FREEDOM ON THE NET 2023

Myanmar

10

NOT FREE

/100

A. Obstacles to Access	2 /25
B. Limits on Content	5 /35
C. Violations of User Rights	3 /40

LAST YEAR'S SCORE & STATUS

12 /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, which seized control of the state in a February 2021 coup, continued to repress internet freedom in the face of ongoing civil disobedience, political opposition, and armed resistance during the coverage period. Localized internet shutdowns, data price hikes, online trolling, and arbitrary prosecutions that result in long prison terms have created a high-risk and hostile online space for the public at large. The military's direct and indirect control over all major service

On Myanmar

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

providers has enabled the enforcement of strict rules on user identity registration as well as mass censorship and surveillance. Despite these and other obstacles—including detentions, egregious physical violence, and the country's first executions in decades—people in Myanmar continue to use digital tools to share information and organize opposition to the military.

Myanmar's already-stalled democratic transition was completely derailed by the February 2021 coup, in which the military arrested dozens of civilian government officials and prevented a newly elected parliament from convening. The National Unity Government (NUG) has led a broad-based opposition to the takeover, overseeing a countrywide Civil Disobedience Movement (CDM) as well as armed resistance, and exercising partial or effective control over a growing swathe of territory outside major population centers. Protesters, journalists, activists, and ordinary people risk criminal charges, detention, and lethal violence for voicing dissent against the military. Millions of people remain displaced or have been newly displaced by violence, including hundreds of thousands of Rohingya, a mostly Muslim ethnic minority group.

Key Developments, June 1, 2022 – May 31, 2023

- The military's broad attempts to make the internet a hostile space, combined with a faltering economy and attacks on infrastructure, resulted in a globally rare decline in internet penetration (see A1).
- Authorities frequently enforced short-term, localized internet shutdowns to prevent the opposition from organizing or sharing information about atrocities, effectively restricting internet access for millions of users (see A3).
- After the country's last two foreign-owned telecommunications service providers, Telenor and Ooredoo, sold their Myanmar operations, all providers

See More ›

Country Facts

Population
54,180,000

Region
Asia-Pacific

Global Freedom Score
8 /100 **Not Free**

Internet Freedom Score
10 /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

were left under either direct or indirect military control, enabling mass interception without safeguards (see A4).

- Most interest users remained confined to a list of approximately 1,500 military-approved websites; only those with circumvention tools were able to bypass extensive blocking and reach other internet resources (see B1).
- Scores of internet users were imprisoned for their online activities during the coverage period; military courts issued multiyear prison sentences and carried out executions in some cases (see C3 and C7).

Freedom in the World 2023

Other Years

2022

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 generally expanded in recent years, access decreased during the coverage period amid damage to infrastructure, internet shutdowns (see A3), and high costs imposed by the military (see A2). By early 2023, 44 percent of the population used the internet, according to the *Digital 2023* report, a decrease from 45.9 percent in January 2022. **1** Separately, the International Telecommunication Union (ITU) reported an internet penetration rate of 44 percent as of 2021. **2** In 2018, the Ministry of Transport and Communications (MoTC) set targets to cover 99 percent of the population with a mobile network and 95 percent with mobile broadband service by the end of 2022, but it has fallen short of these targets. **3**

Most internet users in Myanmar rely on mobile services. **4** The number of mobile connections fell to 64.6 million in February 2023, from 73 million in January 2022, representing a 118.8 percent penetration rate. **5** The penetration rate was relatively

high during the first two years following the coup because many users had multiple SIM cards, [6] discarding and replacing them to avoid surveillance and boycott military-controlled service providers. [7] Fixed-line and wireless broadband represented just 0.5 percent of subscriptions in 2020; while this number had not changed in several years, [8] it may have increased in some urban areas during the initial period of the COVID-19 pandemic. [9]

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

The NUG stated in February 2023 that it had started providing a publicly accessible internet connection of unknown quality to at least 15 townships in areas outside military control. [12] Meanwhile, several cases reported by digital rights defenders during the coverage period indicated that community-led efforts to purchase telecommunications equipment and establish small-scale infrastructure have faced significant barriers. An improvised tower erected by one community was reportedly destroyed by the military. [13] Attempts by a border community to purchase equipment from China was reportedly blocked by Indian authorities. [14]

Infrastructure development has also been hampered by flooding, unreliable electricity, an inefficient bureaucracy, and corruption in the private and public sectors. Daily power outages throughout the coverage period ranged from 5 to 16 hours in length. [15] During the previous coverage period, in March 2022, the Ministry of Power and Energy announced that 24-hour outages could occur in parts of Myanmar due to

infrastructure repairs, though other sources claimed that daylong outages were already taking place in Yangon. [16]

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

The cost of internet access has sharply increased for most users since the coup. Price increases imposed by the military—combined with inflationary pressures and increased unemployment [17] —have forced poorer people in Myanmar to reduce their usage or stop it altogether. [18] Some have sold their devices to pay for basic needs. [19] Widespread internet shutdowns in conflict-affected areas have left large populations without access, though a very small number of opposition activists are able to use expensive satellite connections (see A3). [20]

The military-controlled MoTC ordered all mobile service providers to double their data prices in December 2021, [21] with 1 GB of nonpackaged mobile data costing 10,000 kyat ($4.70). [22] The MoTC also imposed a purchase tax of 20,000 kyat ($9.40) on SIM-card sales in January 2022, tripled telecommunications firms' corporate taxes to 15 percent, [23] and created a 6,000-kyat ($2.80) tax for mandatory registration of international mobile equipment identity (IMEI) numbers. [24] The military said 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." [25] Mobile service providers that were not at the time affiliated with the military reported that they did not request these increases. [26]

Users in large urban areas can access fixed-line and wireless broadband, which halved in price between 2018 and 2021. [27] As of March 2023, the average fixed-line connection cost 45,000

kyat ($21.20) per month, with the cheapest connection costing 22,000 kyat ($10.40). [28] In comparison, the average price of 1 GB of mobile data was $1.11, with the cheapest connection costing $1. [29] Given the disparities in access to broadband and mobile networks (see A1 and A2), poorer and rural internet users, already lacking devices and struggling with the country's rapid postcoup financial downturn, [30] experienced far greater relative increases in internet-access costs than richer urban users.

In 2018, the MoTC established a Universal Service Fund (USF), supported by a 2 percent tax on telecommunications providers. [31] The USF was meant to address regional infrastructural gaps and connect 99 percent of the population to telecommunications services by 2022. [32] Its initial phase started in 2020, [33] but the effort was suspended due to the 2021 coup. [34] In June 2020, the civilian government diverted USF funding to pay for a biometric database of mobile subscribers (see C4), [35] and in October 2022, the fund's resources were directed toward building a comprehensive SIM Registration Management System. [36]

The disparity in access between men and women persists. According to ITU estimates from 2017, which are the most recent available, only 19 percent of women had internet access, compared with 29 percent of men. [37] 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. [38]

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 has 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. **39** The military also instructed service providers to implement extensive restrictions on specific targets, blocking access to websites, applications, and social media platforms (see B1). Since then, the military has frequently restricted connectivity by ordering internet shutdowns, slowdowns, and blocks while threatening service providers to ensure their compliance. **40**

Following the nationwide shutdowns imposed in early 2021, localized internet restrictions continued during the coverage period. **41** Connectivity is typically curtailed in areas where pro-NUG forces are particularly active, and online cuts coincide with severe offline crackdowns by the military. **42** Cuts were reported in Chin State, Kachin State, Karen State, Magway Region, and the cities of Yangon, Mandalay, and Naypyidaw, affecting millions of users. **43** Sagaing Region has faced especially long disruptions, with an indefinite service cut beginning in March 2022. **44** The military has reportedly used portable signal jammers to restrict local communications when raiding villages. **45** Slowdowns and interruptions to fixed-line connections also emerged in Yangon and other cities during the coverage period. **46**

The military was influential in the precoup civilian government's decisions to restrict connectivity. In June 2019, the National League for Democracy (NLD) government imposed a mobile-service shutdown affecting 1.4 million people in Rakhine and Chin States, in an attempt to conceal atrocities committed against the Rohingya ethnic group. **47** Connectivity was restricted at the military's behest in order to "maintain stability and law and order," **48** with restoration expected only after the "security situation" improved. **49** Access was briefly restored in these areas in February 2021. **50**

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, [51] and more were expected, including new satellite connections, [52] because of a projected 70 percent growth in bandwidth. [53] However, this diversification may not materialize as the military seeks to strengthen its grip on Myanmar's internet infrastructure (see A4). [54]

A4 0-6 pts

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

The military directly controls two of Myanmar's four telecommunications service providers. The military-owned 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] it later faced a consumer boycott after the coup. [57] The company was accused in 2022 of facilitating military atrocity crimes. [58] Following the coup, the military also seized direct control of state-owned MPT, [59] which last reported having 24 million subscribers in early 2020. [60]

The other two service providers, ATOM (formerly Telenor) and Ooredoo, were operated by independent foreign companies prior to the coup, but they are now under the ownership of firms with links to the military. In September 2022, the Qatari company Ooredoo sold its Myanmar operations to Nine Communications, a Singapore-based subsidiary that is reportedly owned by military-linked individuals. [61] Ooredoo reported 13 million subscribers as of October 2020; [62] Reuters reported 9 million Ooredoo subscribers in 2022. [63] Although Ooredoo adopted a low profile after the coup and benefited from the customer boycott of Mytel, [64] it has likely employed the military's surveillance technology. [65] In March 2022, the military approved the sale of the Norwegian company Telenor's

local operations to Lebanese company M1, on the condition that the local firm Shwe Byain Phyu hold an 80 percent stake. **66** Military leader Min Aung Hlaing was involved in the negotiations, and there were reports that his daughter bought a stake in the local provider. **67** Shwe Byain Phyu rebranded Telenor's local operation as ATOM in June 2022. **68** Civil society groups strongly criticized Telenor's sale to Shwe Byain Phyu, raising concerns that the military would use Telenor's network and data to identify members of opposition groups. **69** Telenor had announced its intention to sell its Myanmar operations in July 2021, after receiving military orders to activate surveillance technology that was banned by European Union sanctions (see C5). **70**

The military has not made significant public attempts to seize control of fixed-line broadband providers but is heavily investing in marketing efforts for Mytel's broadband services. **71**

Before the coup, the administration of licenses was generally regarded as fair and transparent, and external efforts to influence decisions were largely rebuffed. **72** 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. **73**

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 run by former military officers, the PTD has no legal or practical safeguards for its regulatory and operational

independence, leaving it completely open to political interference. [74]

The military has controlled the PTD's regulation of telecommunications companies and licensing since seizing power; civilian ministers of the MoTC were replaced with military appointees. [75] PTD decisions have been kept secret since the coup, but their effects demonstrated a lack of independence and transparency. For instance, the PTD did not pursue regulatory enforcement measures against Mytel, which ignored its orders on shutdowns, blocking, competition, and gambling [76] —including a Facebook ban [77] —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 its Myanmar operations also showed bias in favor of the military's interests (see A4). [78] The PTD has publicly threatened its own staff for participating in prodemocracy protests and strikes. [79]

Article 86 of the 2013 Telecommunications Law outlines the responsibilities of a Myanmar Communications Regulatory Commission (MCRC), which has not been established. [80] 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. [81] 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. [82]

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	**0** / 6

international human rights standards?	

Score Change: The score declined from 1 to 0 due to the prolonged and extensive nature of the military's systematic website blocking.

The military has consolidated two distinct blocking regimes. Mobile service providers must block all websites except a list of about 1,500 that have been approved by the military. All fixed-line and wireless broadband service providers, which serve only a small proportion of the public, allow access by default but block many specific addresses. More detailed 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 in the first year following the coup—several per week during the most violent periods—with each containing hundreds of thousands of addresses to block. **83** The first such order was issued on February 3, 2021, and targeted Facebook and WhatsApp. **84** Orders to block Twitter and Instagram arrived on February 5, **85** followed later by blocks on most independent media outlets and international sources of information such as Wikipedia (see B6). **86** Some blocking orders were reversed in May 2021. **87** Although the orders themselves are typically not announced to the public, subsequent blocking of additional websites, including news outlets, suggested that more orders were being issued. **88**

The default blocking on mobile services began on May 25, 2021, when the military ordered providers to obstruct access to 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. **89** The list of approved addresses was updated in 2022 to add business sites, including those of local businesses; it is unclear

whether further updates have occurred since then. [90] Facebook, Twitter, and most independent Burmese-language media outlets were not listed and therefore remained blocked during the coverage period. Instagram, YouTube, WhatsApp, LinkedIn, Viber, and Zoom appeared 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." [91] The military cited goals like "preserving stability" and preventing "fake news" from "spreading misunderstanding." [92]

In the immediate aftermath of the coup, service providers did not implement blocking orders consistently, [93] with addresses blocked by some providers but not by others. [94] For example, Facebook was accessible via at least one broadband provider, despite being subject to a blocking order, [95] and for some Mytel subscribers, despite not being on the list of approved sites. [96] 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. [97]

The military's attempts to block censorship circumvention tools such as virtual private networks (VPNs) have been indiscriminate and have led to significant collateral damage, [98] including the disruption of content delivery networks like Google and Amazon services. [99] Blocks have also disrupted banking, transportation, and—during the peak of the COVID-19 pandemic—education and health care. Some businesses and banks have raised concerns about their ability to operate. [100] In addition, the blocks have reportedly undermined networks outside the country. [101]

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

State and nonstate actors continued to exert pressure to remove content during the coverage period.

Most independent media outlets have closed, operated clandestinely, or gone into exile in response to the coup and the military's pressure, including its demands to cease critical coverage. **102** Few if any independent publishers remain within military-controlled areas of Myanmar, and those that opted to stay, such as the previously independent outlet Eleven Media, now avoid content that criticizes the military. **103** The military began pressuring publishers to delete content soon after staging its coup in February 2021. Officials at first warned journalists and then demanded that media outlets cease critical coverage of the military's actions, delete any words translating to "regime" and "junta," and refrain from "biased" reporting (see B5). **104** By March 2021, Myanmar's five daily newspapers had closed down, terminating their online and offline publishing. **105** One of the largest outlets, 7DayDaily, deleted its entire website in response to the deteriorating situation. **106** The military has continued to threatened publishers for using disfavored terms including "coup" and "Rohingya." **107**

Messaging and social media platforms such as Facebook and Telegram have faced ongoing international calls to improve their content moderation in ways that address military propaganda, disinformation, and threats. **108** Facebook had already come under mounting pressure from civil society, the media, and foreign governments to invest in and improve content moderation beginning in 2018, when it was criticized for failing to contain inflammatory online content that encouraged violence against the Rohingya people. **109**

At the same time, digital rights defenders have raised concerns that Facebook's content moderation has led to the removal of valid content, including commentary and documentation of human rights violations. Some in Myanmar's civil society sector suspect that these problems stem from weak training among staff and deficient algorithms; others have pointed to discriminatory decision-making among content reviewers. **110** Myanmar's media outlets have faced particular difficulties in navigating Facebook's community standards while trying to cover the conflict and have reported that they have seen posts removed subject to the platform's policies on coordinating harm and graphic violence. **111**

Other platforms have also been criticized for their content moderation efforts. 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, **112** but it has apparently done little since. **113** Following international media attention and civil society criticism, **114** TikTok removed some videos posted by soldiers on its platform; many such videos depicted soldiers threatening peaceful protesters with various weapons, which were brandished on camera. **115** Although Telegram deleted channels such as Han Nyein Oo and Thazin Oo, which had been promoting the military's propaganda, doxing people, and sexually harassing women activists who opposed the coup, the individuals behind the channels simply started new versions and regained thousands of followers. **116**

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 has

administered the military's orders without publishing information on what, why, when, how, or by whom restriction decisions were made. **117**

The only available sources of information about restrictions have been ministers' comments to the media, service providers' statements, and civil society. The only service provider that documented the receipt of PTD orders, Telenor, stopped doing so in mid-February 2021, citing concerns for the safety of its staff. **118** Telenor then provided irregular updates until mid-April 2021, and later stopped reporting on the issue entirely. **119** During the coverage period, only civil society and media organizations provided information on military blocking orders, though no official and 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 there is no mechanism for appeals. **120** There were no legal challenges to content 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 broad references to "fake news" and the need to protect national stability and ensure public security. **121**

Although it was not enacted during the coverage period, a new draft Cyber Security Law introduced in January 2022 would require digital platforms to remove a wide range of content, including "verbal statements against any existing law," "expressions that damage an individual's social standing and livelihood," and material "disrupting unity, stabilization, and peace." The draft law offers no transparency or appeal mechanisms. Sanctions under the bill include blocking orders and criminal liability for company representatives, who could face up to three years in prison for violations. **122**

The increase in social media companies' content moderation in recent years has not been matched by an increase in transparency about moderation policies, including appeal

processes. In 2018, Facebook increased its moderation activity, expanded its appeal process, **123** and established a self-regulatory Oversight Board. **124** However, the platform's parent company, Meta, publishes very little information about its moderation and appeal process, aside from routine transparency disclosures about global content removals. **125** 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. **126** Telegram has also displayed pronounced deficiencies in transparency surrounding its content moderation. **127**

Global 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 the country quickly evacuated them after the coup began, **128** though some consultants were detained by military authorities. **129**

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 initially condemned the coup and the military. However, those living under military rule increasingly limit their critical speech for their own security (see B8, C3, and C7). **130** Some have stopped publishing online entirely, while others have avoided offering politically sensitive content. **131** Many social media users have edited their histories to remove photos of protests and other high-risk material, changed their social media profiles to hide their identities, or opened new proxy accounts under false identities, despite a ban on that practice by Facebook and other social media platforms. **132**

Self-censorship has also increased in response to the growth of

moderation on social media platforms (see B3). [133] Users have learned to avoid the words and phrases that automatically trigger platform warnings and removals.

Self-censorship was already common prior to the coup. [134] Journalists, commentators, and ordinary users faced a range of pressures to agree with government narratives and majority beliefs on matters related to the military, powerful businesses, armed conflict, the Rohingya, religion, sex and gender, and other politically sensitive topics. [135] For example, most independent media outlets actively self-censored when reporting on the Rohingya to avoid backlash, [136] and when they did address the issue, they generally opted to refer to Rohingya people as "Muslims" or "Bengalis," effectively denying their distinct identity. [137] Women and girls self-censored on a range of topics, particularly those related to sex and gender, due to the risk of abuse and sexual harassment. [138]

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 junta has engaged in concerted efforts to control and manipulate information online, advancing false claims that it initially intervened to restore democracy after fraudulent elections and has since been trying to reestablish public order in the face of a terrorist threat. On the first day of the coup, the military seized control of all state-owned media and government communications services, [139] including all radio and television channels, as well as related Twitter accounts, YouTube channels, and Facebook pages, using them to spread propaganda. [140] The military then began banning sources of alternative information such as independent media outlets, [141] and blocking access to their content (see B6). Several previously independent media outlets were allowed to continue operating, [142] but they now avoid any criticism of the military (see B2).

The military has refined its information manipulation tactics online. After the coup, it ordered soldiers to create social media accounts, spread the junta's talking points online, and troll sources of information that challenged official narratives. A Reuters investigation released in November 2021 identified 200 military personnel operating social media accounts; their posts often spread online within minutes, in some cases via the online groups and fan channels of celebrities and sports teams set up by specialized military units. **143** Military supporters, including military family members and members of nationalist groups, are also encouraged to amplify such content. **144** In an effort to further exert control over online narratives and bypass content moderation policies imposed by global social media platforms, the military announced in 2022 the creation of its own local social media platforms. One such application is OkPar, designed to be an alternative to Facebook. Another is MTube, which is similar to YouTube. **145**

Some social media platforms have tried to prevent the military from promoting false and misleading narratives online. Following the coup, Facebook, Twitter, YouTube, VKontakte, and TikTok all to some extent banned the military or its representatives from using their services. **146** 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. **147** The pages and accounts of various armed groups have also been 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." **148**

Facebook's moderation of promilitary networks has sometimes failed to limit the spread of their 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. **149** Internal Facebook documents leaked in October 2021 also identified the platform's failure to limit the spread of content shared by promilitary accounts. **150**

Some promilitary disinformation networks have migrated to Telegram, which offers fewer restrictions. A Frontier Myanmar investigation of promilitary Telegram accounts in September 2021 found that they disseminated content disparaging armed civilian resistance and ethnic militias. **151** A 2023 report by Myanmar Witness found that disinformation on Telegram is often sexualized to target politically active women (see C7). **152** The platform had removed some promilitary accounts for incitement to violence as of March 2022, though many more remained. **153**

B6 0-3 pts

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

After the 2021 coup began, the military revoked the licenses of most independent media outlets and ordered telecommunications companies to block their websites (see B1), prohibiting them from publishing and cutting them off from their audiences. **154** 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 that they were "no longer allowed to broadcast or write or give information by using any kind of media platform or using any media technology." **155** The military also sought to detain journalists and raid outlets' offices after staging the coup. **156** No independent media outlets have been given a license since the takeover. While some outlets have continued to work underground and have expanded their audiences by publishing on social media platforms, their ability to monetize their

content has been limited due to platform policies and their responses to the coup. **157**

Authorities unilaterally amended the Broadcasting Law in November 2021 to extend licensing requirements to online media, effectively requiring news sites that publish videos—and any internet users who post 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). **158**

In March 2021, the military declared that offenses committed in areas under martial law and addressed by the News Media Law and the 2014 Printing and Publishing Law would be heard in military tribunals rather than in civilian courts. **159** 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 contains a variety of vague and overly broad administrative and criminal sanctions for violations, such as running a website without a license. **160**

B7 0-4 pts

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

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

During the coverage period, most independent Burmese-language media outlets were not directly accessible within Myanmar due to content restrictions (see B1). Media outlets that are active in Myanmar have had to reduce their capacity in response to being banned and exiled. **161** Some new outlets have emerged, many of them providing local information to small communities and staffed by former employees of shuttered or exiled media operations. **162** All outlets have found fact-checking and verification to be more difficult than in the

past, as sources are reportedly fearful of repercussions for sharing information (see C3 and C7), journalists cannot easily travel, and they have no access to official responses from the authorities. **163** Outlets often rely on volunteers, known locally as "citizen journalists," who are in many cases aligned with prodemocracy groups and report to multiple outlets primarily about conflict-related news. **164**

Diversity in Myanmar's online sphere has also been affected over time by the in-country dominance of Facebook and its subsequent blocking. **165** In 2020, 78 percent of mobile users had never used an internet browser or app store, with most accessing the internet via Facebook applications on their mobile phones. **166** 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). **167**

The absence of reliable information has facilitated the spread of false and misleading online content. Particularly prevalent rumors have addressed the status of detained NLD leader Aung San Suu Kyi, **168** impending internet shutdowns, **169** bank fraud, **170** the likelihood of violent crackdowns by the military, **171** deepfake technology, **172** and the role of China's government in supporting the coup. **173** In 2023, a human rights defender was forced to flee when she saw her name on a warrant list circulating online and had no way to check the image's authenticity. **174**

Before the coup, rumors about ethnic and religious minority groups, political leaders, and the COVID-19 pandemic were rife. **175** 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 that were critical of official narratives. **176**

B8 0-6 pts

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

The military continued to impede the public's ability to associate or assemble online throughout the coverage period. **177** The junta's blunt restrictions on internet access (see A3), blocking of tools like Facebook and WhatsApp (see B1), **178** use of interception systems and social media surveillance to identify and locate political and community leaders (see C5), and extrajudicial violence (see C3 and C7) were all designed to prevent popular mobilization. **179** Of the four organizations that led the Myanmar Digital Rights Forum—an annual discussion venue for stakeholders in the civil society, business, and technology sectors—two had shut down, and a third stopped working on digital rights. **180** Civil society–organized online events were rarely held for fear of military reprisal. **181**

The military has forced much of civil society to go into hiding, operate from exile, shift its focus to less politically sensitive topics, shut down, or publicly accept the legitimacy of the coup. **182** The military has also sought to undermine civil society groups' operations and funding. **183** In March 2022, it announced that it was "systematically scrutinizing" civil society organizations. **184** New rules adopted in October 2022 require civil society organizations to register with local authorities and regulate the purposes and activities that registered organizations are permitted to pursue. Organizations that fail to comply face fines and criminal penalties of up to five years in prison for their representatives. **185**

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, **186** and participants continued to mobilize during the coverage period. **187** Political opposition to the military takeover, which was organized within days of the February 2021 coup, **188** has since coalesced into the NUG, a broad-based prodemocracy

resistance movement that appears to rely heavily on its online presence. **189** Small-scale offline protests persisted during the coverage period, as did nationwide "silent protests" aimed at shutting down the economy. **190**

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. **191** The circumvention app Psiphon was downloaded by nearly two million users during the same period. **192** According to industry monitor Top10VPN, VPN usage continued to climb in the year following the coup. **193**

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 coup effectively nullified the 2008 constitution along with the limited protections for free expression it offered. The military carried out the coup under the cover of a state of emergency that it claimed was necessary to address unverified claims of fraud in the November 2020 elections, arguing that the move was in line with its constitutional powers. However, both the justification and the process itself were unlawful. **194** Members of the Constitutional Tribunal, the one state body that might have held the military accountable to the constitution, were all replaced by the junta on February 9, 2021. **195** In April 2021, members of the parliament who escaped military-controlled areas declared that the 2008 constitution was void

and replaced it with an interim charter under the aegis of the NUG. **196** Meanwhile, the military has extended its state of emergency beyond the time limits stipulated in the 2008 constitution, with fresh extensions announced in February and July 2023. **197**

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. **198** It also provided specific—but highly limited—guarantees for citizens to "express and publish their convictions and opinions," **199** and to "freely develop literature, culture, arts, customs, and traditions," **200** 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." **201** The constitution included no provisions directly related to the internet or access to information, although Article 96 and Schedule 1 (8.m) empowered the parliament to establish laws regulating the internet.

A number of laws undermine media freedom and freedom of expression. The 2013 Telecommunications Law criminalizes legitimate forms of 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 since the coup, as the military took control of the judicial system. **202** The military has suspended habeas corpus and other legal rights, tried civilians in military courts, heard cases inside prisons to prevent observers from attending, arbitrarily detained thousands of people, harassed lawyers, and used torture to extract confessions. **203**

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 expanded legal penalties for online activities since the coup.

In November 2021, the military amended the Broadcasting Law to extend criminal penalties to media outlets that publish online without a license, prescribing up to five years in prison for the responsible individuals (see B6).

In January 2022, the military circulated a revised draft of its proposed Cyber Security Law. The draft would undermine due process, enable further blocking, and criminalize the use of VPNs. It would also give the military absolute control over the internet in Myanmar and extend military jurisdiction to foreign companies. **204** Following a widespread outcry, the military had quietly dropped an earlier version of the proposal in February 2021. **205** The January 2022 version has been strongly criticized by human rights organizations like Free Expression Myanmar and multistakeholder coalitions like the Global Network Initiative. **206** The draft's status was unclear at the end of the coverage period.

The military imposed an amendment to 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 Myanmar's foreign relations. **207** The 2004 Electronic Transactions Law also criminalized an ill-defined range of 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. [208]

In February 2021, the military ordered an amendment to the penal code to strengthen punishments for treason and sedition, [209] and added an extremely vague offense under a new provision, 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. [210] The military used Article 505A thousands of times during the coverage period to punish dissent, including online (see C3). [211] The amended penal code contained other provisions that have been used to a lesser extent, including a revised version of the existing Article 505(a), which criminalizes encouraging officials to mutiny, and Article 505(b), which bans causing fear or alarm in public. [212]

In March 2021, the military imposed martial law in many areas. Martial law prescribes capital punishment for crimes including treason, inciting disaffection toward the government or military, and disrupting the government or military. [213] The move also brought the enforcement of the News Media Law, the Printing and Publishing Law, the Electronic Transactions Law, and Articles 505 and 505A under the jurisdiction of military courts in areas under martial law. The military continued to increase the number of areas under martial law during the coverage period. [214]

The Telecommunications Law was enacted by a military-backed civilian government in 2013. It was intended principally to deregulate the market, but it also included new criminal provisions for legitimate digital activities; Article 66(d) addresses defamation, while Article 68 penalizes disinformation. [215] The law was amended in 2017 after significant criticism of the misuse of Article 66(d) to punish dissent, but the changes had no discernible impact. [216] 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. [217]

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, prescribes prison terms of up to three years for defamation. **218** The defamation provisions were amended in 2020 but were still used to prosecute individuals for online speech (see C3). **219** In February 2021, the military suspended parts of the law, including its limited protections against surveillance and the interception of private messages. **220**

The Trademark Law, adopted in 2019, penalizes trademark infringement and counterfeiting with up to three years' imprisonment and a fine of approximately 5 million kyat ($2,400). **221** It was adopted alongside the Patent Law and the Industrial Design Law, which also include criminal sanctions for violations. **222** Later in 2019, lawmakers adopted a copyright measure that includes prison terms of up to three years for commercial copying without consent. **223** Each law applies to online content and could be enforced against internet users.

After the coup, the military began working on a revised hate-speech law that could include punishment for "political" hate speech, which would contradict international human rights standards on the topic. **224** The NLD government had developed a series of draft hate-speech laws in 2017 that were criticized by civil society for being excessively punitive and failing to address Myanmar's significant problem of intolerance. **225** The NLD government in 2020 issued a Directive on the Prevention of Incitement to Hatred and Violence, ordering officials to address the issue of hate speech. **226** The directive came in advance of a reporting deadline set by the International Court of Justice, which was 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

Internet users are frequently punished for their online speech in Myanmar's restrictive legal environment. Military-controlled authorities and courts continued to engage in arbitrary and disproportionate arrests, including of internet users, and imposed extreme sentences during the coverage period. As of May 31, 2023, the Assistance Association for Political Prisoners reported that 22,842 civilians and activists had been arrested since the coup, and that 4,320 had been released. **227**

Free Expression Myanmar reported that nearly 4,000 people were identifiably arrested, detained, charged, or imprisoned under penal code Articles 505 and 505A in the year after the coup; of those, 1,269 people remained in pretrial detention and 143 had 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. **228** Many of these cases were likely related to the individuals' online activities, though specific numbers have been 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. **229** At least 175 journalists, all of whom were affiliated with media outlets that published online, have been detained since the coup, and at least 62 reportedly remained in prison as of December 2022. **230** The majority of imprisoned journalists were detained, charged, or sentenced under Article 505A. **231** Sai Zaw Thaike, a photojournalist for the news site Myanmar Now, was detained in May 2023 for covering the aftermath of Cyclone Mocha; he was sentenced to 20 years in prison in September. **232** Other provisions have also been used against journalists; for example, Hmu Yadanar Khet Moh Moh Tun was sentenced to a total of 13 years in prison, including a 10-year sentence under the Counterterrorism Law handed down in May 2023, for her coverage of a 2021 flash-mob protest that had been organized online. **233** Many journalists, like Ma Thuzar, have been arbitrarily arrested and detained for reporting on protests against the coup. **234** Journalists' relatives have been targeted by the military as well. For example, when

journalist Htet Htet Aung, who reported for the online outlet Thingangyun Post, was detained, her seven-year-old daughter was also held and questioned for two days before being released. **235**

Some 25 percent of those imprisoned under Articles 505 and 505A in the year after the coup were health workers, 13 percent were educators, and 9 percent worked in creative fields, including music. **236** Thousands of students, civil society activists, and politicians have also been detained since then, according to the Assistance Association for Political Prisoners. **237** For example, a young woman from Bago Region was arrested in January 2023 for urging people online to boycott the military-controlled education system. **238** Two women were arrested in Sagaing Region in March 2023 for sharing media outlets' Facebook posts about the civil conflict. **239** At least 60 prominent celebrities were on warrant lists as of April 2021, **240** and many had not engaged in political commentary prior to the February 2021 coup. **241** For example, social media influencer Aung Chan Aye was detained in January 2023 upon his return from Thailand due to his earlier participation in anticoup activities. **242** In September 2022, a woman celebrity who had participated in protests against the coup was sentenced to six years in prison under the Electronic Transactions Law for "harming culture" by posting nude images on the adult subscription site OnlyFans. **243**

Hundreds of people who have avoided being brought into custody have faced other penalties. **244** For example, the military has confiscated the property of absent dissidents, such as the home of Thalun Zaung Htet, editor of online outlet Khit Thit Media, which was seized in February 2022. **245** Individuals who do not receive a custodial sentence after arrest are still forced to delete content. **246**

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**1** / 4

Score Change: The score declined from 2 to 1 because the military enforced mandatory SIM-card registration and threatened people who used circumvention tools, undermining access to secure and anonymous communications.

Users' ability to communicate anonymously has been further restricted by the military since the coup. In March 2021, daily directives from the junta banned the use of VPNs, though some orders barring VPN use had already emerged the month before. **247** 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. **248** Although the blocking limited some people's ability to use circumvention tools, internet users continued to employ them. The military has also conducted random street searches of peoples' devices in order to inspire fear of surveillance. **249**

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). **250** Businesses in Myanmar condemned the proposal as unworkable, as most applications and systems use VPNs for security purposes. **251** Despite the law not being formally adopted, military officers searching people's devices in public places reportedly threatened to arrest those with VPNs installed and extorted bribes from the affected individuals. **252**

Anonymity is limited by mandatory SIM-card registration requirements. After the coup, the military required all subscribers to reregister their SIM cards. In September 2022, authorities warned that SIM cards would be permanently blocked if they had not been reregistered with correct data by January 2023. **253** The military has also called for mandatory registration of the IMEI numbers of all devices, with those that are not registered risking exclusion from telecommunications services; the demand was ostensibly linked to the collection of registration fees (see A2), though it was not yet enforced during the coverage period. **254**

It is unclear whether the military has continued to advance plans for biometric registration that were initiated prior to the coup. In 2019, the NLD government had issued a tender for a biometric SIM-card registration system, **255** which would include fingerprints and facial-recognition information. **256**

There are no clear legal restrictions on encrypted communications, though vague provisions in the Telecommunications Law and the Electronic Transactions Law could be interpreted to restrict the technology.

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 efforts have grown since the coup, dovetailing with its comprehensive offline capacity to intrude on citizens' privacy. Immediately after the coup began, the military unlawfully suspended parts of the Law Protecting the Privacy and Security of Citizens, including modest safeguards against warrantless surveillance and interception of private messages. **257**

During the coverage period, the military introduced new bylaws to the 2014 Counterterrorism Law, including a new chapter that grants the authorities sweeping powers to intercept, block, or restrict mobile and electronic communications without court oversight or any other form of due process. **258**

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). **259** Although the draft had not yet been enacted during the coverage period, 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 Electronic Transactions Law grants the

authorities broad powers to inspect any device on vague bases such as "misuse." **260**

According to a May 2021 Reuters report, former military officials pressured service 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. **261** A January 2023 report by the Israeli newspaper *Haaretz* indicated that the technology, sold by Israeli company Cognyte, had been due to go live in June 2021. The technology's operational status remained unclear during the coverage period. **262** The military's Public Relations and Information Production Unit, known as the Ka Ka Com, reportedly had a network of teams comprising hundreds of soldiers nationwide that were responsible for identifying suspects online and infiltrating their networks; **263** military surveillance networks also utilized information from the devices of detainees, **264** and from security cameras equipped with facial-recognition technology. **265** The communications of soldiers themselves are also under surveillance by the military leadership to identify possible defectors. **266**

Soldiers conduct physical surveillance of devices through random spot-checks and at fixed checkpoints, looking for censorship circumvention tools or politically sensitive content in photo albums, messages, and social media posts. **267** Forensic search technology was reportedly active in Myanmar prior to the coup: police have used products from the Israeli company Cellebrite since 2016. **268** The malware product FinSpy was reportedly in operation in Myanmar as of 2019. **269**

Before the coup, the NLD government had invested in acquiring interception capacity, including by ordering service providers to install the technology that the military later activated after the coup. **270** The NLD government spent $4.8 million on such technology, **271** allocated to the Social Media Monitoring Team (SMMT), **272** a body established under the MoTC. **273** The NLD government argued that the SMMT was necessary to counter individuals who were causing "instability" online, for example

through hate speech and defamation. **274** Little was known about the SMMT's operations or whether there was any independent oversight, **275** but civil society activists assume that the unit is now being used by the military. **276** The SMMT spent its budget on tools from vendors based in Canada, the United States, Sweden, and Israel, among others. **277** 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

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

Myanmar lacks a robust data protection law, despite years of calls from a range of stakeholders in the private sector and civil society. **278** The military imposed amendments to the Electronic Transactions Law in February 2021, adding a new chapter on personal data protection that 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. **279** The amendments notably oblige data controllers to submit information to state authorities without adequate protections for user privacy.

The Law Protecting the Privacy and Security of Citizens, passed in 2017 and partially suspended since the coup, **280** 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 governing how data can be collected, stored, or destroyed, nor does it provide for judicial review. The law's definition of privacy is inadequate and

inconsistent with international human rights standards. **281**

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." **282** The Telecommunications Law also authorizes the government 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. **283** 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. **284**

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 would also impose broad retention requirements for user data. **285**

There is little room for service providers to push back against the military's instructions, and the military's direct or indirect control of the country's providers facilitates even more seamless 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, **286** compared with 188 requests in 2019 and about 70 in 2018. **287** Telenor reportedly complied with all of the requests submitted after the coup; each required call records and call locations spanning months, and in total they covered thousands of users. **288** 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 then. **289**

In at least one instance, 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. **290**

The military has increased regulatory requirements for digital payment operators in an effort to track down donors to the prodemocracy opposition movement. **291** Operators are required to verify their customers' identities and transaction records, and to submit such records to the authorities. **292** Penalties for opposition supporters are extremely punitive, and several young women have received 10-year prison terms, in each case for transferring the local equivalent of less than $10 to an opposition group. **293**

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 its proxies continued to threaten, extort, physically assault, forcibly disappear, torture, and kill online and offline opponents with complete impunity during the coverage period. Many people in Myanmar face extralegal intimidation and violence on a daily basis amid ubiquitous military propaganda, constant surveillance, and physical searches, including of devices. **294**

The military has used threats and violence against people who supported online resistance or participated in protests, the CDM, and political opposition groups, especially the NUG itself (see B8). **295** The unlawful imposition of martial law (see C1) and the threat of capital punishment had an intimidating effect among protesters, strikers, political activists, journalists, and human rights defenders. **296** By March 2023, at least 100 people, including two children, had received death sentences from military courts, and at least four had been executed. **297** In July

2022, the military executed Phyo Zeya Thaw, Kyaw Min Yu, Hla Myo Aung, and Aung Thura Zaw, marking the country's first use of the death penalty in decades.

More than 3,500 people are confirmed to have been killed in military crackdowns between February 2021 and the end of the coverage period, and some were targeted in relation to their online activities. **298** They included at least four journalists working for or previously employed by online media outlets. **299** 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; his body showed signs of torture. **300**

At least 20 civil society workers and activists, and over 120 students, were also among those killed since the coup. **301** In March 2023, for example, Thit Sann Oo reportedly died in detention, having been arrested in September 2022 for his social media posts criticizing the military. **302** In March 2021, activist and teacher Zaw Myat Lynn was tortured to death after being detained for sharing videos online that showed soldiers attacking demonstrators. **303**

Hundreds of other people, including children, have been killed in military custody since February 2021, **304** most of them due to torture. **305** Torture in general remains rampant, sometimes taking the form of sexual violence. **306** Those who have suffered severe torture include a cofounder of the online outlet Kamayut Media, Han Thar Nyein, who was subsequently sentenced to two years' imprisonment in March 2022. **307**

An unknown number of protesters, human rights defenders, activists, and others who engaged in prohibited activity online remained in detention during the coverage period. The military also collected the social media profiles of all individual soldiers and leveled threats against them for any banned online activity, **308** including their VPN-enabled use of Facebook. **309** "Watermelons," or individuals who outwardly support the military but actually prefer the prodemocracy movement, came

under attack during the coverage period. Promilitary users with large followings called for information on "watermelons" and doxed those they accused; such users have also offered bounties for their targets' deaths. **310**

Soldiers, nationalists, and other military proxies, such as members of the "Blood Comrades" group, also tracked down social media users who were opposed to the military, **311** and issued threats, **312** particularly on Telegram. **313** People suspected of opposition activity online after being released from custody were warned that their profiles were under surveillance and that they could be returned to detention. **314** Activists, journalists, human rights defenders, and other dissidents have been regularly doxed since the coup, usually over Telegram, TikTok, and Facebook. **315** While men were typically smeared by military proxies as "terrorists," women faced various forms of sexual intimidation, such as nonconsensual sharing of sexually explicit images—including fabricated images—and calls for offline punishment. **316**

Human rights defenders had faced intimidation and violence prior to the coup. The scale and volume of threats against such activists, 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, **317** exacerbated by the proliferation of anti-Rohingya content on Facebook (see B5). **318** Allegations of torture were also made against police, prison guards, and border guards by student activists, **319** monks, **320** and others. **321** Women reported regular gender-based intimidation and threats of violence online. **322** Common harassment tactics included cyberstalking, phishing, doxing, hacking, and attempts to cast doubt on women's credibility, integrity, and character. As in the period after the coup, many were intimidated through fabricated 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, and the military has reportedly attempted to recruit hackers. **323**

Human rights defenders, journalists, and political activists continued to report regular, often weekly, attempts to hack their devices, email, and social media accounts during the coverage period. **324** Advanced espionage malware, thought to originate in China and be state sponsored, **325** has repeatedly been found hidden in widespread Burmese-language fonts that are commonly shared via USB sticks or available for download online, including on the national presidential website as of June 2021. **326** Several media outlets claim to have had their Facebook and YouTube accounts hacked since the coup, before later restoring them. **327** 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. **328**

In 2021, several government websites, including those of the central bank and state television stations, were hacked and defaced with anticoup messages. **329** Some 330 GB of government-held corporate financial data was leaked in February 2021, including details on how military-controlled firms and coup leaders used Google services. **330**

Advanced spyware has been identified in Myanmar, **331** and human rights defenders, journalists, and political activists have reported the presence of spyware on their mobile phones (see C5). **332**

Footnotes

1. Simon Kemp, "Digital 2023: Myanmar," Datareportal, February 13, 2023, https://datareportal.com/reports/digital-2023-myanmar?rq=myanmar. See previous Freedom on the Net reports.
2. "Myanmar," Digital Development Dashboard, International Telecommunications Union, accessed April 24, 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...
5. "Digital 2023: Myanmar," Datareportal, February 13, 2023, https://datareportal.com/reports/digital-2023-myanmar?rq=myanmar;

More footnotes