SURVIVING MYANMAR’S DIGITAL COUP
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>The military’s “digital coup”</td>
<td>11</td>
</tr>
<tr>
<td>Online Communities</td>
<td>21</td>
</tr>
<tr>
<td>The response of social media</td>
<td>28</td>
</tr>
<tr>
<td>Self-censorship</td>
<td>35</td>
</tr>
<tr>
<td>Conclusion</td>
<td>42</td>
</tr>
<tr>
<td>About FEM</td>
<td>44</td>
</tr>
</tbody>
</table>
Executive Summary

In the early hours of 1 February 2021, the Myanmar military launched a coup to depose the newly elected government. The military’s offline offensive was accompanied by a digital coup intended to prevent people from learning about, objecting to, and organising against the military’s unlawful act.

The digital coup has violated many human rights, including the rights to freedom of expression, information, media, association, non-discrimination, assembly, privacy, and liberty.

This report reveals the lived experiences of censorship among Myanmar’s most active online dissenters working under the digital coup, including journalists, human rights defenders, bloggers, activists, students, and others. It complements other publications focused on dissenters’ courageous responses, and more general or technical assessments of the digital coup, including FEM’s annual “Freedom on the Net” reports.

Dissenters experienced disconnection right from the start of the coup as the military shut down internet access, blocked social media, and banned mainstream media outlets. Dissenters were forced underground or into exile following military campaigns of surveillance, interception, hacking, extrajudicial violence, and arbitrary criminalisation of online activities.

The military quickly extended its battlefield online, threatening dissenters with digital dangers including coordinated trolling, cyberstalking, and “doxing”, with serious offline consequences. The extended battlefield ignored offline consequences. The extended battlefield ignored territorial limits, threatening dissenters everywhere.

Social media platforms’ responses were mixed; some under-moderated deeply problematic content such as harassment and incitement, and others over-moderated and censored public debate. Many dissenters were particularly concerned about platforms censoring the brutal reality of conflict.

Dissenters felt traumatised with heightened feelings of fear, anxiety, guilt, and depression, all of which contributed to widespread self-censorship online,
Free Expression Myanmar - Page 3

The military’s digital coup has failed so far but its attempt to resurrect a “discipline-flourishing” internet and impose it upon dissenters, online communities, platforms, and internet infrastructure, continues. The online space is critical for dissenters to defend against the military and restore the democratic transition, and vigilance is required to constantly protect it.
**Recommendations**

**Future governments**

- Consult widely and adopt commitments and plans to protect digital rights. These plans should include new progressive laws, bans on internet shutdowns and arbitrary website blocks, a ban on arbitrary digital surveillance, and ratification of international human rights treaties.

- Prioritise and make real commitments to providing justice and appropriate remedies to all those whose digital rights have been violated.

**Digital businesses (including telecoms operators, social media platforms, internet service providers, technologists)**

- Endorse and abide by the UN Guiding Principles on Business and Human Rights. Specifically, conduct proper due diligence before decision-making.

- Adopt, continuously develop, and implement Myanmar-specific policies that recognise contextual needs such as enhanced digital security, increased support for anonymity, smarter conflict-sensitive moderation, and greater access to reliable public interest information. Facebook in particular should invest more in reducing over-moderation. Telegram in particular should address widespread abuse by dangerous organisations and individuals.

- Refuse and subvert the military’s attempts to create a so-called “discipline-flourishing” internet. Identify digital issues in any of the military’s new proposed laws or policies, and advocate for reform.

- If operating from a physical location under military authority, interpret all military orders in the narrowest way possible to ensure the least harm to digital rights.

**Civil society**

- Increase general public awareness of digital security with an emphasis upon safer digital use rather than self-censorship. Ensure awareness raising efforts are accessible to diverse communities.
Embrace and encourage encryption, anonymity, and other digital technologies with the aim of defending civic space and ensuring robust public debate continues online.

**International community**

- Hold digital businesses, including social media platforms and technologists developing surveillance capabilities, accountable to their human rights obligations internationally. Encourage digital businesses to endorse and abide by the UN Guiding Principles on Business and Human Rights. Reflect on businesses’ international performance under the Principles when deciding on future contracts.
- Highlight, condemn, and sanction any foreign State, or foreign business, that provides support, knowledge, or equipment that encourages or facilitates violations of digital rights in Myanmar.
- Recognise the importance of the digital space by providing financial support to civil society and technologists seeking to defend digital rights in Myanmar.
In 1988, the Myanmar military detained opposition leaders, invoked martial law, violently suppressed protests, established a “council”, and launched a propaganda campaign to justify their coup “in the people’s interests”. 33 years later on 1 February 2021, the military repeated it all once again but with an additional “digital coup” aimed at oppressing online dissent.

FEM set out to investigate the lived experiences of the “digital coup” among human rights defenders, journalists, bloggers, activists, and other dissenters trying to counter the military.

In particular, FEM wanted to analyse how dissenters experienced the military’s digital coup, the behaviour and attitude of online communities, social media platforms’ responses, and the depth of any digital self-censorship.

This report accompanies FEM and Freedom House’s publication, Freedom on the Net, published in October 2022 assessing internet freedom using a range of comparative global indicators.
Methodology

This report is based on research and 24 structured key informant interviews with senior human rights defenders, journalists, and political activists from Myanmar carried out between September 2022 and March 2023. Interviewees were selected to be representative of those most at risk from the digital coup, including women and members of ethnic minorities.

Each interview was an interactive discussion structured around 97 questions across four themes: the military-controlled State; social media platforms; online communities; and self-censorship.

As a human rights organisation, FEM intentionally sought to identify discriminatory policies and practices and used disaggregation to look for differences in the opinions and experiences of marginalised groups. Differences are flagged in the report whenever they were apparent in the research.
<table>
<thead>
<tr>
<th>Participant demographics</th>
</tr>
</thead>
<tbody>
<tr>
<td>50% women</td>
</tr>
</tbody>
</table>

| 38% aged 19-29 | 29% aged 30-39 | 21% aged 40-49 | 13% aged above 50 |

| 42% journalists | 38% human rights defenders | 4% armed group supporters | 13% non-aligned activists, development workers, and digital technologists |

| 96% were in Myanmar before the coup began |

| 42% remain in Myanmar | 58% have moved into exile since the coup began |

**Limitations**

FEM selected interviewees at risk from the military. In many cases, the lived experiences of these individuals would be representative of the public at large, and any findings could be broadly generalisable, but this will not always be the case as some may be an extreme or exaggerated experience of only those at greatest risk.
The military

FEM has referred to “the military” throughout as shorthand for a complex institution that not only includes the military but also military-owned and allied businesses, and military-controlled government ministries, all of which contribute to enabling the digital coup. The military’s State Administration Council (SAC) may be accountable for the digital coup, but FEM regards military officers, military business leaders, cronies, and senior government officials as complicit, and therefore all included within “the military”.

The military’s coup was immoral and unconstitutional. Nevertheless, the military unlawfully controls large parts of the State, including government ministries and the courts. Any referral to unlawfully adopted “laws” or unlawfully-controlled government ministries is not an endorsement of the military’s legitimacy.
100% experienced threats or limitations to their internet access

58% received a verbal or written warning because of their online activities

42% received violent warnings for their online dissent

29% detained, arrested, charged, prosecuted, fined, imprisoned, sued

36% believed that they had been subjected to digital surveillance

29% had websites, social media accounts, or emails hacked

91% used VPNs to access blocked websites and social media platforms

91% taken steps to circumvent the military’s digital surveillance
There have been three phases of the military’s digital coup. The first phase was like a hammer shutting down access to the internet for all. Next came the search-and-destroy phase in which the military began to reopen limited and irregular internet access while identifying and silencing dissenters. The third and current phase has been using digital to increase overt and covert surveillance intended to strike fear into the public.

Disconnected in the dark

The military’s digital coup disconnected people from each other and from the news that affected their lives.

The military initiated “blanket censorship” through widespread internet shutdowns right from the start of the coup (M10). 100% of participants had experienced threats or limitations to their internet access. One participant summarised most people’s feelings at the time: “I felt like I was in hell. I did not know what was happening outside. I was in the dark” (M13).

For months after the coup began, many people only received basic information about what was happening via short SMS messages (AG26). According to one participant, the whole country felt the impact of being disconnected by shutdowns and as a result could “empathise with those in remote areas” such as Rakhine and Chin States where previous shutdowns had been used as a tool to conceal human rights abuses (M13).

Shutdowns decreased in scale over the following months. However, they continued for many people living outside of major cities (A11, M27). One participant remarked: "There is still no internet at all in our remote area and we need to climb up to hilly places every day just to get a signal, and even then, a really slow one" (A15). Accessing the internet in the Sagaing Region, which has faced some
The military’s doubling of data prices was particularly challenging for many people. One participant remarked: “The increase in data tariffs is clearly intended as a barrier to stop many of us using the internet” (AI16).

With businesses, particularly banks, struggling to operate without internet access, the military shifted their digital coup strategy away from blanket shutdowns towards website and social media blocks. One participant said that this continued to have a similar effect: “We could not use Facebook and as a result, the flow of information disappeared” (M13).

People learnt that they needed access to VPN software to access Facebook (AG26, AG9). 91% of participants used VPNs to access blocked websites and social media platforms. But free VPNs were slow and the military tried to block them (AG7). 65% of participants experienced problems using VPNs. Some people continued to use VPNs and others stopped, fearing the military’s VPN ban and their random searches of devices (AG19).

“I felt like I was in hell. I did not know what was happening outside. I was in the dark”
Media targeted

The military targeted the media in an attempt to control and censor public debate and sharing online.

63% of participants experienced some form of digital censorship by the military. The media came under particularly severe pressure. Participating journalists remarked that the military’s subservants at first began warning the media to “be careful” (O1). Public officials ominously requested journalists to “talk to us before publishing news” (M20). Independent newspapers, terrestrial television, and FM radio channels moved entirely online almost overnight.

The military soon stopped giving warnings to the media and started making demands (O21). One participant said that the General Administration Department began telling media outlets to “delete your articles” from websites and social media (M21). The Department also used ethnic group leaders to pressure outlets to delete content (M20, O20). Another participant reported that they were ordered to delete photos and videos (M1). The military was particularly concerned with reports on “attacks against civilians and women” (O19).

Refusals were met with the threat of prosecution (V20). The military also threatened international media journalists (AB19). One participant observed that within days of the coup starting “journalism had become a crime” (M19). The military soon began raiding the empty offices of media outlets, which had by then gone entirely
Unable to immediately find and control the media, the military blacklisted and blocked the websites of almost all independent media outlets (M6). 33% of participants had been unable to access their websites blocked or slowed. Participating journalists noted that public officials also became terrified to talk with journalists from those blacklisted outlets (X5).
Punishing online dissent

The military attacked and criminalised activists and others leading online dissent.

The military captured just a small number of dissenters in the immediate aftermath of the coup, most of them older political leaders. It later began to hunt the many other dissenters, including political activists, human rights defenders, civil society leaders, artists, celebrities, students, journalists, and unionists, many of whom had gone underground and predominantly worked online.

58% of participants had received a verbal or written warning from the military because of their online activities. 57% of those warnings included a demand to stop, delete, or change online activities. Less threatening warnings were given to those people whose criticism of the State was not directly related to the coup (M14).

The military used a range of tactics to find and capture dissenters. In many cases, the military interrogated and threatened the dissenter’s friends and family (BT20, O11). In others, they just blantly called the dissenter and asked them where they were (AM2).

29% of participants had been detained, arrested, charged, prosecuted, fined, imprisoned, sued, or otherwise faced legal sanctions because of their online activities. One participant explained: “The military published warrants for my arrest in at least three townships, all of which used my profile photo and personal information taken from Facebook” (O12). Participants faced prosecution for their online dissent under several laws including the Penal Code (Q5), the Telecommunications Law (Q21), and the Printing and Publishing Law (Q9). Some participants had their homes confiscated (AR9, O11, AR5).

42% of participants had received violent warnings for their online dissent from the military and its subservients. One participant revealed: “They said that they will kill me” (Q19). Another forewarned: “I am worried that they will either torture or assassinate me” (W12). Several participants had been forced to go into exile and take their families with them (W11).

The military also hunted any civil society organisations that continued to dissent online, including their staff. Many organisations closed, went underground, or went into exile (Z20). One participant was particularly
The military conducted widespread surveillance and covert interception to hunt dissenters.

36% of participants believed that they had been subjected to digital surveillance by the military. The military set up checkpoints nationwide to capture and search people’s devices looking for dissent (M27). They also confiscated the devices of anybody detained (AR19, AR8). One participant explained: “The soldiers told us to hand over all our devices and passwords and warned they would recover every deleted file too” (AR5).

Captured devices revealed digital trails that the military used for surveillance to hunt down other dissenters (O22). One participant believed that a single electronic device could uncover an entire network of dissenters: “They used the phone of someone detained to trace other connections” (AM5). Another participant revealed:

“They used the phone of someone detained to trace other dissenters. If they discover from our website or Facebook page that our organisation is still active, they will come after us” (M15).
"They went through my files and then opened up all my email and social media accounts and sent messages to my contacts pretending to be me and setting up meetings to entrap them" (AR8).

Websites and social media accounts were also being monitored by the military. One participant claimed that the military required all government departments to conduct surveillance: “We know that they are watching us because the ministry calls us when we publish online” (M14). Several participants said that they were aware of being followed online (AM12, AM20).

14% of participants suspected that they had been subjected to interception, a form of surveillance that is notoriously difficult to detect. The military had captured the means to implement blanket interception: “The military now occupies every telecom operator in the country” (A11). Participants did not know what kind of technology the military was using for interception but insisted: “They will do whatever they can” (AP12).

29% of participants stated that one of their websites, social media accounts, or emails had been hacked. One participant explained: “We face at least 50 hacking attempts every week originating from Yangon, Naypyidaw, Russia, and Singapore” (AK21). Other participants also reported seeing regular attempts to hack their accounts (AK2, AK27).

91% of participants had taken steps to circumvent the military’s digital surveillance. Some participants destroyed their old SIM cards and regularly switched to new SIM cards (AP10). Other participants explained that they actively self-censored when making phone calls to avoid any words or phrases that they thought could trigger interception (AP27).
Several participants, particularly those from ethnic communities, raised concerns about digital censorship by organised armed groups opposed to the military’s coup. Ethnic armed organisations (EAOs) reportedly made threats about online activities. One participant stated: “Sometimes we have to be more worried by ethnic armed organisations than we do by the military, especially when community leaders members write warnings on social media” (W1). Another claimed: “Community leaders also call us and warn us by name” (O1). A participating journalist revealed: “They threatened to come and burn down our homes and that forced us to all go underground” (W21).

Most participants did not experience any form of intimidation from the National Unity Government (NUG) whatsoever (M11). However, one participant disclosed that they had chosen to delete their social media content after being contacted by an acquaintance: “I raised concerns about the NUG’s financial practices...”
and was then contacted by a senior NUG member who politely expressed their disapproval” (M3).

21% of participants had been approached by members of the People’s Defence Forces (PDF). In many cases, the PDF members asked for content to be removed that could compromise their security and lead the military to them (M19, O19, M3).

However, participants felt intimidated by persons claiming to be PDF members. One participant explained: “A PDF member accused me of being a military informer and warned that I could be attacked anywhere and at any time” (T22). Another participant remarked: “They posted a threat on social media calling for members of the public to send them information about me. I felt like they were watching everything that I did just like military surveillance” (T10). One participant was threatened by some PDFs in Shan State for disclosing their fake statuses (BJ21).
Censorship by the Military

1: Internet shutdown. "Cutting the internet is not hard, just bite through the cables." "Wow is that all?". 2: They increase data prices if they cannot cut the internet. VPN undermines the free flow of information. It is such a hassle. But we need VPN because they are watching us all the time. 3: They arrest this person or that person. They block this or block that. As though information itself is criminal. 4: They are arresting people simply for their Facebook profile. "That guy is active on Facebook so find and arrest him now!" 5: They are monitoring phone lines. Semi-military owned enterprise. Surveillance. 6: "Phew..."
100% attacked by online communities that were intent on censorship

46% trolled

17% impersonated

33% cyberstalked

25% doxed or swatted

42% believed that attacks used gender-specific language or methods

33% of women experienced pornification, slut-shaming, or image-based sexual violence

33% saw signs of coordination
Myanmar’s online communities reflected and extended the public’s widespread revulsion and creative reaction to the coup, as well as increased political debate on what should replace the military. Online communities also reflected the violence, intimidation, and manipulation that spread offline as the military increasingly oppressed dissent.

**Surge in online dangers**

People faced a variety of serious threats online with severe offline consequences.

100% of participants had been attacked by online communities that were intent on censorship. 46% had been subjected to unsolicited comments intended to provoke, commonly known as trolling, since the coup began. One participant reported that trolling included emotive allegations like “you receive money from the OIC,” challenges like “come out on the streets if you are brave,” or outright threats like “it is better if you disappear” (BJ12).

Trolls often used fake accounts to remain anonymous (BN20). Some trolls created fake accounts that impersonated real people or organisations. 17% of participants had been impersonated online. One participant explained: “If you go on Facebook, you will see many impersonations publishing a mixture of edited original content and completely fake content” (BP21). Impersonation of media outlets was particularly common (BP6).

Some trolls were deeply obsessive. 33% of participants had experienced “cyberstalking” or repeated harassment, threats, and intimidation since the coup started. One participant reported: “They send us messages, make fake accounts, and criticise us repeatedly” (BN20).
42% of participants believed that such attacks often used gender-specific language or methods. Women were particularly subjected to trolls who spread fake, private, or compromising photos or content. 33% of women participants had experienced this form of genderised attack, sometimes called pornification, slut-shaming, or image-based sexual violence, compared to 9% of men. A woman participant explained: “They stalked us looking for photos that they could edit for their attacks” (BN10). Another added: “they also sent us sexual imagery” (BN19).

Doxing (publishing identifying personal information) and swatting (giving personal details to the police or military) were particularly dangerous online. 25% of participants had been doxed or swatted. One participant complained: “All my personal information was spread online with demands to arrest me” (M11). Another shared: “First they doxed me and then the military came to my house” (AK8). Some participants fled into exile after being doxed, as one noted: “the doxing was a written warning to flee” (O10). Once the individual had fled, their family was then doxed too (BT10).
Coordinated trolling

Online attacks often appeared coordinated by the military and its allies.

Some trolling, cyberstalking, pornification, and doxing attacks showed signs of being controlled and coordinated by a mastermind, rather than being conducted by isolated individuals (BZ27). 33% of participants saw signs of coordination, including a similar tone and content of messages. One participant noted that attacks “appeared organised because they were so similar” (BZ20). Another stated that attacks were often “copy-pasted” (BZ12).

The scale of attacks was also a sign of coordination, such as in pile-ons in which many trolls worked together. One participant explained that while online acts such as commenting may have seemed diverse and organic in nature, the comparatively large number was a sign of coordination (BZ19). A woman participant reported: “One group attacked me wherever my name appeared, sending hundreds of death and rape threats” (CB10).

It was more than reasonable to assume that the military and its allies masterminded many of the coordinated attacks against dissenters. One participant called the military’s network of soldiers, their families, and supporters, a “click army” and argued that people knew they were military allies because their attacks were so similar (BX12, BZ12). Another participant alleged that they had seen evidence of the military giving their allies orders to attack.
“One group attacked me wherever my name appeared, sending hundreds of death and rape threats.”

Dictating the revolution

Although the military was the main threat online, revolutionary fervour was sometimes controlling and exclusionary.

38% of participants had faced condemnation online when speaking about the National Unity Government (NUG), Committee Representing Pyidaungsu Hluttaw (CRPH), ethnic armed organisations (EAO), or revolutionary forces. Some condemnation showed signs of coordination among fellow users (BZ10).
Several participants raised concerns that differences in opinion or criticism were sometimes labelled as a betrayal of the entire revolution. One participant stated: “Some people cannot tolerate differences in opinion and want to draw a line between their ‘real’ revolution and what they call a ‘fake’ revolution” (BL10).

Revolutionary factions were emerging online with one group attacking another (BX20). One participant revealed that they were labelled a “traitor” to the revolution and a “military propagandist” (BT12). A participating journalist stated that publishing factual news about the revolution sometimes resulted in their media outlet being attacked as a “military informant” (BJ22, BJ19).

Several participants reported being condemned for working on issues that their attackers did not think were important according to their understanding of the revolution. “They said they are sacrificing everything for the revolution while I am working on labour rights which is less important,” said one participant (BL14). Another was told that their focus on “less important” women’s rights would “delay the revolution” (CD12). A third participant reported that they were repeatedly told “not to talk about human rights during the revolutionary period” (BL11).

“Some people cannot tolerate differences in opinion and want to draw a line between their ‘real’ revolution and what they call a ‘fake’ revolution”
Community censorship

Protection could be controlling if the emphasis was on self-censorship rather than self-defence.

Many participants revealed that their friends and family members had told them to be silent online. One said: “my relatives told me not to share information online because their neighbours were arrested for social media activities” (BJ27). Another said: “My family told me to keep my opinions to myself and not to share them on social media” (CL18). Refusing to stay silent led to serious arguments within families (BJ26).

Pressures to stay silent also came from the broader community. One participant said that their employer had contacted them online and urged them to “control their emotional criticism” of the military (BJ18). Another participant described how many of their colleagues who worked in public sector jobs stopped messaging and unfriend them because they refused to stay silent (BJ26).
“Censorship by Online Communities”

1: What is happening online? 2: Something like this. [Status] “It is important to be authentic in the revolution. If not...” [Comment 1] “You are too talkative for a boy.” [Comment 2] “What has it got to do with you woman?” 3: Unconstructive attacks. “He has been talking on Facebook about how the revolution should be, haha.” 4: Sexual violence. “The whore criticising the revolution.” “The whore criticising the military.” “Come to CB if you want to see her [sex video].” “That woman is not me.” 5: Impersonation. “Add me if you like me.” “How come he looks like [famous Korean actor]?”
"Censorship by Revolutionary Forces and Others"

1: Everything has pros and cons and the revolution also has authentic and inauthentic behaviors. 2: "Shhh. Do not dare thinking about disclosing our activities." 3: [News heading] Interview with a person who smiles after doing what they want. [Interviewer question] "How do you respond to your critics?" [Critics comments] "You are ineffective", "That's not okay", "That's not correct", "It shouldn't be like that". 4: [Interviewee] "I don't care. My critics are just loud and must be traitors or military informers." 5: People who want to critique federal democracy. 6: These people have to be afraid of friend and foe. 7: That is not easy.
63% experienced at least one case of over-moderation on Facebook

29% had content deleted by Facebook

17% had accounts suspended by Facebook

54% intentionally used techniques to avoid social media moderation
The response of social media

Social media platforms responded in varying degrees to the military coup, from the inaction of Telegram, to the brief action of YouTube, to the late action of TikTok, to the substantial but flawed action of Facebook. Each action and inaction whether through policy or practice created serious online impacts as well as offline consequences.

Exploiting ineffective moderation

Ineffective moderation encouraged harassment which led to censorship and self-censorship.

YouTube, TikTok, and Facebook have all been accused of ineffectively moderating Myanmar language content that would not be protected under international human rights law, such as harassment, sexual violence, and incitement to commit a crime. However, participants were most concerned about Telegram’s ineffective moderation (M11). Participants reported that Telegram in particular had failed to moderate doxing whereby people published other people’s identifying personal information, such as their name and address, intending at the very least for them to feel threatened online, and in many cases to be harassed or arrested offline (O15, AK8).

Several participants alleged that many people were openly “screen-grabbing Facebook content and reposting it on Telegram” together with personally identifying information and demands for the military and their allies to “take action” against the Facebook user (BT10, BJ9, BJ5). Such threats on Telegram led some people to “change their profiles and use alternative names on other platforms” (CF12). One participant believed that such doxing had led to demonstrable offline risks and yet Telegram had made little to no attempt to moderate (M11).
Over-moderation as censorship

Facebook moderation was not sufficiently intelligent and penalised legitimate content.

63% of participants had experienced at least one case of over-moderation on Facebook. 29% of participants - all of whom were journalists, human rights defenders, and activists - had their content deleted by Facebook, and 17% had their accounts suspended.

Many participants believed that using specific words or phrases would trigger Facebook moderation. Several participants claimed that using the verbs “kill”, “beat with a stick”, or “burn” in any context whatsoever would lead to a warning from Facebook (AX7, AV18). Moderation was reportedly predictable: “Facebook will ban you for
Free Expression Myanmar - Page 30
Moderation sanitised conflict

Hiding the inherent violence, pain, and suffering of conflict was not always in the public interest.

Many participants raised concerns that social media moderation was failing to strike the right balance between enabling public awareness of the conflict against protecting the rights of victims and of traumatised audiences (AV22, AV21, AV1, AV12, AX1, AX6, AX19, AX5).

In particular, participants were concerned about what they believed was Facebook’s disproportionate removal of images of graphic violence. One participant summarised these concerns: “Their moderation systems regard reports of brutal acts as dark matters,” which are not welcome on the platform (AX5).

Participants repeated very similar comments: “We received warnings for unpleasant images” (AV22); “I was warned about graphic violence” (AV21); “Photos of blood and injuries were removed” (AX6); “Our account was restricted for posting news about killed people” (AV1); “I saw a decline in our engagement rate because of warnings about violence” (AV12).

Facebook’s response was to mask graphic violence. Some participants agreed with Facebook’s proposal but believed it did not prevent moderation in practice: “We blurred our images but our content still got removed” (AX1). Some participants were concerned that masking would hide the reality of conflict: “How can we show people the military’s violence if we have to blur every photo?” (AZ19).

A participating journalist highlighted the longer-term impact of over-moderating the reality of conflict: “Yesterday our Facebook page was given a red warning because we reported on war casualties and today 16 more showed people the military’s violence if we have to blur masking would hide the reality of conflict: removed” (AX19).
"How can we show people the military’s violence if we have to blur every photo?"

Creative responses to moderation

People’s responses to censorship were just as creative online as they were offline.

54% of participants intentionally used different techniques to try to avoid social media moderation warnings, deletions, and suspensions. For example, one participant said people split up what they believed were moderation trigger words with spaces or alternative characters (AZ2). Another participant recommended replacing trigger words with “Myanglish”, a mixture of English and Myanmar that would confuse moderation...
Another technique was to avoid unedited photos and use multimedia content instead of words. One participating journalist said that they intentionally posted audio files to avoid moderation of written content (AZ8). Another said that they used satirical images to cover topics that may have attracted moderation (AZ4). A third said that they edited any photos of violence to make them black and white (AZ22).

(AZ16). One participant inserted English words believing that English moderation was less restrictive than Myanmar moderation (AZ16).
100% believed the general public had changed the way that they expressed themselves online

75% believed that they themselves had also changed

96% taken steps to mitigate or manage their personal risk

71% said that they reduced how much they expressed themselves online

67% changed their online voice, tone, and language

71% believed there were particular topics being avoided

58% had changed their public online profile to a private one
The near-universal desire to express outrage about the military coup created a significant peak in internet use in the first few months of the coup. Members of the public, many of whom were previously excluded from politics, joined celebrities, business leaders, and activists to denounce, criticize, and express their contempt for the military’s behaviour. Then the military began ramping up its oppression encouraging self-censorship.

Widespread self-censorship

Widespread online dissent was replaced by widespread self-censorship.

100% of participants believed that members of the general public had changed the way that they expressed themselves online since the coup started. 75% of participants believed that they themselves had also changed.

The public debate began declining as the military’s violent crackdown grew. 71% of participants said that they reduced how much they expressed themselves online. One participant summarised: “Public debate has clearly decreased” (CF7). Another added: “Before many people expressed themselves about the coup but now, they do not share their opinions” (CF12).

The decline was partly due to increased self-censorship. Many participants stated that they had intentionally stopped expressing themselves online. One said: “I used to be an active social media user but not so much since the coup started” (CH15). “We continued working covertly but we self-censored,” said another (CH10). Others may have chosen not to express themselves online to avoid attacks or to focus on their offline actions.

Although many participants self-censored in relation to the military and the coup, several explained that they also self-censored in relation to the National Unity...
Motivations for self-censorship

Self-censorship was a manifestation of rational feelings of anxiety, fear, guilt, and depression.

67% of participants changed their online voice, tone, and language since the coup started. Public discourse online reflected the widespread increase of intense feelings (W20). "I became much more emotional online," was a common opinion among participants (CO4, CO25, CO13, CO18).

In the first few months of the coup, the predominant public feeling was deep anger at the military's actions and the impact on people's lives (CO16, CO7, CO26, CO14). As one participant said: "I was angry and I am still angry". The feeling of anger gave people the strength to speak out online (CO6). It also made the public more formidable and demanding than ever before (CO18, CO16, CO7). "I no longer had any tolerance for the military's misbehaviour," said one participant (CO14).

Anger turned to fear as the military's campaign of oppression increased. Several participants highlighted a significant increase in their own personal anxiety in response to increasing public tension (CO15, CO8, CF26, W18). Participants were anxious and fearful about surveillance, their devices being seized, their online presence being checked, being criticised online, or being detained (CF8, AG16, BJ18, CF16).

Anger and fear were not the only common feelings. One participant stated that they felt a deep sense of guilt (CO27). Other participants said that these intense feelings encouraged numbness and depression (CF3, CO26, CO20).
It was these rational feelings of anxiety, fear, guilt, and depression that encouraged “feelings of caution” and self-censorship (CO8). 96% of participants said that they had taken steps to mitigate or manage their personal risk. As one participant stated: “The public has been overwhelmed with fear and responded by not only self-censoring their own opinions but also becoming reluctant to share what others are saying” (CF8).

Those who were prepared to accept their own personal risk were still fearful for their friends and family. Participants were concerned about the impact of their online actions on the security of their siblings, parents, and grandparents (CH18, CF27, CH2, CH9). One participant stated: “I always considered the effect of my own activities upon others and as a result self-censored every day” (BJ10).

Such feelings have drastically affected everything people did online: "We had to be very careful online and we sometimes felt like we were not ourselves anymore. We cannot speak. We cannot write. We cannot participate. We were afraid of being seen and recognised. We made ourselves invisible. We did not like living like this because this is not us. However, we were afraid that our parents and sisters would face difficulties because of what we did online” (CF15).
Political self-censorship

Any form of political expression became taboo once again.

71% of participants believed that there were particular topics being avoided since the coup began. One participant said that many people remained silent on certain topics (CH19). Another described such topics as taboo (CM3). Several participants stated that one such taboo topic was politics generally: “I rarely talk openly on social media about politics anymore” (CL9, CL20, CL14, CM20).

Taboo political topics were primarily anything relating to the military’s coup (CL27). Anything critical of the National Unity Government (NUG) or Myanmar’s largest political party, the National League for Democracy (NLD) was less taboo (CL4, CM1).

One participant noted the online return of attitudes and behaviours last seen during the previous military regime: “Common phrases that implied politics was a taboo topic such as ‘you are talking about politics’ disappeared for a decade but have started to appear again online since the coup started” (CF4).

“We cannot speak. We cannot write. We cannot participate. We were afraid of being seen and recognised. We made ourselves invisible.”
Organisational self-censorship

Media outlets, civil society organisations, and even the United Nations were systematically self-censoring online.

Participants explained that institutional self-censorship included editing or taking down websites, deleting Facebook pages, and closing social media accounts (AD27, AD25). A participating organisational leader said: “We had to censor our organisation because we saw what was happening to our peers and we were afraid of the military turning to us next and being able to trace all our past work” (CH15). Another said: “We decided to go low-profile and stop publishing anything anywhere” (AD25).

Some media outlets have also been forced to self-censor. Those outlets that have decided to continue operating openly in Myanmar systematically self-censor negative news about the military (AB19). Participating journalists stated that independent outlets also had to self-censor sometimes in order to protect their staff (X9) or to mitigate serious threats to their existence: “We avoid publishing news if it can be used against us” (X1).

Some organisations made more subtle acts of self-censorship. One participant said that they toned down everything that they published in public to make it less strong (Z9). Another said that they had gone through all their previous online content taking down anything that could be regarded by the military as “political” in nature (AD15).

Organisations also had clear plans to self-censor for the foreseeable future. “We have agreed that we will no longer share any content about our activities online, including conferences and professional activities,” said one participant (CM27). Another participant said that the existence of their entire organisation was being self-censored: “We will no longer mention the name of the organisation online” (CM25).
Privacy and self-censorship

Surveillance and attacks online prompted people to effectively self-censor by withdrawing into private online spaces.

58% of participants had changed their public online profile to a private one since the coup started. The purpose of going private was to reduce personal risk: “People wanted to prevent strangers from capturing screenshots of their content and sharing it with the military on Telegram” (CF13).

Going private was very common and involved locking down social media accounts to restrict conversations and sharing to only close friends and family (CS2, CS6, CS21, CS16, CS22, CS25, CS13, CS7, CS19, CS26). It also involved reviewing who had access to shared private spaces and getting rid of anybody who presented a potential risk. One participant stated: “I looked at who was there and removed anybody who was pro-military” (BL25). Another participant said: “I restricted them so they could not see me and I could not see them” (BL16).

Many people moved to more private and secure digital technologies. Email and Messenger were replaced by Signal and Proton Mail (CQ11, CQ1, CQ3, CQ15, CQ18, CQ27, CQ16, CQ25, CQ19). Disappearing messages, secret conversations, and quick deletions of messages all became common (CF14).

A sense of privacy enabled some people to continue their online activities against the military coup. As one participant explained: “Even if the military knows you are supporting the People’s Defence Forces (PDF) do not let them see you visibly do it” (BJ16). Another explained: “I was aware of security risks since I started fundraising for the opposition but I created a private and trusted network online” (AN16).

Privacy protections were insufficient or unconvincing for many. One participant said that even after making their
online profile private: “I no longer put personal content online and neither do my friends” (CM27). Another confirmed: “I no longer publish anything about where I am, what I am doing, or who I am with. We should not believe there is any privacy online and we should assume everything can end up public.” (CM10).

Locking down social media accounts, blocking people or ending friendships, and withdrawing into private spaces are all rational steps to mitigate risks, but they also raise questions about the balance between protection and self-censorship. As one participant raised: “People pointed out that I am taking a big risk because some of my Facebook friends are military allies, but I have not unfriended them because they are the people that I most want to speak to” (BJ2).
1. "Arrgh... Min Aung Hlaing!" "Dude, shhh!" "Mmm." 2: "You look like me but who are you?" "I'm your anxiety my friend." 3: "Remember that there are eyes everywhere watching you so don't mention politics. Shhh." 4: "Mmm." 5: "But I should be able to say what I want!" 6: "Shhh."
Conclusion

Journalists, activists, human rights defenders, celebrities, politicians, bloggers, students, and many other dissenters have been forced to live through the military’s digital coup for almost two years. They have experienced gross, systematic, and sustained violations of their rights to freedom of expression, privacy, association, assembly, liberty, and other rights, by internet shutdowns, blocks, imprisonment, surveillance, hacking, trolling, death threats, rape threats, under and over-moderation, and self-censorship.

The military attempted to resurrect its old authoritarian agenda but now as a “discipline-flourishing” internet. Its first preference, as witnessed in Sagaing Region, was to shut down all internet access wherever doing so did not interfere with its business interests.

Lacking the power to completely control the online space the military resorted to poisoning it. Online communities faced increased violence, much of it coordinated or at the very least inspired by the military and its allies. Violence was accompanied by surveillance and interception extending the military’s deteriorated network of offline spies.

Social media platforms have failed to stem the military’s poison. Restricting moderation may protect freedom of expression but under-moderating internationally unlawful expressions such as harassment and incitement only encouraged self-censorship. Over-moderation that misunderstood language and context further enabled censorship. Facebook’s decision to deprioritise current affairs information from Newsfeeds will worsen the bad situation.

The societal impact of the digital coup will be long-lasting. Online communities are traumatised and have low levels of trust. Violence has permeated throughout the online space and there is a risk that meaningful public discourse will increasingly disappear. Genuine desires to protect people online may become coercive and controlling.

However, the military’s digital coup has failed so far. Their proposed law to seize control of internet
Dissenters have seized upon anonymity, encryption, mass communication at the hierarchical lackeys, and money. Their attempts to fracture the internet by blocking inconvenient parts were thwarted by its inherent interconnectivity.

Their attempted digital coup has failed to stop the online space from encouraging, facilitating, and strengthening dissent. The National Unity Government (NUG) may actually be one of the world’s first online administrations. Dissenters have seized upon anonymity, non-hierarchical infrastructure, encryption, mass communication at the click of a button, and the incredible technical expertise of youth to bring an end to the coup online and offline.
Free Expression Myanmar (FEM) is a national human rights organisation that is expert in free expression and information, engaging in legal reform, defending victims of violations, and promoting best international standards.

This report forms part of FEM’s objective to promote appropriate and needed reforms. See:

- www.FreeExpressionMyanmar.org
- www.facebook.com/FreeExpressionMyanmar
- coordinator@FreeExpressionMyanmar.org

The report is copyrighted under a Creative Commons Attribution-NonCommercial-ShareAlikeLicense. This license lets you remix, tweak, and build upon FEM’s work non-commercially, as long as you credit FEM and license your new creations under the identical terms.

Acknowledgements

FEM would like to thank all the participants for sharing their experiences and views.

Support

The report is funded by the Swedish International Development Cooperation Agency (SIDA). The views represented in this report are FEM’s and do not necessarily represent the views of SIDA.

---

1 The OIC or "Organisation of Islamic Cooperation" is an intergovernmental organisation. The allegation implies that the target is paid to act against the interests of the people of Myanmar. It was notoriously used by religious extremists to demonise anybody who criticised the abuses against the Rohingya which are now understood to have been atrocity crimes.

2 Facebook’s sweeping classification of the word “Chinese” as hate speech has already been rejected by Facebook’s Oversight Board.
Surviving Myanmar’s digital coup

In the early hours of 1 February 2021, the Myanmar military launched a coup to depose the newly elected government. The military’s offline offensive was accompanied by a digital coup intended to prevent people from learning about, objecting to, and organising against the military’s unlawful act.

The digital coup has violated many human rights, including the rights to freedom of expression, information, media, association, non-discrimination, assembly, privacy, and liberty.

This report reveals the lived experiences of censorship among Myanmar’s most active online dissenters working under the digital coup, including journalists, human rights defenders, bloggers, activists, students, and others. It complements other publications focused on dissenters’ courageous responses, and more general or technical assessments of the digital coup, including FEM’s annual “Freedom on the Net” reports.