Freedom House

FREEDOM ON THE NET 2022

Myanmar

NOT FREE

12

/100

A. Obstacles to Access	2 /25
B. Limits on Content	6 /35
C. Violations of User Rights	4 /40

LAST YEAR'S SCORE & STATUS

17 /100 **Not Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Overview

The military continued to repress internet freedom in the face of ongoing civil disobedience, political opposition, and armed conflict after staging its February 2021 coup. Following the nationwide, long-term shutdowns imposed in early 2021, authorities instead imposed localized restrictions ahead of military attacks against opposition forces. Most internet users in the country can only access 1,200 government-approved websites. The military directly controls two mobile service providers and forced the sale of another two to military-linked companies, leaving people in Myanmar even more vulnerable to censorship and surveillance. Despite these and other obstacles—including detentions, egregious physical violence, and the country's first executions in decades—people in Myanmar continued to use digital tools to share information and organize opposition to the military.

Myanmar's already-stalled democratic transition was completely derailed in February 2021, when the military seized control of the government, arresting dozens of senior government officials and preventing the newly elected parliament from convening. The National League for Democracy (NLD), which won a sweeping victory in the November 2020 elections, led a broad-based opposition to the takeover, organizing the country-wide Civil Disobedience Movement (CDM). Protesters were met with indiscriminate violence from military forces, and journalists, activists, and ordinary people risked criminal charges and detention for voicing dissent. Armed conflict between the military and ethnic armed groups continued, as did the forced displacement of hundreds of thousands of Rohingya, a mostly Muslim ethnic minority group.

Key Developments, June 1, 2021 - May 31, 2022

- The military imposed large price increases on mobile data and multiple new taxes on phones, sharply restricting the affordability of internet access

—especially for poor people already disadvantaged by the declining economy (see A2).

- Authorities frequently deployed short-term, localized internet shutdowns to prevent the opposition from organizing or sharing information about atrocities, restricting internet access for millions of users (see A3).
- After Norway-based Telenor announced its intent to sell its telecommunications business in Myanmar in July 2021, the military forced a sale to a military-linked company, putting Telenor users' data within its reach (see A4 and C6).
- Civil society and those involved in mobilizing online communities were subjected to continuous physical attack, online harassment, and imprisonment, driving many organizations and groups into exile or self-censorship (see B4 and B8).
- Scores of internet users were imprisoned for their online activities during the coverage period; military courts issued multiyear prison sentences and carried out executions (see C3 and C7).
- The military struck against online anonymity by seeking the criminalization of virtual private networks (VPNs), imposing mandatory registration of devices, and increasing surveillance on both social media platforms and via telecommunications companies (see C4 and C6).

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**2**/6

Though internet penetration in Myanmar has expanded in recent years, internet access was severely impeded during the coverage period by damage to infrastructure, internet shutdowns (see A3), and high costs imposed by the military (see A2). By January 2022, 45.9 percent of the population had access to the internet, according to the *Digital 2022* report, an increase from 43 percent in 2021. [1] The

International Telecommunication Union (ITU) reported an internet penetration rate of 35 percent as of 2020. [2] In 2018, the Ministry of Transport and Communications (MoTC) had set a target of 99 percent internet penetration by the end of 2022, but it will likely fall far short. [3]

Most users rely on mobile services, [4] with 73 million mobile connections as of January 2022, representing a 134 percent penetration rate. [5] The penetration rate is comparably high because many users have multiple SIM cards, [6] a trend that increased after the coup began as people discarded and replaced SIM cards to avoid surveillance and to boycott military-controlled service providers. [7] Fixed-line and wireless broadband represented just 0.5 percent of connections in 2020; while this number has not changed in several years, [8] the number of connections may have increased in some urban areas during the COVID-19 pandemic. [9]

Telecommunications infrastructure has been damaged as the armed conflict between the military and antigovernment forces continued, and expansion has similarly been curtailed by physical insecurity. A state-controlled newspaper reported that than 400 cell towers were destroyed between February and December 2021. [10] The military has planted antipersonnel landmines around other towers, and telecommunications providers have stopped servicing towers after at least four engineers were seriously injured by unmarked mines in September and October 2021. [11]

Infrastructure development continues to be hampered by flooding, unreliable electricity, an inefficient bureaucracy, and private- and public-sector corruption. Daily power outages throughout the coverage period, [12] ranging from 5 to 16 hours in length, [13] have also impacted connectivity. In March 2022, the Ministry of Power and Energy announced that 24-hour-long outages may occur in parts of Myanmar, citing infrastructure repairs, though sources claimed that daylong outages were already taking place in Yangon. [14]

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**0** /3

Score Change: The score declined from 1 to 0 as the doubling of data prices and increases to the SIM card purchase tax severely limited internet affordability.

The cost of internet access sharply increased for most users during the coverage period. Price increases imposed by the military—combined with rampant inflation, [15] an 18 percent contraction of the economy, and major postcoup unemployment [16] —have forced poorer people in Myanmar to stop using the internet altogether. Some have sold their devices to pay for basic needs. [17]

The military-controlled MoTC ordered all mobile service providers to double their data prices in December 2021. [18] The MoTC also imposed a purchase tax of 20,000 kyat ($11) on SIM card sales in January 2022, tripled telecommunications firms' corporate taxes to 15 percent, [19] and created a 6,000-kyat ($3) tax for mandatory international mobile equipment identity (IMEI) registration. [20] The military said that the price increases were necessary to reduce the "effects triggered by extreme use of internet services on the employment of the people and mental sufferings of new generation students." [21] Then independent mobile service providers reported that they did not request these increases. [22]

Users in large urban areas can access fixed-line and wireless broadband, which halved in price between 2018 and 2021. [23] As of March 2022, the average fixed-line connection cost 47,000 kyat ($25.96) per month, with the cheapest connection costing 25,000 kyat ($13.80). [24] Given the disparities in access to broadband (see A1 and A2), poorer and rural internet users, already lacking computers and struggling with the country's rapid postcoup financial downturn, [25] will have experienced far greater increases in internet-access costs than richer urban users.

In 2018, before the coup, the MoTC established a Universal Service Fund (USF), funded by a 2 percent tax on telecommunications providers. [26] The USF was meant to address regional infrastructural gaps and connect 99 percent of the population to telecommunications services by 2022. [27] The USF's initial phase started in 2020 [28] but was suspended due to the 2021 coup. [29] In June 2020, the civilian government diverted USF funding to pay for a biometric database of mobile subscribers (see C4), [30] and the USF is now spent on military needs. [31]

The gender digital divide remains. According to ITU estimates, which were the most recent available, only 19 percent of women have internet access as of 2017, compared to 29 percent of men. **32** For women, barriers to owning and using a mobile phone to access the internet include perceived lack of relevance, high costs, and insufficient literacy skills. **33**

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**0** / 6

The military repeatedly shut down telecommunications services since seizing direct power. In the early hours of February 1, 2021, armed soldiers forcefully entered telecommunications providers' offices and demanded a national internet shutdown. **34** Since then, the military has repeatedly restricted connectivity by ordering internet shutdowns, slowdowns, and blocks while threatening service providers to ensure their compliance. **35**

Mobile services were repeatedly restricted at the local level during the coverage period. Cuts were reported in Yangon, Mandalay, Chin State, Kachin State, Karen State, Magway Region, and Tanintharyi Region, affecting millions of users. **36** Sagaing Region has faced particularly long disruptions, with an indefinite service cut beginning in March 2022. **37** Connectivity is curtailed in areas where antigovernment forces are particularly active, and online cuts coincide with severe offline crackdowns. **38**

As the February 2021 coup began, the military ordered day-long national internet shutdowns timed to undermine anticoup protests. **39** Internet restrictions were imposed after the coup took place. A digital curfew was enforced between February 15 and April 28: the military ordered access restricted overnight and irregular shutdowns and slowdowns during the day. **40** On March 15, the military shut down all mobile connections on March 15, public Wi-Fi connections were shuttered on March 18 and wireless broadband service was restricted on April 1. **41** Rare fixed-line broadband services (see A1) were the only way to access the internet for months. **42**

The MoTC directed the initial internet shutdowns, apparently under orders from the military-controlled Ministry of Home Affairs (MoHA) according to Telenor disclosures. **43** The military began loosening national connectivity restrictions in late April 2021.

In addition to the imposition of wide-ranging shutdowns, the military also instructed service providers to implement extensive restrictions on specific targets, blocking access to websites, applications, and social networks (see B1).

The military was influential in the precoup civilian government's decisions to restrict connectivity. In June 2019, the NLD government imposed a mobile shutdown affecting 1.4 million people in Rakhine and Chin States, in an attempt to conceal atrocities committed against the Rohingya ethnic group. **44** Connectivity was restricted at the military's behest **45** in order to "maintain stability and law and order," **46** with restoration only coming after the "security situation" improved. **47** Access was briefly restored in these areas in February 2021. **48**

The MoTC has significant powers to disrupt connectivity without oversight or safeguards, as it controls much of the telecommunications infrastructure via the state-owned company Myanmar Posts and Telecommunications (MPT). Private-sector providers were gradually diversifying ownership of mobile infrastructure and the internet backbone prior to the coup. Myanmar has three underwater and four overland internet gateways, **49** and more were expected, including new satellite connections, **50** because of a projected 70 percent growth in bandwidth. **51** However, this diversification may not materialize as the military seeks to strengthen its grip over Myanmar's internet infrastructure (see A4). **52**

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**0** / 6

Score Change: The score declined from 1 to 0 because the military forced the sale of Telenor to a military-aligned provider, consolidating its control over the telecommunications market.

The military directly controls two of Myanmar's four service providers. In March 2022, the military forced Telenor to sell a majority stake to Shwe Byain Phyu, a company with close historical links to the military. **53** Ooredoo sold its operations to a military-linked company in September 2022, after the coverage period. **54**

The military-owned operator Mytel, part of which is indirectly owned by the Vietnamese military, was licensed in 2017, **55** and had approximately 10 million subscribers as of June 2020 **56** before facing a consumer boycott. **57** In February 2021, the military seized more direct control of state-owned MPT, **58** which last reported having 24 million subscribers in early 2020. **59**

Telenor announced its intention to sell its Myanmar operations in July 2021, after receiving military orders to activate surveillance technology banned by European Union sanctions (see C5). **60** Telenor sought to sell its local operations to Lebanese company M1 Group for $105 million. **61** In March 2022, the military approved the sale on the condition that Shwe Byain Phyu hold an 80 percent stake in the local venture. **62** Junta leader Min Aung Hlaing was involved in the negotiations, and his daughter reportedly bought a stake in the local provider. **63** Shwe Byain Phyu rebranded Telenor's local operation as ATOM in June 2022. **64**

Civil society groups strongly criticized Telenor's sale to Shwe Byain Phyu, raising concerns that the military will use Telenor's network and data to identify members of opposition groups. **65**

The only independent mobile service provider remaining at the end of the coverage period was the Qatari-owned Ooredoo, which reported 13 million subscribers as of October 2020. **66** Although Ooredoo took a low profile since the coup started and benefited from the customer boycott of Mytel, **67** it has likely employed the military's surveillance technology. **68**

In September 2022, after the coverage period, Ooredoo signed an agreement to sell its Myanmar operations to Singapore-based Nine Communications, which is linked to the military through one of its parent companies. **69**

The military has not made significant attempts to seize control of fixed-line

broadband providers but is heavily investing in marketing Mytel's broadband services. [70]

Before the coup, the administration of licenses was generally regarded as fair and transparent, and external efforts to influence decisions were largely rebuffed. [71] Deregulation in 2013 removed many of the legal and regulatory barriers to entry for internet service providers (ISPs) and mobile service providers, leading to a proliferation in the number of licenses awarded. At least 207 telecommunications licenses had been awarded by 2020. [72]

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

Myanmar's regulatory bodies have been under the authority of the military since the February 2021 coup. The MoTC's Posts and Telecommunications Department (PTD) is responsible for regulating the telecommunications sector. As a ministerial department, the PTD has no legal or practical safeguards for its regulatory and operational independence, leaving it completely open to political interference. [73]

The military has controlled the PTD's regulation of telecommunications companies and licensing since seizing power. [74] PTD decisions during the coverage period demonstrated a lack of independence and transparency. For instance, the PTD did not pursue regulatory enforcement measures against Mytel, which ignored the PTD's orders on shutdowns, blocking, competition, and gambling [75] —including the Facebook ban [76] —in an apparent attempt to increase its subscriber base after the consumer boycott (see A4). The PTD's interference in Telenor's request to sell also showed bias in favor of the military's interests (see A4). [77] The PTD has repeatedly and publicly threatened its own staff for participating in anticoup protests and strikes. [78]

Article 86 of the 2013 Telecommunications Law outlines the responsibilities of a Myanmar Communications Regulatory Commission (MCRC), which has not been established. [79] Even though the mandate for the MCRC's composition does not

sufficiently safeguard its independence, the Telecommunications Law calls for the MCRC to take over regulatory functions from the PTD. The MCRC would also operate a mechanism to adjudicate any administrative disputes in the telecommunications sector. **80** Many analysts suggested that the NLD government failed to establish the MCRC because it was unwilling to relinquish the more direct control it had over the telecommunications sector through the PTD. **81**

B. Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	**1** / 6

The military has consolidated two distinct blocking regimes. Mobile service providers must block all websites except for 1,200 addresses approved by the military. All fixed-line and wireless broadband service providers, which serve just a small proportion of the public, allow access by default but block many specific addresses. Information about the two blocking regimes was not publicly disclosed during the coverage period.

The military-controlled MoTC regularly issued secretive blocking orders to service providers following the coup—several per week during the most violent periods—containing hundreds of thousands of addresses to block. **82** The military's first order arrived on February 3, 2021, to block Facebook and WhatsApp. **83** Orders to block Twitter and Instagram arrived on February 5, **84** followed later by blocks on most independent media outlets and international sources of information such as Wikipedia (see B6). **85** Some blocking orders were reversed in May 2021. **86** Although blocking orders are hidden, more websites, including media, have been blocked subsequently. **87**

On May 25, the military ordered mobile service providers to block all websites and internet protocol (IP) addresses except for 1,200 approved addresses that included a

large contingent of banking and financial sites, a small number of entertainment sites like YouTube and Netflix, news sites such as the *New York Times* and US-based Cable News Network (CNN), and gaming platforms. [88] The list of approved addresses has been irregularly updated since, but only to add business applications, including local businesses. [89] Facebook, Twitter, and most independent Burmese-language media outlets were not listed and therefore remain blocked. Instagram, YouTube, WhatsApp, LinkedIn, Viber, and Zoom appear to remain accessible.

Telenor disclosed that MoTC orders issued in 2021 required telecommunications companies to block access to URLs and IP addresses under Section 77 of the Telecommunications Law, which allows authorities to issue blocking orders to license holders in "emergency situations." [90] The military cited reasons like "preserving stability" and preventing "fake news" from "spreading misunderstanding." [91]

Service providers did not implement blocking orders consistently, [92] as some addresses were blocked by some providers but not by others. [93] For example, Facebook was accessible via at least one broadband provider, despite being subject to a blocking order, [94] and for some Mytel subscribers, despite not being on the list of approved sites. [95] It was unclear whether this was due to confusion, technical difficulties, or discretion; some staff at service providers reportedly tried to limit the effects of military orders by interpreting them narrowly or subverting their application. [96]

Prior to the coup, the NLD government had directed service providers to block more than 2,100 addresses in 2020, most from Interpol's list of banned child sexual abuse websites. [97] The NLD government also controversially issued blocking orders for 67 websites for publishing so-called "fake news," including well-known independent media outlets [98] and civil society organizations critical of the military. [99] Telenor initially resisted blocking media outlets [100] but later complied for fear of losing its license. [101]

The military's attempts to block censorship circumvention tools such as virtual private networks (VPNs) were indiscriminate and led to significant collateral damage, [102] including the disruption of content delivery networks like Google and Amazon

services. **103** Blocks disrupted banking, transportation, and—during the peak of the COVID-19 pandemic—education and health care. Some businesses and banks raised concerns about their ability to operate. **104** The blocks also undermined networks outside the country. **105**

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?	**1** / 4

Pressure to remove content continued to originate from state and nonstate actors within Myanmar during the coverage period, as well as from outside the country. Most independent media outlets have closed, hid, or gone into exile in response to the military's pressure, including its demands to cease critical coverage. **106** Few if any independent publishers remain within military-controlled areas of Myanmar, and those that remain, such as the previously independent outlet Eleven Media, avoid content that criticizes the military. **107**

The military began pressuring publishers to delete content soon after staging its coup in February 2021. The military demanded that media outlets cease critical coverage of their actions, delete any words translating to "regime" and "junta", and refrain from "biased" coverage (see B5). **108** By March, Myanmar's five daily newspapers had closed down, terminating their online and offline publishing. **109** One of the largest outlets, 7DayDaily, deleted its entire website in response to the deteriorating situation. **110** The military continued to threaten any publisher saying "coup" **111** or "Rohingya" during the coverage period. **112**

The military has forced users to delete content, including while in custody. **113** Under the draft Cyber Security Law proposed in January 2022, authorities can force hosts and platforms to comply with its orders, blocking and holding them criminally liable if they refuse (see C2).

Before the coup, the NLD government regularly called for content hosts and

platforms to address intolerance, misinformation, and incitement, [114] even though that government had failed in addressing those problems and NLD officials were alleged to have engaged in such behavior. [115] The NLD government's proposed Cyber Security Law was designed to make platforms criminally liable for a variety of ill-defined prohibited content. [116]

Pressure from civil society, media, and foreign governments had a significant effect upon Facebook to invest in and increase content moderation beginning in 2018, in response to atrocities committed against the Rohingya. [117] During the current coverage period, digital platforms faced continued pressure to introduce, increase, and improve content moderation in order to address military propaganda, disinformation, and threats. [118] The increase in content moderation efforts by companies like Facebook, YouTube, and TikTok have also led to the removal of significant amounts of content, including content produced by antigovernment groups (see B3). [119]

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**0** / 4

Since the coup, broad restrictions on digital content have been enforced without transparency and with gross disproportionality. The military-controlled PTD administered the military's orders without publishing information on what, why, when, or how restriction decisions were made, or by whom. [120]

The only available sources of information about restrictions have been media comments from ministers, service providers' statements, and civil society. The only service provider documenting the receipt of PTD orders, Telenor, stopped doing so in mid-February 2021, citing concerns for the safety of its staff. [121] Telenor then provided irregular updates until mid-April 2021, and later stopped entirely. [122] By the end of the coverage period, only civil society and media organizations are providing information on military blocking orders, though no public records exist.

Under the Telecommunications Law, the PTD can direct telecommunications

providers to temporarily block and filter content "for the benefit of the people," and does not allow for appeals. [123] There were no legal challenges to restrictions either before or after the coup. The NLD government occasionally articulated vague aims, and the military, when it did offer a rationale, included only vague references to "fake news" and the need to protect national stability and ensure public security. [124]

The draft Cyber Security Law introduced in January 2022 would require digital platforms to remove a wide range of content, including online criticism, with provisions requiring removal of "verbal statements against any existing law," "expressions that damage an individual's social standing and livelihood," and content "disrupting unity, stabilisation and peace." The draft law offers no transparency or appeals mechanisms. Sanctions under the bill include blocking orders and criminal liability for company representatives, including as much as three years' imprisonment. [125]

Social media companies have introduced new moderation systems and governance on a global basis in recent years. In 2018, Facebook increased its moderation activity, expanded its appeals process, [126] and established a self-regulatory Oversight Board. [127] The platform's parent company, Meta, publishes very little information about its moderation aside from routine transparency disclosures about global content removals. [128] Facebook also suspended much of its appeals process in 2020, citing the COVID-19 pandemic. [129] In August 2021, the Oversight Board overturned a decision to remove a Myanmar post that was labeled as hate speech; the post discussed possible methods to limit financing for the military. However, the overall effect of this decision on moderation remains unclear. [130] Activists have continued to raise concerns that some of Facebook's removals have compromised the public's right to know about important national stakeholders, and that they have swept up a wide range of valid content, including commentary on and documentation of human rights violations. Some in Myanmar's civil society suspect that these decisions are the result of internal problems, such as poorly trained staff, problematic automated content moderation, weak coordination, lack of investment, [131] and discriminatory decision-making. [132] For example, some Rohingya activists believe that content removal trends demonstrate anti-Rohingya prejudices among content reviewers. [133]

Other platforms have also been criticized for transparency and proportionality in content removal practices. After the February 2021 coup, YouTube initially removed some channels, including the state-owned MRTV and the military-owned Myawaddy Media, MWD Variety, and MWD Myanmar, [134] but has apparently done little since. [135] Following international media attention [136] and civil society criticism, [137] TikTok removed some videos posted by soldiers on its platform; many videos depicted soldiers threatening peaceful protesters with various weapons, which were brandished on-camera. [138] The company's transparency reports do not include Myanmar-specific disclosures. [139] During the coverage period, civil society actors voiced concern at Telegram's lack of action in response to serious abuses such as doxing of protesters and human right defenders (HRDs). [140]

Digital platforms largely avoided establishing facilities within Myanmar before the coup due to the high risk of intimidation and weak legal safeguards (see C2). Those with employees inside quickly evacuated them after the coup began, [141] although some consultants were taken hostage. [142]

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Since the coup, self-censorship online has grown significantly. Many journalists, commentators, and ordinary users condemned the coup and the military after February 2021. Those living under military rule increasingly practice self-censorship for their own security (see B8, C3, and C7). [143] Some stopped publishing online while others have avoided offering politically sensitive content. [144] Many social media users have edited their histories to remove sensitive content, including photos of protests, changed their social media profiles to hide their identities, or opened new proxy accounts under false identities, despite a ban on the practice by Facebook and other social media platforms. [145]

Self-censorship has also increased in response to the growth of moderation on social media platforms (see B3). [146] Users have learned to avoid the words and phrases

that automatically trigger platform warnings and removals.

Self-censorship was common prior to the coup. **147** Journalists, commentators, and ordinary users faced a range of pressures to agree with government narratives and majority beliefs on matters related to the military, businesses, armed conflict, the Rohingya, religion, sex and gender, and other politically sensitive topics. **148** For example, most independent media outlets actively self-censored when reporting on the Rohingya for fear of backlash, **149** and when they did, opted to call them "Muslims" or "Bengalis." **150** Women and girls self-censored on a range of topics, particularly related sex and gender, for fear of abuse and sexually harassment. **151**

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**1** / 4

The military has prioritized control over online information to advance the narrative that it is acting to reestablish public order and restore democracy after fraudulent elections. On the first day of the coup, the military seized control of all state-owned media and government communications services, **152** including all radio and television channels, as well as related Twitter accounts, YouTube channels, and Facebook pages, which have since promoted the military's narrative. **153** The military then began banning sources of alternative information such as independent media outlets, **154** and blocking access to their content (see B6). Several previously independent media outlets were allowed to continue operating, **155** but only if they followed the military's narrative (see B2).

Reports released during the coverage period indicate that the military has refined its tactics to spread its narrative online. **156** After the coup, the military ordered its soldiers to create social media accounts, spread the military's talking points online, and troll sources of alternative information. **157** Military supporters, including members of nationalist groups, are encouraged to amplify the content. **158** A Reuters investigation released in November 2021 identified 200 military personnel operating

social media accounts; their posts often spread online within minutes, often via online groups and fan channels of celebrities and sports teams set up by specialized military teams. **159**

Some social media platforms tried to prevent the military from promoting their narrative online. Following the coup, Facebook, Twitter, YouTube, Vkontake, and TikTok all to some extent banned the military or its representatives from using their services. **160** For example, Facebook removed or reduced the distribution of many pages run by the military or military-owned companies in February 2021, including the military's "True News Information Team" and state media. **161** The pages and accounts of various armed groups were also removed in recent years, as the company deemed them "dangerous organizations." Prior to the coup, Facebook removed the accounts of military organizations that perpetrated atrocities against the Rohingya and sought to limit the reach of military proxies, banning a number of pages and accounts in 2019 and 2021 for engaging in "coordinated inauthentic behavior." **162**

Reporting during the coverage period indicated that Facebook's moderation of promilitary networks sometimes failed to limit the spread of such content. A June 2021 investigation by Global Witness found that Facebook's page-recommendation algorithm had been amplifying military content that violated many of its own violence and misinformation policies. **163** Internal Facebook documents leaked in October 2021 also identified the platform's failure to limit the spread of content shared by promilitary accounts. **164**

Some promilitary disinformation networks have transitioned to Telegram, which offers fewer restrictions. A Frontier Myanmar investigation of promilitary Telegram accounts in September 2021 found that they disseminated content that disparaged armed civilian resistance and ethnic militias. **165** The platform had removed some promilitary accounts for incitement to violence as of March 2022, though many more remain. **166**

While it often voiced a desire for media freedom, the NLD sought to retain control over state-owned media during its time in government. **167** As a result, the NLD-led

government and the military dominated the broadcasting sector and a significant portion of print media prior to the coup, including those outlets' online presences, either directly through the Ministry of Information or via joint ventures with private companies. **168**

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**0** /3

The military revoked the licenses of most independent media outlets and ordered telecommunications companies to block their websites after the coup began (see B1), prohibiting them from publishing and blocking access to their audiences. **169** The first revocations were announced by state media in March 2021, as five of the most critical media outlets—Myanmar Now, Khit Thit Media, Democratic Voice of Burma, Mizzima, and 7Day News—were told they were "no longer allowed to broadcast or write or give information by using any kind of media platform or using any media technology." **170** The military also sought to detain journalists and raid outlets' offices after staging the coup. **171** No independent media outlets have been given a license since the coup began.

The military expanded its control over online outlets during the coverage period. Authorities unilaterally amended the Broadcasting Law in November 2021 to extend licensing requirements to online media, effectively requiring news sites that publish video and any internet users posting news videos on social media to apply for a license from the Ministry of Information. Those broadcasting without a license can face imprisonment under the amended law (see C2). **172**

In March 2021, the military declared that matters addressed by the News Media Law and the 2014 Printing and Publishing Law would instead be heard in courts-martial, which could issue capital sentences. **173** The Printing and Publishing Law created the licensing regime for publishing houses, news agencies, and websites, which must register prior to producing content, including for publishing online. The law also contains a variety of vague and overly broad administrative and criminal sanctions for

violations, such as running a website without a license. [174]

The Telecommunications Law has no specific regulations relating to net neutrality, zero-rating data transmissions by apps or telecommunications providers, or open internet policies.

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	**1** / 4

Myanmar's online environment is less diverse and reliable as a result of the February 2021 coup.

Most independent Burmese-language media outlets were not directly accessible within Myanmar due to content restrictions (see B1). Media outlets active in Myanmar have had to reduce their capacity in response to being banned and exiled. [175] Some new media outlets emerged, many of them providing local information to small communities and staffed by former employees of shuttered or exiled media outlets. [176] All outlets found fact-checking and verification harder because journalists could not easily travel and had no access to official responses from the authorities. [177]

Diversity in Myanmar's online sphere has also been reduced due to the in-country dominance of Facebook and has been further impacted by its blocking. [178] In 2020, 78 percent of mobile users had never used an internet browser or app store, with most users accessing the internet via Facebook apps on their mobile phones. [179] Global Witness research published in June 2021 found that Facebook's page-recommendation algorithm had been amplifying military content that violated many of its own policies (see B5). [180]

Some media outlets lost income originating from their YouTube and Facebook activity over the past year due to both the platforms' policies and their responses to the coup. [181] For example, outlets operating in exile have been unable to access funds generated on Facebook because of restrictions requiring them to maintain a

presence in their home country. **182**

The absence of reliable information has facilitated the spread of false and misleading content. Before the coup, rumors about ethnic and religious minorities, political leaders, and the COVID-19 pandemic were rife. **183** Since the coup, particularly prevalent rumors have addressed the status of detained NLD leader Aung San Suu Kyi, **184** impending internet shutdowns, **185** bank fraud, **186** the likelihood of violent crackdowns by the military, **187** deepfake technology, **188** and the role of China's government in supporting the coup. **189**

Before the coup, the NLD government also tried to limit the diversity of information available to the public by overseeing and sometimes leading attempts to marginalize media outlets critical of official narratives. For example, in 2019 the military requested that the media refrain from saying "civil war" when referring to the country's internal conflicts. **190** Such pressure, unhindered and indeed supported by the NLD government, led the British Broadcasting Corporation (BBC) and Radio Free Asia (RFA) to withdraw from country-based partnerships in 2017 and 2018, respectively, in order to protect their editorial freedom. **191**

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**1** / 6

Score Change: The score declined from 2 to 1 because the military's repression has sharply curtailed online organizing and has impeded mobilization within Myanmar, though some small-scale digital activism persists.

The military continued to impede the public's ability to associate or assemble online throughout the coverage period. **192** The military's blunt-force tactics of curtailing internet access (see A3) and blocking access to tools like Facebook and WhatsApp (see B1) were used repeatedly to prevent mobilization and armed resistance. **193** The military also used interception systems and social media surveillance to identify and locate political and community leaders (see C5). People participating in antimilitary activities or associating themselves with groups like the CDM or the National Unity

Government (NUG), including online, face serious risks of extrajudicial violence and imprisonment if identified and caught (see C3 and C7). **194** The military also announced it was "systematically scrutinizing" other civil society organizations in March 2022, further narrowing the space for community formation. **195**

The military has forced much of civil society into hiding, going into exile, shifting their focus to less politically sensitive topics, shutting down, or publicly accepting the legitimacy of the coup. **196** For example, of the four organizations that led the Myanmar Digital Rights Forum—an annual discussion for stakeholders in civil society, business, and technology—at least one had shut down, a second stopped working on digital rights, and the director of a third, Vicky Bowman, was imprisoned in September 2022, after the coverage period. **197** Civil society–organized online events were rarely held for fear of military reprisal. **198** The military also attempted to undermine civil society groups' operations and funding. **199**

Despite these restrictions, people continued to use online tools to organize and share information whenever possible. The CDM was launched on Facebook the day after the coup started **200** and participants continued to mobilize during the coverage period. **201** The military's political opposition, which launched within days of the February 2021 coup, **202** has coalesced into the NUG, a resistance movement that appeared to rely heavily on its online presence during the coverage period. **203** Some small-scale protests persist: In early 2022, some shop owners closed down their establishments in a general strike against the coup, with people mobilizing online to show support; at least 193 people were subsequently detained, including people who supported the strike on social media (see C3). **204**

Users have tried a range of tactics to circumvent the military's blocking efforts; VPNs and secure communications tools have become widespread. One secure communications app, Bridgify, was downloaded over a million times in Myanmar within two days of the coup. **205** The circumvention app Psiphon was downloaded by nearly two million users during the same period. **206** VPN usage was 7,200 percent higher by the end of February 4, 2021, than it was a week before, according to industry monitor Top10VPN; VPN usage continued to climb during the coverage period. **207**

The NLD government also targeted assembly and association rights before the coup, with protesters regularly facing arrest. **208** Dozens of people were arrested during 2020 for participating in offline protests against internet shutdowns and many later received prison terms. **209** Proposed amendments to the outdated legal framework were insufficient. **210**

C. Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**0** / 6

The military's coup effectively nullified the 2008 constitution along with the limited protections for free expression it offered. The military claimed that the coup—carried out under the cover of a state of emergency that the military said was necessary to address unverified claims of fraud in the November 2020 elections—was in line with its constitutional powers. However, both the justification and the process itself were unlawful. **211** Members of the Constitutional Tribunal, the one state body that might have held the military accountable to the constitution, were all replaced by the military on February 9, 2021. **212** In April 2021, parliamentarians who escaped the military declared the 2008 constitution void and replaced it with an interim charter under the NUG. **213**

The 2008 constitution and other laws in Myanmar largely failed to protect human rights online. The constitution, drafted by a previous military government and approved in a flawed 2008 referendum, stated that "enhancing the eternal principles of justice, liberty, and equality" was one of the country's six objectives. **214** It also provided specific—but highly limited—guarantees for citizens to "express and publish their convictions and opinions," **215** and to "freely develop literature, culture, arts, customs, and traditions," **216** provided that they were "not contrary to the laws enacted for Union [of Myanmar] security, prevalence of law and order, community

peace and tranquility, or public order and morality." [217] The constitution included no provisions directly relating to the internet or access to information, although Article 96 and Schedule 1 (8.m) granted the parliament authority to establish laws regulating the internet.

A number of laws undermine media freedom and freedom of expression. The 2013 Telecommunications Law criminalizes legitimate expression and authorizes restrictions on online content. A range of other laws further impede online expression, including the Electronic Transactions Law (see C2), the Printing and Publishing Law, and the Broadcasting Law (see B6).

The rule of law has essentially collapsed. [218] Before the coup, judicial independence was minimal as courts generally adjudicated cases in accordance with the government's interests, particularly in cases with political implications. [219] Since the coup, the military has suspended habeas corpus and other legal rights, tried civilians in military tribunals, heard cases inside prisons to prevent observers from attending, arbitrarily detained thousands of people, harassed lawyers, and used torture to extract confessions. [220]

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**0** / 4

The military has drastically expanded legal penalties for online activities following the coup, including during the coverage period.

In November 2021, the military imposed amendments to the Broadcasting Law that extended criminal penalties to media outlets publishing online without a license, punishable by up to five years' imprisonment (see B6).

In January 2022, the military circulated a revised draft of the Cyber Security Law. The draft undermines due process, eases further blocking, and criminalizes the use of VPNs. The draft would also give the military absolute control over the internet in

Myanmar and extend military jurisdiction to foreign companies. [221] Following widespread outcry, the military quietly dropped an earlier version of the proposal in February 2021. [222] The January 2022 proposal has been strongly criticized by human rights organizations like Free Expression Myanmar and multistakeholder coalitions like the Global Network Initiative. [223] The draft's status was unclear at the end of the coverage period.

The military also amended the Electronic Transactions Law in February 2021, incorporating many of the problematic provisions from the initial draft of the Cyber Security Law. These included new rules that could be used to criminalize the publication of "false information" or information that could damage foreign relations. [224]

In February 2021, the military unilaterally amended the penal code to strengthen punishments for treason and sedition, [225] and added an extremely vague criminal offense under Article 505A, which criminalized causing fear, spreading false news, or disrupting officials; Article 505A prescribes penalties of up to three years' imprisonment, a fine, or both. [226] The military used Article 505A thousands of times during the coverage period to punish dissent, including online (see C3). [227] The amended penal code contains other provisions that have been used to a lesser extent, including Article 505(a), which criminalizes encouraging officials to mutiny, and Article 505(b), which bans causing fear or alarm in public." [228]

In March 2021, the military imposed martial law, which prescribes capital punishment for a range of crimes including treason, inciting disaffection towards the government or military, or disrupting the government or military. [229] The law also brought the adjudication of the News Media Law, Printing and Publishing Law, and Electronic Transactions Law under the jurisdiction of courts-martial, as well Sections 505 and 505A of the penal code.

The 2004 Electronic Transactions Law criminalized online activity. For instance, it barred "any act detrimental to" state security, law and order, community peace and tranquility, national solidarity, the national economy, or the national culture —including "receiving or sending" information with those effects. The law was

routinely used to criminalize internet activism during the previous period of military rule. **230** The Telecommunications Law was enacted by a military-backed civilian government in 2013 principally to deregulate the market but also included new criminal provisions for legitimate digital activities; Article 66(d) addresses defamation while Article 68 covers disinformation. **231** The law was amended in 2017 after significant criticism of the misuse of Article 66(d) to penalize dissent, with no discernible impact. **232** In December 2020, a civil society coalition launched a new push to amend Article 66(d) and the country's five other criminal defamation provisions, putting forward four reform options. **233**

The Law Protecting the Privacy and Security of Citizens, which was enacted in 2017 and widely condemned by civil society for being debated and passed without proper consultation, provides for prison terms of up to three years for defamation. **234** The defamation provisions were amended in 2020 but were still used to prosecute individuals for online activity (see C3). **235** In February 2021, the military suspended parts of the law, including its limited protections against surveillance and the interception of private messages. **236**

The Trademark Law, adopted in January 2019, penalizes trademark infringement and counterfeiting with up to three years' imprisonment and a fine of approximately 5 million kyat ($3,800). **237** It was adopted alongside the Patent Law and the Industrial Design Law, which also include criminal sanctions for violations. **238** In May 2019, a copyright law that includes prison terms of up to three years for commercial copying without consent was adopted. **239** Each law applies to online content and could be used against users.

The military was working on a revised hate speech law and wanted to include punishment for "political" hate speech in contradiction to international human rights standards. **240** The NLD government had developed a series of drafts in 2017 which were criticized by civil society for being punitive and failing to address Myanmar's significant problem of intolerance. **241** The NLD government in April 2020 issued a Directive on the Prevention of Incitement to Hatred and Violence, ordering officials to address the issue of hate speech. **242** The directive came in advance of a reporting deadline set by the International Court of Justice which is investigating genocide

against the Rohingya.

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**0** / 6

Score Change: The score declined from 1 to 0 because military-controlled authorities and courts engaged in arbitrary and disproportionate mass arrests, including of internet users, and imposed extreme sentences.

Internet users are frequently penalized in Myanmar's restrictive legal environment. Free Expression Myanmar reported that almost 4,000 people were identifiably arrested, detained, charged, or imprisoned under Articles 505 and 505A in the year since the coup; of those, 1,269 people remained in pretrial detention and 143 received prison terms as of February 2022. A further 7,200 people were held on unknown charges and may have been prosecuted under Articles 505 and 505A. **243** Many of these cases were likely related to people's online activities, though specific numbers are difficult to establish due to the collapse in due process, increased court secrecy, and the removal of evidentiary requirements in trials.

The military-controlled government is one of the world's worst jailers of journalists. **244** Between February 2021 and March 2022, 122 journalists, all of whom were affiliated with media outlets that published online, were arrested according to Detained Journalists Information Myanmar. As of March 2022, another 48 were still detained, 22 had received convictions, **245** and 25 had warrants out for their arrest. **246** Since then, more have been detained. **247** The majority of imprisoned journalists were detained, charged, or sentenced under Article 505A. **248** Other penal code provisions have also been used against journalists; for example, Tin Shwe, a journalist for the news site Magway Post, received a three-year prison term under Article 505(c) in January 2022. **249** Many journalists, like Ma Thuzar, were penalized for covering anticoup protests. **250** Journalists' relatives were also targeted by the military. For example, when journalist Htet Htet Aung, who reported for the online outlet Thingangyun Post, was detained, her 7-year-old daughter was also imprisoned

and questioned for two days before being released. **251**

In July 2022, after the coverage period, the military executed prominent activist Kyaw Min Yu, better known as Ko Jimmy, alongside former lawmaker and rapper Phyo Zeya Thaw and two others (see C7). Kyaw Min Yu was arrested in October 2021, after the military issued a warrant for his arrest in February 2021 over social media posts criticizing the coup. **252**

At least 959 students, 165 civil society workers, and 465 politicians were detained as of April 2022, according to the Assistance Association for Political Prisoners. **253** Research released by Free Expression Myanmar found that of over 2,400 people detained, charged, or sentenced under Articles 505 or 505A between February 2021 and January 2022, 25 percent were health-care workers, 13 percent were educators, and 9 percent were in creative fields, including music. **254** At least 60 prominent celebrities were on warrant lists as of April 2021. **255** Many did not engage in political commentary until the February 2021 coup. **256** For example, actors Eaindra Kyaw Zin and Pyay Ti Oo were sentenced to three years' imprisonment in April 2021 for encouraging civil disobedience against the coup via social media in April 2021; they were pardoned in March 2022. **257**

Users were arrested during the coverage period for supporting protesters. Between late January and early February 2022, at least 193 people were detained for encouraging a general strike, including people who supported the strike on social media (see B8). **258** In February 2022, a senior police officer was detained for condemning military brutality against protesters in a December 2021 social media post. **259** Members of the public were also detained on the street after the military searched their phones and found purported criticism of the coup, according to a February 2022 report. **260**

Those who have evaded being brought into custody have faced other penalties. For example, authorities confiscated the home of Thalun Zaung Htet, the editor of online outlet Khit Thit Media, in February 2022. **261**

Penalization of users was also common before the coup, to a lesser extent. In January 2021, just before the coup began, the military filed a criminal defamation lawsuit

under Article 66(d) of the Telecommunications Law against the editor of Rakhine-based Development Media Group for posting a story about military corruption online. **262** In December 2020, high school student Maung Tin Chan was sentenced to five years' imprisonment for incitement under Article 33(b) of the Electronic Transactions Law, having published critical Facebook posts related to the conflict in Rakhine State. **263** Also in December, Thinzar Than Min was sentenced to nine months' imprisonment under Article 505(a) of the penal code for alleging that the military-backed Union Solidarity and Development Party was corrupt. **264** In February 2020, Kay Khine Tun, Paing Phyo Min, and Su Yadanar Myint of the poetry troupe Peacock Generation received six-month prison terms under Article 66(d) of the Telecommunications Law for sharing images of and live-streaming their performances, which satirized the military, on social media. **265**

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**2** / 4

Users' ability to communicate anonymously has been further restricted by the military since the coup. In March 2021, daily directives banned the use of VPNs, though some orders barring VPN use emerged the month before. **266** The Open Observatory of Network Interference (OONI) confirmed that multiple circumvention-tool websites were blocked at least once alongside their IP addresses in February 2021. **267** Although the blocking limited some people's ability to use circumvention tools, internet users continued to employ them. During the coverage period, the military used random street searches of peoples' devices in order to inspire fear of surveillance. **268**

The military's proposed Cyber Security Law would, if adopted, criminalize possession of VPN software and the use of pseudonyms on Facebook, with a sentence of up to three years' imprisonment in both cases (see C2). **269** Businesses in Myanmar condemned the proposal as unworkable in January 2022, as most applications and systems use VPNs for security purposes. **270** Despite the law not being formally adopted, military officers searched people on the street and threatened to arrest

those with VPNs installed on their devices, collecting bribes. **271**

Prior to the coup, anonymity was limited by the government's enforcement of SIM card registration requirements. In 2017, the NLD government enforced mandatory registration whereby subscribers must provide their name, citizenship identification document, birth date, address, nationality, and gender. Noncitizens had to provide their passports. **272** Some subscribers reported that service providers required information beyond the bounds of the regulations, including their ethnicity. **273** Many did not register. **274** In February 2020, the NLD government announced that it had blocked 6.5 million unregistered SIM cards. **275** The government also ordered service providers to bar outgoing calls for users of millions more unregistered SIM cards beginning that April. **276**

After the coup, the military has extended SIM card registration to include mandatory registration of the IMEI numbers of all devices or face deregistration, ostensibly linked to IMEI tax payments mandated during the coverage period (see A2). **277**

Prior to the coup, the NLD government issued a tender in November 2019 for a biometric SIM card registration system, **278** including fingerprints and facial-recognition information, **279** and it had requisitioned the money from the USF (see A2). **280** It is unclear whether more SIM cards were blocked after the coup began, or whether the military is continuing the biometric plans.

There are no clear restrictions on encryption in law, although vague provisions in the Telecommunications Law and the Electronic Transactions Law could be interpreted to restrict the practice.

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

The military's online surveillance and interception has grown since the beginning of the coup, dovetailing with its comprehensive offline capacity. Immediately after the coup began, the military unlawfully suspended parts of the Law Protecting the

Privacy and Security of Citizens, including its modest safeguards against warrantless surveillance and interception of private messages. **281**

The draft Cyber Security Law would, if adopted, strip away almost all privacy protections and require all data to be stored on devices and servers designated by and accessible to the military without any form of oversight (see C2). **282** Although the draft has not yet been enacted, the military unilaterally amended the Electronic Transactions Law in February 2021 by adding some of the same problematic provisions included in an earlier draft of the Cyber Security Law. For instance, the revised law grants the authorities broad powers to inspect any device on vague bases such as "misuse." **283**

According to a May 2021 Reuters report, former military officials pressured providers in late 2020 to install interception technology that would enable the military to view texts and emails, listen to phone calls, and locate users without assistance or approval. **284** Some observers believed that the technology was not yet fully proactive but rather relied on the military to actively identify what it wanted to monitor. **285** The military's Public Relations and Information Production Unit, known as the Ka Ka Com, reportedly had a network of teams involving hundreds of soldiers nationwide responsible for identifying suspects and networks online, and then infiltrating them; **286** military surveillance networks also included information with data from the devices of captured detainees, **287** and from security cameras equipped with facial-recognition technology. **288**

The military also used soldiers to conduct physical surveillance of devices through random spot-checks and fixed checkpoints, looking for censorship circumvention tools or politically sensitive content in photo albums, messages, and posted on social media. **289** Forensic search technology was reportedly active in Myanmar prior to the coup: Police have used products from the Israeli company Cellebrite since 2016. **290** The malware product FinSpy was reportedly in operation in Myanmar in 2019. **291**

Before the coup, the NLD government had already invested in acquiring interception capacity, including by ordering service providers to install the technology that the military later activated after the coup began. **292** The NLD government spent $4.8

million on technology, [293] allocated to the Social Media Monitoring Team (SMMT), [294] a body established under the MoTC. [295] The NLD government argued that the SMMT was necessary to counter individuals causing "instability" online, including through hate speech and defamation. [296] Little was known about the SMMT's operations or whether there was any oversight, [297] but civil society assumes that it is now being used by the military. [298] The SMMT spent its budget on tools from vendors based in Canada, the United States, Sweden, and Israel, among others. [299] Purchases included MacQuisition forensic software, which can extract data from Apple computers; tools that can extract deleted content from mobile devices; and additional technology for determining the home addresses of online critics.

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**0** / 6

Score Change: The score declined from 1 to 0 as the lack of separation between the military and service providers enables authorities to access user data with no restrictions.

Service providers are obliged to hand data over to the state without sufficient oversight or safeguards.

Myanmar lacked a robust data protection law, despite years of calls from a range of private-sector and civil society stakeholders. [300] The military imposed amendments to the Electronic Transactions Law in February 2021, adding a new chapter on personal data protection which falls far short of international standards. The amended law does assign some duties for data controllers, but those duties are ill-defined and amended bylaws were not published. [301] The amendment also obliges data controllers to hand data over to the state without sufficient oversight or safeguards.

The Law Protecting the Privacy and Security of Citizens, passed in 2017 and partially suspended since the coup, [302] prohibits the interception of personal communications without a warrant, but it contains a vague exception allowing

surveillance if permission is granted by the president or a government body. The law does not outline clear procedures to prevent data from being collected, stored, and destroyed, nor does it provide for judicial review. The law's definition of privacy is inadequate and inconsistent with international human rights standards. **303**

The Telecommunications Law grants the government the power to direct unspecified persons "to secure any information or communication which may harm security, rule of law, or peace of the state." **304** The Telecommunications Law also grants the government the power to inspect the premises of telecommunications firms and to require them to hand over documents—for the ill-defined purposes of defending the "security of the state" or "the benefit of the people"—without safeguards for individuals' privacy and other human rights. **305** A 2018 amendment to the Narcotic Drugs and Psychotropic Substances Law included a new provision requiring telecommunications firms to disclose user information without due process. **306**

The draft Cyber Security Law proposed in January 2022 would require platforms and service providers with over 100,000 users in Myanmar to store data on servers designated by and fully accessible to the military, functionally amounting to data localization. The bill also imposes wide retention requirements for user data. **307**

There is little room for providers to push back against the military's directives, and the military's direct or indirect control of service providers in Myanmar facilitates even more direct access to user data. Between February 2021 and February 2022, the military-controlled MoTC handed Telenor more than 200 data request orders under the Telecommunications Law, **308** compared to 188 requests in 2019 and about 70 in 2018. **309** Telenor reportedly complied with all of the requests submitted after the coup; each required call records and call locations spanning months, and in total covered thousands of users. **310** The largest state-owned service provider, MPT, has never publicized the number of requests for data it receives from authorities. Mytel stated that it received over 100 requests in 2019 but has not published numbers since. **311**

In at least one instance during the coverage period, providers did successfully resist a

military order for information. In March 2022, a regional military official ordered service providers to disclose subscriber lists in order to identify who still had internet access; the companies reportedly appealed successfully to the military on the grounds that the move would violate their license requirements. **312**

Prior to the coup, telecommunications providers claimed that the majority of requests were related to human trafficking, missing people, and drugs. **313** One provider stated in 2018 that it initially required three documents before disclosing information, including a letter from a senior police officer and a letter from the PTD, but it later dropped the third requirement for a judicial warrant. **314**

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**0**/5

The military and their proxies continued to threaten, extort, physically assault, forcibly disappear, torture, and kill online and offline opponents with complete impunity. **315** Many people in Myanmar face extralegal intimidation and violence on a daily basis from military propaganda, constant surveillance, and physical checks, including of devices. **316**

The military targeted people who supported online resistance or participated in protests, the CDM, and political opponents, especially the NUG (see B8). **317** The unlawful imposition of martial law (see C2) and the threat of capital punishment increased fear among protesters, strikers, political activists, journalists, and HRDs. **318** By June 2021, at least 64 protesters, including 2 children, received death sentences from military courts. **319** In July 2022, the military executed Phyo Zeya Thaw, Kyaw Min Yu, Hla Myo Aung, and Aung Thura Zaw—the first in decades (see C3).

Over 1,500 people were killed by the military between February 2021 and the end of the coverage period, some of whom were targeted in relation for their online activities. **320** This included at least three journalists working for or previously employed by online media outlets. Pu Tuidim was abducted and killed in January 2022, two days after he was captured while covering fighting between the military

and antigovernment forces. **321** Sai Win Aung was shot on Christmas Day in 2021 while covering fighting. **322** Photojournalist Soe Naing died in the military's custody in December 2021; Soe was tortured after being detained earlier that month while photographing a protest. **323** After the coverage period, in July 2022, photographer Aye Kyaw, whose photos of anticoup protests were published on social media and in local outlets, died while in military custody; Aye's body showed signs of torture. **324**

Others killed since the February 2021 coup, some in retaliation for their online activities, included 15 civil society workers, over 100 students, and a large number of activists. **325** In March 2021, for example, activist and teacher Zaw Myat Lynn was tortured to death after being detained for sharing videos online of soldiers attacking demonstrators. **326**

Hundreds of people, including children, were killed in military custody after the coup began, **327** most of them due to torture. **328** Torture is rampant, including through sexual violence. **329** Those severely tortured included the cofounder of Kamayut Media, Han Thar Nyein, who was subsequently sentenced to two years' imprisonment in March 2022. **330** An unknown number of protesters, HRDs, activists, and others who conducted activities online remained in detention. The military also collected the social media profiles of all individual soldiers and leveled threats against them over their online activity, **331** including their VPN-enabled use of Facebook. **332** "Watermelons," or individuals outwardly supporting the military but actually preferring the opposition, came under attack during the coverage period. Users with large followings called for information on "watermelons" and doxed them; they have also offered bounties for their targets' deaths. **333**

Soldiers, nationalists, and other military proxies also issued threats **334** and tracked down social media users opposed to the military. **335** Those suspected of opposition activity online after being released from custody were warned that their online profiles were under surveillance and they could be returned to detention. **336** Activists, journalists, and HRDs have been doxed since the coup, usually over Telegram, TikTok, and Facebook. **337** Women have faced various forms of sexual violence including nonconsensual sharing of sexually explicit images and of doctored images. **338**

Online journalists, HRDs, and political activists reported intimidation, threats of violence, and torture prior to the coup, although to a significantly lesser degree. In one opinion survey published in May 2020, most journalists reported that they believed violence against members of the media had increased compared with the previous year. **339** Journalists reporting on the Rohingya crisis or covering the Rakhine State and Shan State conflicts risked violence in recent years. **340** During the trial of Reuters journalists Wa Lone and Kyaw Soe Oo, defense lawyers informed the court that the journalists were tortured in detention. **341** In July 2018, Kyaw Soe Oo told the court that he was subjected to sleep deprivation and forced to kneel for hours while he was interrogated. **342** He also said that authorities covered his head with a black hood.

HRDs also faced intimidation and violence prior to the coup. The scale and volume of threats against HRDs, all of whom used the internet as their principal tool for advocacy, varied depending on the issue they focused on in their work. Pro-Rohingya and peace activists reported high levels of intimidation via direct and indirect messages and comments online. **343** Allegations of torture were also made against police, prison guards, and border guards by student activists, **344** monks, **345** and others. **346** Women reported regular gender-based intimidation and threats of violence online. **347** Common harassment tactics included cyberstalking, phishing, doxing, hacking, and attempts to cast doubt on women's credibility, integrity, and character. Many were intimidated through doctored sexual or intimate images, which were sometimes used in extortion attempts.

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**1** / 3

Websites, Facebook accounts, and email services have been subjected to technical attacks in Myanmar.

HRDs, journalists, and political activists continued to report regular, often weekly,

attempts to hack their devices, email, and social media accounts after the February 2021 coup. **348** Advanced espionage malware, thought to originate in China and be state-sponsored, **349** was repeatedly found hidden in widespread Burmese-language fonts commonly shared via USB sticks or available for download online, including on the national presidential website as of June 2021. **350** Several media outlets claimed to have had their Facebook and YouTube accounts hacked since the coup, before later restoring them. **351** Prior to the coup, pro-Rohingya and Muslim activists reported frequent hacking attempts, and online activists noted that Google regularly warned them of "government-backed attackers" attempting to hack their Google accounts. **352** **353**

During the previous coverage period, several government websites, including those of the central bank and state television stations, were hacked and defaced with antimilitary messages after the coup. **354** Some 330 gigabytes of government-held corporate financial data was leaked in February 2021, including details on how military-held firms and coup leaders used Google services. **355**

Police used sophisticated technology to break into the devices of journalists, including Reuters reporters Wa Lone and Kyaw Soe Oo in 2017. **356** Advanced spyware has been identified in Myanmar, **357** and HRDs, journalists, and political activists have reported the presence of spyware on their mobile phones (see C5). **358**

Footnotes

5 Simon Kemp, "Digital 2022: Myanmar," Datareportal, February 15, 2022, https://datareportal.com/reports/digital-2022-myanmar. See previous Freedom of the Net reports.

2 Myanmar, Digital Development Dashboard, International Telecommunications Union, accessed September 28, 2022, https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Develo....

3 Government of Myanmar, "Executive Summary: Universal Service Strategy for Myanmar 2018–2022," January 2018, https://ptd.gov.mm/ckfinder/userfiles/files/Executive Summary of Universal Service Strategy (English)_0.pdf

4 "Speedtest Global Index Republic of the Union of Myanmar," Ookla, accessed on March 16,

2022, https://www.speedtest.net/global-index/republic-of-the-union-of-myanmar; "Establishing Internet Exchange in Myanmar," Ministry of Transport and Communications, September 7, 2020, https://www.unescap.org/sites/default/files/6%20Myanmar%20CLMV-%20Inter...

"Digital 2022: Myanmar," Datareportal, March 18, 2022, https://datareportal.com/reports/digital-2022-myanmar; Ministry of Transport and Communications, "Establishing Internet Exchange in Myanmar," September 7, 2020, https://www.unescap.org/sites/default/files/6%20Myanmar%20CLMV-%20Inter...

More footnotes

On Myanmar

See all data, scores & information on this country or territory.

See More ›

Country Facts

Global Freedom Score

9 /100 **Not Free**

Internet Freedom Score

12 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2022

Other Years

2021

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org