI, Section A; and Alexandre Charles Kiss, 'Permissible Limitations on Rights', at 308.

<sup>83</sup> General Comment No. 34, at para. 34.

<sup>84</sup> Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 16 May 2011, para. 31.

<sup>85</sup> UN Special Rapporteur on Freedom of Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet, 1 June 2011, para. 6(b), available at: <https://www.osce.org/fom/78309>.

<sup>86</sup> ARTICLE 19, 'Joint Declaration on Freedom of Expression and the internet', 22 May 2011, available at: <https://www.article19.org/resources/joint-declaration-freedom-expression-internet/>.

<sup>87</sup> ARTICLE 19, 'Freedom of Expression Unfiltered: How blocking and filtering affect free speech', December 2016, available at: [https://www.article19.org/data/files/medialibrary/38586/Blocking\\_and\\_filtering\\_final.pdf](https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf).

In June 2016, the UN Human Rights Council, in response to a number of States having recently shut down access to the internet or digital communication tools, condemned 'measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law' and called on all States to refrain from and cease such measures.<sup>88</sup> The Human Rights Council's strongly-worded statement reflected the severity of the impact of network shutdowns on the enjoyment of the right to freedom of expression and information.

## RECOMMENDATIONS

### **To the private sector, including internet service providers and social media companies:**

- Advocate for the government of Myanmar to lift internet restrictions and to refrain from enacting new restrictions, including by opposing the proposed Cyber Security Law.
- Consider options for litigation at the national or international level to challenge throttling or shutdown requests.
- Continue to document the ways in which the internet is restricted in Myanmar and undertake to share this information with relevant accountability mechanisms, including the Independent Investigative Mechanism for Myanmar (IIMM).
- Share evidence of human rights violations and international crimes—including government orders relating to internet shutdowns and content removed through content moderation processes—with relevant accountability mechanisms, including the IIMM and international tribunals, and ensure future access by other key stakeholders including civil society and academics.
- Continue to provide free services, such as VPNs, and digital security devices to human rights defenders, journalists, and others.
- Consider ways of expanding affordable internet access, such as through increasing the provision of fixed line connections or introducing discounted high bandwidth data plans available.
- Review corporate policies and operational guidelines on assessing and responding to user data requests by governments and takedown, throttling or internet shutdown orders, including contingencies for what conditions represent legal or ethical red lines, and adopt new policies or guidelines to this end if they do not exist or are not adequate for addressing challenges in contexts like Myanmar.
- Ensure that corporate transparency reports on Myanmar include the number of government requests for user data; the number of takedown requests for individual posts, accounts, or other user generated content; the number of internet throttling or shutdown orders; the corporate policies relevant to such requests; and the measures taken to resist orders that violate human rights. Where possible, such information should also include the legal basis used by authorities for issuing such requests.
- Invest appropriate resources to speed up the localisation of circumvention and security tools along with and relevant FAQ or guidebooks in Myanmar languages, including ethnic minority languages such as Kachin and Shan.
- Assess financial losses caused by internet disruptions in Myanmar and consider making the result publicly available.

<sup>88</sup> Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet', UN Doc A/HRC/32/L.20, 27 June 2016, para. 10, available at: <https://undocs.org/A/HRC/32/L.20>.



- Ensure the hiring of employees with linguistic and cultural knowledge sufficient to guarantee effective, strategic, and appropriate decision-making relating to Myanmar.

**To States:**

- Continue to raise concerns about ongoing restrictions in all relevant fora, including bilaterally and through human rights and trade mechanisms.
- In all diplomatic engagement with the Myanmar government, systematically integrate the issue of digital censorship and surveillance, internet throttling, and shutdowns.
- Ensure regional and international foreign policy alignment in diplomatic engagement with other actors that oppose internet throttling and shutdowns.
- Investigate whether internet disruption and shutdown-related economic harms constitute non-tariff barriers to trade or other trade-related violations and consider remedies for such violations.
- Continue to provide funding to Myanmar civil society organisations in country and in exile, adopting creative solutions to address the increasingly limited operating space.
- Ban the export to Myanmar of technologies, including 'dual-use' technologies, that could be used to surveil or otherwise repress the population, and where relevant halt licensing and software updates or any other support services for technology already possessed by the Myanmar authorities.

**To United Nations bodies:**

- Improve effective coordination across UN agencies on matters of human rights and internet censorship, surveillance, throttling, and shutdowns, such as aligning the work of the International Telecommunications Union with the Office of the High Commissioner for Human Rights and others.
- Consider greater inter-agency analysis of internet throttling and shutdowns as relate to violations of international criminal law, including crimes against humanity, war crimes, and genocide as defined by the Rome Statute.
- Enhance the role of the Secretary General's Envoy on Technology to ensure greater coordination among UN agencies and to provide expert guidance to member states.