Myanmar Coup and Internet Shutdowns

Overview

On 1 February 2021, the Myanmar military junta, alleging widespread voter fraud staged a coup and took political control of the country. They did so after months-long refusal to accept the National League for Democracy’s (NLD) victory in the 2020 general election (Reuters, 2021). A one-year public emergency was declared under section 417 of the 2008 Constitution. Since 1 February, the military junta has shut down the internet, blocked access to online sites, disabled mobile internet access, closed down media companies and arrested online dissenters and journalists as the protests continue into April 2021. There has been an intensification of internet and media control with the aim of crippling the protests and halting the spread of pictures and videos of security personnel using disproportionate force against protestors. What we see in Myanmar is a shift in tactics by the military junta from internet content censorship to infrastructure control.

Myanmar

Internet Statistics

2021

<table>
<thead>
<tr>
<th>Population</th>
<th>54,610,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Penetration</td>
<td>43.3% (23,650,000)</td>
</tr>
<tr>
<td>Social Media Penetration</td>
<td>53.1% (29,000,000)</td>
</tr>
<tr>
<td>Mobile Connectivity</td>
<td>127.2% (69,430,000)</td>
</tr>
</tbody>
</table>

Source: Compiled from We Are Social (2021)

Internet Shutdowns

On the day of the coup, the Myanmar Times reported: “access to TV channels, phone lines and Internet service have been cut” (Kang, 2021). The Tatmadaw imposed internet shutdowns across major cities such as Naypyidaw, Yangon, and Mandalay. Using Section 77 of the country’s Telecommunication Law (2013), the military junta compelled Telcos and Internet Service Providers (ISPs) such as Telenor Myanmar, Ooredoo Myanmar, Myanmar Post and Telecommunication (MPT), Mytel, Welink, 5BB and Frontiiir to adhere to their demands of service disruption. The Section gives the government the authority to direct ISPs to “suspend a telecommunication service or restrict specific forms of communication” on the occurrence of public emergency (Telecommunications Law, 2013).
From 3 to 5 February, the Ministry of Transport and Communication issued a ban asking telecommunication operators to block access to social media platforms including Facebook, Telenor, Instagram, FB Messenger and WhatsApp until 7 February, citing the necessity to guarantee public security (Telenor, 2021). UK-based internet rights monitoring group NetBlocks revealed the internet disruptions during 1 February to 7 February showing the below-average connectivity, between 50% to 75% lower than ordinary levels (Netblocks, 2021).

Since 15 February, the Ministry of Transport and Communication imposed nationwide internet outages from 1 AM to 9 AM with connectivity at 14%-15% of ordinary levels. On 18 February, all language editions of Wikipedia, Wikimedia, and wikidata were blocked to ban the use of some certain words which referred to coup d’etat and pro-democracy movements. Such restriction also prevented editing online articles of those platforms, particularly in relation to the General Min Aung Hlaing’s biography, so-called an “edit war” (Netblocks, 2021).
Telecommunication controls intensified on 15 March, when the Ministry of Transport and Communication disabled mobile data nationwide. Since then, at 7 PM every night, letters ordering internet shutdown, with daily lists of VPNs to be banned, would be sent to the telecommunication companies (Myanmar Now). This was followed by, on the 18 March, a disruption to the publicly available WiFi networks. On 23 March, the military junta reaffirmed their intention to keep the internet banned in the country, citing violence and unrest being encouraged online, and blamed the media for fanning the nationwide protest. As of 31 March 2021, Myanmar people have had no access to the mobile data for 15 consecutive days, 12 days with intermittent WiFi networks and the 43rd night without internet access.

The internet shutdowns, the blocking of online access, disabling of mobile data and connectivity, following the February 2021 coup, are the latest in Myanmar. Earlier, in June 2019, internet shutdowns were imposed in Rakhine and Chin states. These states have experienced the longest suspension of internet service in the world.

Globally, regionally and nationally individuals and groups have condemned the internet shutdowns. Yet, the government continues to forestall online protests, manifestations and coordination.

**MEDIA FREEDOMS**

On 2 February 2021, a day after the coup, the newly appointed Minister of Information issued a public warning that some media outlets “were spreading false rumours and statements which can cause unrest”. In a statement to the Myanmar Press Council, the Ministry of Information instructed the media against using “incorrect words” such as coup and referring to the military as a “junta” or “regime” (Bangkok Post, 2021). As the internet shutdown was imposed, journalists tried to use mobile phones to record incidents and protests rather than cameras to avoid attracting attention from the security force. They also exercised extra caution when handling sensitive data such as notes and recordings as these can be used to implicate them for violating the law. On 9 March, the military moved from public warnings to closing media outlets, ordering 5 independent media companies/organisations to shut down (7 Day News, Democratic Voice of Burma, Khit Thit News, Mizzima and Myanmar Now). Under the order, media organisations would be deemed to be breaking the law if they continued to “publish or broadcast articles, programmes or reports or transmit messages via social media” (RSF, 2021). On the same date, Myanmar Now’s office also suffered a raid from the authorities, who forced their way in and seized documents and office materials. According to Reporting ASEAN, as of 27 March, a total of 55 journalists were arrested, 25 of which remained in custody. Most were charged under Article 505(b) for spreading falsehood causing public mischief.

**Responses to the Internet Shutdowns**

There have been speculations as to why the nightly internet shutdowns since mid-February 2021. Apart from the initial argument that this was to slow down the mobilisation of the protests, other explanations range from the military junta installing new surveillance technology to slowing down the data over the to study the protest communications over social media (Al Jazeera, 2021). Nevertheless, these internet shutdowns, blocking of access to specific sites, crippling mobile data and connectivity has met with responses from the protesters, technology companies and the international community.
1. Protestors

In the first few days of the military takeover, the general populace responded to the coup with symbolic, sporadic protests, while discontent and attempts to organize anti-coup assemblies were manifested on Facebook. Online protest-mobilising content shifted to Twitter after Facebook was blocked on 3 February. Hashtags such as #RespectOurVotes, #HearTheVoiceofMyanmar, and #SaveMyanmar became rallying points (Potkin, 2021). On 6 February, after all access to social media platforms were denied, people took to the streets en masse in Naypyidaw, Yangon, Mandalay, and Bago to protest against the military junta. People have used virtual private networks (VPN) that enable circumventing Internet restrictions to gain access to Facebook and Twitter or they have migrated to other social media platforms such as WhatsApp and Signal. Some also created SMS groups or made landline calls to update each other (Chew, 2021). Ingeniously, Bridgefy, a Bluetooth-based messaging application came to the rescue for the protesters, using Mesh Networks to communicate without internet connections (The Straits Times, 2021). Though limited in range around 100 metres, it bypasses the cell tower and the necessity to connect to the mobile network by opting for a direct peer-to-peer channel.

On 17 February, a group of tech-savvy local hackers Myanmar Hackers took down the websites of government institutions and government related entities such as the Central Bank of Myanmar, Port Authority, Food and Drug Administration, military-run Tatmadaw True News Information Team, Myawady TV and state-own Myanmar Radio and Television. Myanmar Hacker would be joined by the infamous international hacking group Anonymous who, from 4 - 12 March, continued to disrupt government sites helping the protesters. Since Facebook, Twitter and Instagram was banned in the first week of February, local people have mainly used the virtual private networks (VPN) to gain access to social media platforms and contents that were otherwise denied access. According to the independent research group Top10VPN, the usage of VPN surged by 7,200% in Myanmar. With regards to the regular internet curfew, as most local protesters are not active at night, this has not affected the political activism much. In any case, young people have adjusted to their new lifestyle with the disruptions to the internet access. Some of them have used Thailand’s Sim2fly AIS—a data roaming SIM card which would rout data to the AIS telecommunication firm’s data centre in Bangkok—for 24 hours internet access, others have adopted a self-learned approach and turn to a variety of alternative social media applications such as Bridgefy, Telegram, FireChat to skirt around the internet shutdown. Internet/ networking hopping, using mobile hotspots connecting one cellphone to another within a given radius, is also being employed by the protesters.

2. Technology Companies

While complying with the government’s directive to block the internet and access to social media platforms, technology companies also issued statements and took several actions.

Telenor group considered the order a human rights violation and contradictory to the principles of necessity and proportionality of international human rights standards. Twitter, in response to the military’s crackdown on social media, stated it was deeply concerned by the decision and that the order “undermines the public conversation and the rights of people to make their voices heard” (Reuters, 2021).
Earlier on 3 February, Facebook classified Myanmar as “Temporary High-Risk Location,” an action which allows removal of content or events in a country that involve “any calls to bring armaments” and protect online discussion that criticizes the military coup (Nashrulla and Mac, 2021). Facebook, which owns Instagram and WhatsApp, acknowledged disruptions to their services in Myanmar and urged the authorities to restore access to its platforms. On 12 February 2021, Facebook restricted circulation of contents on Facebook accounts and profiles run by the military on the grounds that these pages have spread disinformation (Disis, 2021). This action means that Facebook users will considerably see less content from those pages on their News Feed.

**Responses from Technology Companies (February, 2021)**

- **3 Feb**: Telenor Group issued a statement expressing their grave concerns over MoTC’s order to block access to social media platforms.
- **6 Feb**: Facebook designated Myanmar as a “Temporary High-Risk Location”.
- **12 Feb**: Twitter expressed concerns over the blockage of its service in Myanmar.
- **24 Feb**: Facebook and Instagram banned all the Myanmar military accounts, including other military-controlled pages on their platforms.

*Source: Compiled from media reports*

On 24 February, Facebook announced a ban on Myanmar military and its entities accounts and Pages from Facebook and Instagram, including advertising from military-linked commercial entities. The guidance for its ban was from the UN Fact-Finding Mission on Myanmar’s 2019 report, on the economic interests of the Tatmadaw, and the obligation under the UN Guiding Principles on Business and Human Rights. Its decision was based on four reasons: (1) the past severe human rights abuses and the risk of future military violence in Myanmar had been committed by the Tatmadaw; (2) its contents and behaviors had frequently violated Facebook policies; (3) since the February 1 coup, its behaviors and contents had violated Facebook policies, particularly violence and incitement and coordinating harm policies, which were previously removed by Facebook; and (4) such behaviors considerably increased danger and possibly shifted online threats to offline harm (About Facebook, 2021).

On 4 March, TikTok started banning some accounts used by Myanmar’s military personnel. After Facebook, Twitter and other social media platforms were banned in the country, the Tatmadaw resorted to TikTok to deliver death threats, hate speech and violence towards the protesters. Spokesperson of TikTok expressed that “the promotion of hate, violence, and misinformation has absolutely no place on TikTok....and the firm will continue to make a significant investment to respond to new threats in order to keep TikTok in Myanmar a safe platform”
On 23 March 2021, Global System for Mobile Communications (GSMA), a telecommunication industry association, urged Myanmar authorities to restore internet access. In the statement, it said “governments should only resort to service restriction orders in exceptional and pre-defined circumstances, and only if absolutely necessary to attain specified and legitimate aims consistent with internationally-recognised human rights and relevant laws”.

Meanwhile, the U.S. trade suspension announced on 29 March 2021 stands to affect U.S. cloud companies providing services to users in Myanmar. However, it is unclear how precisely this will interfere with internet and social media usage in Myanmar (Whittaker, 2021).

3. International Community
The UN, break-away Myanmar ambassadors, individual governments, regional blocs such as the EU and ASEAN have issued statements and expressed concern over developments in Myanmar. When making such statements, they sometimes refer to the impact on freedom of expression and internet freedoms but more explicit statements are needed.

On 15 February, the Secretary-General of the United Nations, António Guterres, called for respect of the right to freedom of expression and insisted that internet access and communication must not be disrupted. He also appointed the Special Envoy, Christine Schraner Burgener, to assess the situation in Myanmar (UN News, 2021). During the discussion between the Special Envoy and the Myanmar army’s Deputy Commander-in-Chief, Soe Win, she cautioned him that internet shutdowns certainly impaired the democratic principles, negatively affected essential infrastructure and sectors, and led to higher tensions in Myanmar (The Business Times, 2021). Additionally, the United Nations Special Rapporteur on the situation of human rights in Myanmar, Tom Andrews, blamed Military’s actions towards protesters, including massive arrests, attacks during the late nights, and internet shutdowns, and warned the Military commanders to be responsible (Bangkok Post, 2021).

On 19 March, Ambassadors to Myanmar from the Delegation of the European Union (EU) and EU Member States—Denmark, Czech Republic, Finland, France, Germany, Italy, Netherlands, Spain, & Sweden—the United Kingdom and the United States issued a joint statement calling on the Tatmadaw to cease all violence against unarmed civilians and peaceful protesters. The statement also reaffirms the delegations’ support towards the rights to peaceful assembly of the people of Myanmar and their rights to freely access information, emphasizing that “internet blackouts and the suppression of the media will not hide the military’s abhorrent actions”.

Countries, such as the US, UK, EU have come out strongly calling for a reversal of the coup, condemning the junta, to introducing targeted sanction against the generals. Others such as Australia, South Korea, Japan and New Zealand have added their voices. In ASEAN, Indonesian President Joko Widodo called for democracy to be restored and violence stopped in Myanmar, and urged Brunei as the current Chair of ASEAN to convene an ASEAN high-level meeting on the Myanmar crisis, involving all ASEAN leaders. However, calls to guarantee and protect internet freedoms have not been made explicit.
Legal Analysis
To understand the junta’s control over the internet, the Constitution and other laws are important to understand the censorship regime in Myanmar. The Constitution sets the scope for individual freedoms and redress which was negated by the coup. The Telecommunication Law was used to immediately shut down the internet. Thereafter, amendments to existing laws further removed rights and protection. The amendments approach was taken after measures to control the internet through the leaked draft Cybersecurity Bill was met with widespread criticism. Presently the Bill has not made any legal progress but in the meantime, the junta has quietly introduced a series of amendments that includes elements of the Cybersecurity Bill into the Electronic Transactions Law, or suspension of protective clauses that safeguard individuals’ rights in the Law Protecting the Privacy and Security of Citizens.

Laws Impacting Internet Freedoms

<table>
<thead>
<tr>
<th>Constitution Article 379 and 381</th>
<th>Citizen redress denied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecommunications Law Section 77</td>
<td>Possible suspension or revocation of license of service provider</td>
</tr>
</tbody>
</table>

Amendment to Existing Laws During the Coup

<table>
<thead>
<tr>
<th>Law Protecting the Privacy and Security of Citizens</th>
<th>Suspend the sections protecting citizen from abuse of power as long as the SAC is in power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Transactions Law</td>
<td>Introduce an exception allowing officials to confiscate personal data, and prohibit sharing various types of information online</td>
</tr>
</tbody>
</table>

Source: Compile from legal document
1. Constitution

The Constitution of Myanmar, in Article 354, guarantees that “every citizen” shall be at liberty in the exercise of the following rights, if not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility or public order and morality:

(a) to express and publish freely their convictions and opinions;
(b) to assemble peacefully without arms and holding procession;
(c) to form associations and organizations;

However, the suspension of rights of citizens under the Constitution may take place, as per Article 379, only “in time of war,” “in time of foreign invasion” and “in time of insurrection”. (Constitution of Myanmar 2008) In these situations, citizens may be denied redress as per Article 381. The constitution prescribes in Article 383 vaguely worded duties every citizen must uphold: “[a] non-disintegration of the Union; (b) non-disintegration of national solidarity; (c) perpetuation of sovereignty” (Constitution of Myanmar, 2008).

A State of Emergency can be imposed by “The President” under section 417, pursuant to Section 410. The latter stipulates that the Emergency is to be promulgated “If the President learns [of a situation warranting a public emergency] he may, after coordinating with the National Defence and Security Council, promulgate an ordinance and declare a state of emergency” (Constitution of Myanmar, 2008; emphasis added).

In the current case, the President of the elected, civilian authorities did not perform this function. The military staged a coup under the guise of an alleged public emergency and the President was detained, along with other top civilian leaders.

The coup d’état came months after the November 2020 election, with no threat to sovereignty, or insurrection during the time prior to the coup that could pose an existential problem for the Union. Section 417 of the 2008 Constitution states that for a state of emergency to be justified, there must be “sufficient reason” that conditions have arisen that may “disintegrate the Union, disintegrate national solidarity”, and “cause loss of sovereignty of the Union by insurgency, violence and wrongful forcible means” (Government of Myanmar, 2008). This was not the case.

2. Telecommunications Laws

Internet shutdowns, in fact, is nothing new in Myanmar. Previously, it had been imposed in conflict zones, such as in Rakhine and Chin states, where armed minority groups frequently clashed with the Tatmadaw. National security is always cited as the main reason behind the decision to impose internet outage. Disruption to telecommunication networks and internet is usually activated by invoking Section 77 of the Telecommunications Law which states that:

The Ministry of Communications and Information Technology may, 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 Equipment (Government of Myanmar, 2013).
Following the coup, especially after February 6, when resistance to military takeover began to form and mass protests started to take shape, MoTC has sent letters to telecommunications firms to shut down the internet to disrupt protesters’ ability to organize themselves. From 15 February onwards, claiming violence and unrest were being encouraged on the internet, the military imposed internet curfews at night, which often coincides with night raids targeted at journalists, NLD politicians and protesters.

3. Cybersecurity Bill
After staging the coup, on 9 February 2021, the State Administration Council sent the Draft Cybersecurity 2021 Law to telecommunications companies in Myanmar, asking for input on the draft law by 15 February. The draft bill would later be leaked to the media and civil society members. Under Article 29, the government had the right to impose “interception, removal, destruction or cessation” of one’s account, when contents are deemed as (per a very vaguely worded clause) “causing hate or disrupting unity, stabilization and peace,” any “disinformation, or any comment violating any existing law”.

Under this law, those found guilty of breaking it will be punished with up to 3 years imprisonment and a fine of $US 7,500. (RSF, 2021) Article 30 of the draft bill prescribed that online service providers must, when requested, hand over to the government “the user’s name, IP address, phone number, ID card number and physical address” (RSF, 2021). Article 31 stipulates that an online service provider in Myanmar “may provide all or part of the information contained in Section 30 if the assigned person or authorized organization [is] requested under any existing law”.

The draft law drew criticisms from international communities for its overly-broad provisions that could be used to stifle freedom of expression and criminalize government critics, and the lack of transparency.

4. Amends to Existing Laws
On 15 February, two weeks after the coup, the State Administration Council amended the Law Protecting the Privacy and Security of Citizens, known locally as the Privacy Law. Essentially, the amendment expanded the scope of actions that could be taken by authorities to conduct search, seizure of equipment, arrest and detention; this also includes interception of telecommunication, investigation and surveillance activities without judicial oversight. Section 8 of the Privacy Law stipulates the prohibitive actions on the state authorities as followed:

“In the absence of an order, permission, or warrant issued in accordance with existing law, or permission from the Union President or the Union Cabinet, a Responsible Authority:

1. Shall not enter into a citizen’s private residence or a room used as a residence, or a building, compound or building in a compound, for the purpose of search, seizure, or arrest.
2. Shall not surveil, spy upon, or investigate any citizen in a manner which could disturb their privacy and security or affect their dignity.
3. Shall not intercept or disturb any citizen’s communication with another person or communications equipment in any way.
4. Shall not demand or obtain personal telephonic and electronic communications data from telecommunication operators.
5. Shall not open, search, seize or destroy another person’s private correspondence, envelope, package or parcel.
6. Shall not unlawfully interfere with a citizen’s personal or family matters or act in any way to slander or harm their reputation.
7. Shall not unlawfully seize the lawfully owned movable or immovable property of a citizen, or intentionally destroy it either directly or by indirect means.”

By suspending Section 8, the actions mentioned above are now permissible and legal when carried out by government officials. The interception of communications and obtaining personal data from telecommunication and technology firms would prove most damaging to freedom of expression and internet freedoms in Myanmar.


On 15 February, an amendment to the Electronic Transactions Law was made to include vaguely-worded provisions allowing the government to confiscate personal data and outlaw the act of sharing online information. It is important to note that some elements of Draft Cybersecurity Law have been incorporated into this amendment.

For example, under Chapter 10 of the Electronic Transactions Law, a new clause, Section 27(c), was added to provide for an exception to the safeguarding of personal data in the occurrence of “detecting, investigating, organizing of information, verifying the information conducted in accordance with management power on the cyber security and cybercrime matters relating to stability, tranquility, national security of the state”. This addition is almost “copied and pasted” from the Chapter 6 (Personal Information Management) of the Draft Cybersecurity Law, which drew criticisms from the public and international human rights organizations. Meanwhile, under the newly amended Section 38(c), it is a punishable offense with up to three year imprisonment and/or a fine of $US 7,000 for those “who, at the cyberspace, commits creating false news or fake news with the intention to cause public panic, to lost trust, to lower the dignity by public or to destroy the unity of any association”. Apart from the amount of fine, Section 38(c) is almost a word-by-word duplication of Article 64 of the Draft Cybersecurity Law.

The 2021 military coup in February has severely affected internet freedoms in Myanmar. With the Constitution suspended, marshalling of the Telecommunications Law to deny access to the internet and social media, proposing a Cybersecurity Bill which contains prohibitive sanctions and sneaking some of those sanctions by amending the Law Protecting the Privacy and Security of Citizens and the Electronic Transactions Law all go against international standards that guarantee freedom of expression.
International Obligations

General Comment 34 (2011) of the Human Rights Committee stipulates that freedom of expression and opinion are guaranteed under the ICCPR both offline and online (OHCHR, 2011).

In situations of conflict, a 2015 joint declaration on freedom of expression by special rapporteurs from African, American and European human rights mechanisms stated that “using communications ‘kill switches’ (i.e. shutting down entire parts of communications systems)... can never be justified under human rights law.” (OHCHR, 2015)

The United Nations Human Rights Council further made it clear in its resolution 32 of 27 June 2016, “that the same rights that people have offline must also be protected online, in particular freedom of expression” in accordance with Article 19 of the ICCPR (UNHRC, 2016).

In the context of the Myanmar coup, on 4 February 2021, the United Nations Security Council (UNSC) expressed “concern at the restrictions on civil society, journalists and media workers”. The Council called upon the military junta to “fully respect human rights, fundamental freedoms and the rule of law” (UNSC, 2021).

The UN Special Rapporteur on the Situation of Human Rights in Myanmar, in a special session of the UN Human Rights Council on 12 February 2021, noted:

The junta is instituting regulations and laws to systematically abrogate the people’s rights of freedom of expression, access to information and privacy. ... It has blocked Facebook and other apps, cut off the Internet as it sees fits, and has put forward a new draconian Cyber Security Law to assure that Myanmar is truly a police state that uses modern technology to harass, intimidate and arrest anyone who stands in their way. The new law would allow the junta to ban content it dislikes, restrict Internet providers and intercept data. (OHCHR, 2021).

In short, the legal instruments used by Myanmar to curb internet freedoms are not aligned with international norms and standards. Instead, the coup has brought the entire communications infrastructure and all forms of media under strict control of the military junta, in an already highly centralised political context of Myanmar.

Conclusion

Since 1 February 2021, the junta has progressively throttled down on internet freedoms and privacy in an attempt to disrupt the organisation of the protests, address the reputation damage caused by digital images of security force violence against protestors and to control overall public opinion around the coup. Hence, condemnation of the junta and calls to stop the violence should also include calls to ensure internet freedoms are protected so that access to information can be maintained. Throughout the coup, the internet has served as an archive documenting both the use of force against protestors as well as recording the countless acts of resistance. Without the internet, it would lead to an absence of critical information that would shield the military junta from scrutiny, sanction and eventually punishments.
Bibliography


International Centre for Not-for-Profit Law (2021), The Situation in Myanmar: Draft Cyber Security Law and Other Threats to Fundamental Freedoms.


