Freedom House

FREEDOM ON THE NET 2020

# Myanmar

NOT FREE

**31** /100

| | |
|---|---|
| A. Obstacles to Access | 7 /25 |
| B. Limits on Content | 13 /35 |
| C. Violations of User Rights | 11 /40 |

LAST YEAR'S SCORE & STATUS

36 /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

Internet freedom in Myanmar declined dramatically, as the government ramped up its censorship ahead of elections expected in November 2020. The government has shut down mobile internet access in parts of Rakhine and Chin States since June 2019, taking over a million people offline. Moreover, authorities ordered service providers to block independent and regionally based news outlets in March 2020. The military and ruling party continued manipulating online content, while users were hesitant to discuss sensitive topics such as gender, the predominantly Muslim Rohingya ethnic group, and conflicts in Rakhine, Shan, and Kachin. Worryingly, some individuals who criticized the government online faced prosecutions and even prison time under a range of laws, including the repressive Telecommunications Law.

Myanmar's transition from military dictatorship to democracy has faltered under the leadership of the National League for Democracy (NLD) party, which came to power in relatively free elections in 2015 but has failed to uphold human rights or bring security to areas affected by armed conflict. The military retains significant influence over politics, and the government's 2017 military operation that forced more than 700,000 members of the Rohingya to flee to Bangladesh remains a point of international concern. Journalists, demonstrators, and ordinary people risk legal charges and detention for voicing dissent.

# Key Developments, June 1, 2019 - May 31, 2020

- In June 2019, the government cut off mobile internet for over a million people in parts of Rakhine State and Chin State, areas where the military has conducted crackdowns, first against the Rohingya, and more recently against the Rakhine ethnic group. The shutdown continued as of September 2020 (see C3).
- In March 2020, the Ministry of Transport and Communications (MoTC) issued a

series of directives ordering internet providers to block websites, such as Narinjara News, Mandalay In-Depth News, Mekong News, Voice of Myanmar, and Karen News (see B1 and B3).

- The government reportedly threatened to cancel licenses unless license-holders complied with demands to block websites (see A4).
- From February through June 2020, the online #StopInternetShutdownMM campaign was combined with offline protests to call for an ending to the shutdowns in Rakhine and Chin States. Some offline demonstrators faced criminal charges for protesting without the necessary government permission (see B8).
- Internet users continued to be prosecuted, convicted, and sentenced to prison under the Telecommunications Law and the Law Protecting the Privacy and Security of Citizens (see C3).
- In November 2019, authorities released a tender to create a database that can store up to 70 million records of biometric data as part of its efforts to institute new biometric sim card registration requirements (see C4).

# A. Obstacles to Access

*Internet access continues to improve in Myanmar, as more users connect via smartphones with fast fourth-generation (4G) technology. However, in June 2019 the government implemented a draconian internet shutdown affecting over a million people across conflict-ridden areas in the Rakhine and Chin States. Continuing into 2020, it is one of the longest-running shutdowns in the world.*

**A1** 0-6 pts

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

Access to the internet continued to improve during the reporting period. As of 2020, 41 percent of the population used the internet, an increase of one million people since the beginning of 2019. [1] The speed and quality of service have increased in

recent years due to the launch of 4G services in 2017, [2] and international bandwidth reached 445 Gbps in 2018, 15 times higher than 2013. [3] However, the overall number of users remains lower than the average for the Asia-Pacific region, [4] and internet speed is comparatively slower, particularly through fixed-line connection. [5]

Private fixed-line internet connections remain rare, and while fixed-line speeds increased during the coverage period, they remain slower than mobile connections. [6] As of 2017, only 1 in 1,667 people has a fixed broadband line, compared to 1 in 10 on average across the Asia-Pacific region. [7]

The number of mobile connections has continued to grow, increasing to 68 million in January 2020, which is equivalent to 126 percent of the population. [8] Despite this growth, the percentage of the population with a mobile connection is lower than in neighboring countries. [9] Just over 50 percent of the population has mobile connections, and many people have multiple SIM cards. [10]

Infrastructure development continues to be a challenge, with flooding and unreliable electricity hampering connectivity, while an inefficient bureaucracy and private and public corruption limit growth and improvement in the sector. [11] New sanctions adopted in the wake of the Rohingya crisis have also been applied to the export of telecommunications equipment to Myanmar, although it is unclear whether or how the sanctions have affected infrastructure development. [12] Meanwhile, infrastructure has been damaged by a range of problems such as rodents, car accidents, and construction. [13]

**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?** | **1** /3 |
|---|---|

The internet became accessible to more people during the coverage period. Mobile data plans are affordable relative to other countries in the region. [14]

Prices for fixed broadband lines have continued to decrease, dropping on average by

half between 2018 and 2020, though prices vary by region. **15** The costs of fixed-line connections have decreased due to competition with 4G and a dearth of demand from customers. The average fixed-line connection now costs $37 per month in urban areas, which remains prohibitively expensive for the majority of the population.

The Digital Economy Development Committee (DEDC) was launched in 2017 to support and develop economic policies that promote a digital economy. **16** In March 2019, the DEDC launched its Digital Economy Roadmap, which includes several plans to build digital inclusivity, improve connectivity, and harness technology to foster socioeconomic development. **17** The DEDC had met only twice by mid-2019 and has thus far largely operated in secret, without significant public consultation. **18** The DEDC's Facebook page and website have not been updated since 2018 and 2017, respectively. **19** Although the Roadmap divides responsibilities among different ministries, how much, if any, budget has been allocated to operationalizing it is unclear.

National figures on internet access hide a digital divide that affects marginalized groups. Urban users who have access to 4G consume almost five times more data on average each month than the national average for all users. **20** The number of households, particularly in rural areas, that have access to a computer or to the internet remains small. **21** Users in rural areas and small towns have poorer internet connections than those in urban areas.

In recognition of the geographical disparity in people's internet access, the government announced the development of a Universal Service Fund (USF) in April 2018 to invest in telecommunications services for areas that are otherwise underserved, with the eventual aim of reaching 99 percent of the population. **22** The USF is supported by a new 2 percent telecommunications tax that was rolled out in mid-2018. **23** However, at least some of the USF has since been reallocated into paying for a new proposed biometric database for mobile subscribers. **24**

Gender-based disparities in access are generally ignored by the government. Women are still less likely than men to own a mobile phone and significantly less likely to use the internet. **25** For women, barriers to owning and using a mobile phone to access

the internet include affordability, literacy skills, and security and safety concerns. [26]

**A3** 0-6 pts

| **Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?** | **1** / 6 |
|---|---|

*Score Change: The score declined from 4 to 1 due to the government's shutdown of mobile internet services in parts of Rakhine and Chin States, which has been in place since June 2019.*

While the government previously refrained from restricting connectivity, the coverage period saw one of the longest internet shutdowns in the world.

In June 2019, the government cut off mobile internet for over a million people in parts of Rakhine State and Chin State, areas where the military has conducted crackdowns, first against the Rohingya, and more recently against the Rakhine ethnic group, in order to "maintain the stability and law and order." [27] On August 31, 2019, the government restored mobile access in about half of the impacted area, but this decision was reversed in February 2020. [28] As of September 2020, the restrictions were still in effect for approximately 1.4 million people. [29] Members of parliament, journalists, human rights defenders, and civil society have spoken out about the damaging effects and the economic cost of the shutdown on an already marginalized and underdeveloped population. [30] The government has said that it will restore access when the security situation improves, [31] and a presidential spokesperson said that the government would "fulfil every request made by" Myanmar's military with regards to the shutdown. [32]

The Ministry of Transport and Communications (MoTC) has the power to cut off the internet without oversight or safeguards, as it owns and controls much of the telecommunications infrastructure via the state-owned Myanmar Posts and Telecommunications (MPT). However, private providers are gradually diversifying ownership of mobile infrastructure and the internet backbone. Myanmar has seven internet gateways. Because experts project bandwidth demand will grow 70 percent annually in the near future, more companies are expected to develop infrastructure,

including through new satellite connections. [33] [34] New private internet gateways are thus making the international connection more resilient.

Myanmar has 68,000 kilometers of fiber-optic cable. [35] The first private undersea internet cable, the Myanmar-Malaysia-Thailand-International Connection (MYTHIC), was installed by the Campana Group, a company based in Singapore and jointly owned by Myanmar and Thailand. It began selling wholesale to telecommunications companies in 2017. [36] Campana Group plans to build a second undersea cable, called SIGMAR, to be launched in 2020 with enough bandwidth to serve for at least 10 years. [37] Myanmar's government plans to launch a second satellite, MyanmarSat-2, in 2020 to support telecommunications infrastructure. [38]

The legal framework has no specific regulations relating to bandwidth throttling, but many legal provisions are vague and broad, meaning that they can be misused for such purposes. A draft cybersecurity law under consideration could include restrictive provisions that affect Myanmar's internet infrastructure (see C2). [39]

**A4** 0-6 pts

| **Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?** | **2**/6 |
|---|---|

Although the government has awarded a number of telecommunications licenses, giving a mobile operating license to a military-owned telecommunications company has increased the state's control over telecommunications and restricted the diversity of the market. Providers face a range of obstacles to effectively operate.

Myanmar has seen a proliferation of telecommunications licenses awarded since 2013, when deregulation removed many of the legal and regulatory barriers to entry for internet service providers (ISPs) and mobile service providers. At least 137 telecommunications licenses have been awarded, [40] and the share of subscribers using state-controlled mobile service providers is just above 50 percent. [41] The 2017 award of a telecommunication license to the military-owned operator Mytel, and the comparative scale of Mytel's investment since launching in 2018, has undermined the diversity of providers and reasserted the state's dominance over the

telecommunications market.

Mytel is jointly owned by the Vietnamese military–controlled company Viettel, a consortium of local firms, and Star High Public Company, which is owned by the Myanmar military's Myanmar Economic Corporation (MEC). **42** Mytel operates using the telecommunications infrastructure owned by MECTel, which is also owned by MEC. **43** MEC was sanctioned by the US Treasury Department between 2008 and 2016 for its role in the human rights violations committed by Myanmar's military. **44** Some activists have called for a boycott of Mytel due to the company's connections with the military and human rights violations. **45** In 2018, the European Union considered applying sanctions to Mytel in response to the military's human rights abuses in Rakhine, Shan, and Kachin States. **46**

Mytel launched its 4G-only service in February 2018, **47** and had reportedly reached eight million subscribers by 2020. **48** It joined three other mobile service providers in Myanmar, all of which are owned by the Myanmar government or foreign governments. **49** Two foreign mobile service providers, Telenor and Ooredoo, have 21 and 10 million subscribers, respectively, and a third provider, the state-owned MPT, has 24 million subscribers. **50** Other providers that have received telecommunications licenses include a mixture of national and local fixed-line and mobile services. For example, Amara Communications, owned by a large domestic conglomerate, launched in May 2018 and provides a data-only service using MiFi boxes, including in Yangon, where it had already installed 300 towers by March 2018. **51** The Global Technology Group launched wireless broadband in 30 cities beginning in May 2018. **52**

The administering of licenses has been generally regarded as fair and transparent, and external efforts to influence decisions have been largely rebuffed. **53** However, in 2020, the government reportedly threatened to cancel licenses unless license-holders complied with demands to block websites, including news outlets (see B1). **54** Telecommunications providers have raised concerns about restrictions on building new towers, **55** and local government officials have stressed the need for providers to obtain permits to lay fiber-optic cables, build towers, and install Wi-Fi devices. **56**

**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?** | **1** / 4 |
|---|---|

Myanmar's regulatory bodies remain vulnerable to political interference and lack transparency. The MoTC's Posts and Telecommunications Department (PTD) is responsible for regulating the telecommunications sector. Under previous governments, the PTD was the regulator and a monopoly service provider for the telecommunications sector. These roles have now been separated, with the PTD acting as the regulator and the MPT acting as the state-controlled service provider. The PTD's responsibilities include issuing and renewing telecommunications licenses, regulating the frequency spectrum, addressing consumer protection, inspecting and supervising telecommunications providers, and carrying out any administrative actions against providers. **57**

However, both the PTD and MPT lack proper safeguards to protect regulatory and operational independence, making them vulnerable to political interference. For example, presidential spokesperson, Zaw Htay, said in regard to the long internet shutdown that the government would "fulfil every request made by the [military]" (see A3). **58** Furthermore, the bodies' decision-making processes are opaque and they rarely engage or consult with civil society. **59** Article 86 of the 2013 Telecommunications Law outlines a Myanmar Communications Regulatory Commission (MCRC), which is yet to be established. **60** Even though the mandate for the MCRC's composition does not sufficiently safeguard the commission's independence, the Telecommunications Law dictates that the MCRC take over regulatory functions from the PTD. Further, the commission would institute a mechanism to adjudicate any administrative issues in the telecommunications sector. Many analysts believe that the government's failure to establish the MCRC is due to its unwillingness to relinquish the direct control it has over the telecommunications sector through the PTD. **61**

In February 2020, Facebook removed 23 pages and accounts which it said were linked to Vietnam's Viettel and Myanmar's Mytel service providers. **62** Facebook reported

that the pages were posing as news outlets and fake customers sharing reviews about the alleged failures of competing companies. **63**

The Pricing and Tariff Regulatory Framework showcases how telecommunications rules favor state-owned service providers. The framework, an initial set of rules for mobile service providers, came into force in 2017 and included new floor pricing and a ban on offering free SIM cards or supplying telecommunications services below cost, among other rules. The rule on floor pricing included a minimum charge for data ($0.00065 per 1 MB of data), calls, SMS, and other services. The floor pricing, which was more expensive than some providers' prices at the time of adoption, was established for all providers to follow. However, the government waived floor pricing for the military-owned Mytel, reportedly to enable it to achieve rapid growth when it was first launched. **64**

Another state institution, the Myanmar Computer Federation, which was formed under the 1996 Computer Science Development Law and is comprised of industry professionals, is the designated focal point for coordination with technology-related associations, working groups, and other stakeholders in the sector. Civil society groups have raised concerns that the federation is progovernment and operates opaquely. **65** For example, the federation's leadership has supported some of the government's more draconian digital surveillance policies. **66**

# B. Limits on Content

*The coverage period saw an escalation in technical censorship, with the government ordering the blocking of independent and regionally based news outlets in March 2020. Civil society and ordinary users responded to both the website blocks and internet shutdown with a combination of digital campaigns and offline activism. Self-censorship on a range of subjects, including the military, corruption, and the Rohingya, remains high. Social media companies have responded to pressure by opaquely increasing content removals, even when the content is legitimate. There is a lack of diversity in the ownership and content of online media outlets. Meanwhile, the government and military actively promote their own narratives online and reject much independent reporting as "fake news."*

**B1** 0-6 pts

| Does the state block or filter, or compel service providers to block or filter, internet content? | 3/6 |
|---|---|

*Score Change: This score declined from 6 to 3 due to new website blocks that notably impacted independent and regional news outlets reporting on developments in conflict areas.*

While the government refrained from blocking or filtering content prior to 2020, the Ministry of Transport and Communications (MoTC) ordered ISPs to block websites in March 2020, including independent and regional news outlets. **67**

In March 2020, MoTC issued a series of directives ordering internet providers to block 2,147 websites under Section 77 of the Telecommunications Law, which allows for authorities to issue blocking orders to license-holders under "emergency situations." Although the directives have not been publicly released, well-known independent and local news outlets and websites based in conflict-ridden areas were then blocked, including Rakhine State, such as Narinjara News, Mandalay In-Depth News, Mekong News, and Voice of Myanmar, among others. Karen News, a Karen State local news agency, was also found to be inaccessible. Several blocked outlets are owned by the Development Media Group, which previously has been targeted by authorities for their coverage of the Arakan Army (see C3). **68** According to Telenor Myanmar, 67 websites were requested to be blocked for alleged "fake news," and 154 websites for adult or explicit content. The remaining 1,917 websites included in the MoTC's directives are also on Interpol's list of banned child sexual abuse websites, content which can be legitimately restricted under international human rights standards. **69**

Major telecom providers complied with the blocking orders. Telenor Myanmar, however, initially resisted the blocking of 67 websites for alleged "fake news," citing a lack of a sufficient legal basis. **70** The provider later complied, after meeting with MoTC and determining that the "risk involved in not following the directive as regards [sic] fake news is likely to have wider implications in terms of servicing the

public." [71] In May 2020, Telenor reported that the PTD issued a directive for service providers to block an additional 22 websites that contribute to "fearmongering" and "misleading" people about COVID-19. [72]

Again in August 2020, after the coverage period, the provider announced that the PTD ordered service providers to block a website and three associated IP addresses. [73] The civil society group Justice for Myanmar reported that its website was blocked, with a message saying the page "has been blocked per directive received from the Ministry of Transport and Communications of Myanmar" when trying to access the site. Justice for Myanmar is a group of activists that had previously exposed corruption among the military.

Since the website blockings began in March, civil society has initiated campaigns to raise public awareness of the blocks. [74] Given the lack of transparency around content restrictions, it remains unclear whether more directives have been issued and testing for restrictions is ongoing (see B3).

In 2012, the government lifted all prior censorship of traditional and electronic media, with the exception of films, dissolving the Press Scrutiny and Registration Division shortly thereafter. The government does not actively publish blocking and filtering lists.

**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?** | **1** / 4 |
|---|---|

Pressure to remove content continues to originate from state and nonstate actors both within Myanmar and from outside the country. Google, Twitter, and Facebook have not reported any official requests for content removals from the government. [75] Facebook does not declare how many private restriction requests it receives, but has reported restricting access to some allegedly defamatory content. [76] There are no publicly available reports on formal government or court requests for publishers and content hosts to remove content.

However, the government employs other channels to pressure social media platforms and users. The government continues to call for content hosts and platforms, notably Facebook but also WhatsApp, to address rampant intolerance, misinformation, and incitement on their platforms. **77** But the government itself has failed to tackle these problems and individuals linked to the government are often alleged to be responsible for perpetrating them. **78**

Ahead of elections expected in November 2020, the Union Election Commission has announced the establishment of its social media monitoring mechanism to flag and remove content that is hateful and harmful to the vote. While the Commission has reported that Facebook agreed to remove flagged content, Facebook had not confirmed its participation as of May 2020 beyond working with the Commission generally in the lead up to the vote. **79**

Civil society organizations have also pressured digital platforms to remove content, particularly after investigative reports on inflammatory online content that encouraged violence against the Rohingya people. **80** Some organizations are concerned that the quantity of problematic content, much of it organized, will increase in the run up to the 2020 general elections. **81**

Partially as a result, Facebook has increased its moderation practices and the use of its automated filtering mechanisms to remove content. **82** According to the company, it has removed hundreds of pages and accounts on Facebook and Instagram originating within and outside of Myanmar—accounts with millions of followers—for violating its community standards. **83** Removals included the accounts and pages of Commander-in-Chief Min Aung Hlaing of the Myanmar Armed Forces, the military's Myawaddy television network, and other military leaders, **84** as well as nonstate actors such as the ultranationalist anti-Muslim monk Wirathu and pages run by the Buddhist ultranationalist group Ma Ba Tha. **85** In August 2019, Facebook removed 89 accounts and 107 pages—some of which the platform claims are associated with the military—for engaging in "coordinated inauthentic behavior." **86** The pages and accounts of the Arakan Rohingya Salvation Army (ARSA), Arakan Army, Myanmar National Democratic Alliance Army, Kachin Independence Army, and Ta'ang National Liberation Army were also removed because Facebook considered

them "dangerous organizations." [87] This designation meant that any content and pages supporting these individuals or groups could also be removed once identified. However, the consequence of the increasing number of takedowns has been that legitimate content has been removed as well. [88]

A 2020 survey of journalists conducted by Free Expression Myanmar found that Facebook had warned a third of the participants that their journalistic content violated the platform's Community Standards. [89] Of those surveyed, 15 percent have had content removed.

Activists, particularly women and religious minorities, reported being subjected to violence or threats intended to force them to remove their own content. [90] Pressure to remove content is also prevalent in coordinated reporting campaigns. In these campaigns, users exploit Facebook's mechanism for reporting content that violates the platform's community standards in order to disable pages or temporarily limit users' ability to post or send messages, although Facebook has stated that such actions have been prevented. [91] Activists argued that progovernment and military users carried out a targeted campaign to report the content of pro-Rohingya and human rights groups.

**B3** 0-4 pts

| **Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?** | **1** / 4 |
|---|---|

A number of restrictions on digital content lack proportionality and transparency. The Telecommunications Law includes a broad provision giving the MoTC the absolute power to temporarily block and filter content "for the benefit of the people." [92] The law does not explicitly hold intermediaries liable for content, although some provisions are vague and could feasibly be used for content removal. [93] There are also no avenues for appealing restrictions, [94] and the only potential safeguard against abuse, the MCRC, has still not been established (see A5).

In lieu of the MCRC, the PTD retains control over content restrictions. The PTD does not publish procedural information on how or when any such decisions are made,

and by whom. Government directives ordering the internet shutdown in Rakhine and Chin States, and ordering website blocks, have not been published, and users have had to rely on telecommunications companies and civil society testing for more information about content restrictions. **95** Recipients of directives are sometimes unwilling to publicize the order's exact terms and there are no reported legal actions to test the directives' lawfulness.

Facebook expanded its appeals process for account and page takedowns **96** after civil society groups continued to raise concerns that the platform's policies had become unreasonable; accounts and pages were being removed, which did not specific issues. **97** Some activists continue to argue that some of Facebook's removals have compromised the public's right to information about important national stakeholders, and that they have swept up a wide range of legitimate content, including commentary on and documentation of human rights violations. **98** For example, some media outlets, journalists, and human rights defenders have alleged that their content has been wrongfully removed, particularly journalistic content covering banned organizations. **99** Despite requests from civil society, **100** Facebook is only minimally transparent about its restrictions.

Facebook is similarly opaque about its new appeals process and does not publish substantial information about content removal decisions. Some in civil society suspect that such opacity masks significant internal problems, such as poorly trained staff who lack contextual and language expertise, problematic and insufficient algorithms, **101** and disproportionate decision-making. **102**

**B4** 0-4 pts

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

Self-censorship online remains widespread, including among journalists. **103** Journalists, online personalities, and ordinary users face a range of pressures to agree with government narratives on matters relating to the military, big business, armed conflict, religion, and certain sensitive social and religious issues. **104** The use

of pseudonyms, which developed during military rule and enables people to speak out with less fear of repercussions, remains common online despite a ban on the practice by Facebook and other social media platforms. **105** Users are also learning to self-censor words and phrases deemed likely to be automatically identified and removed by content hosts such as Facebook, regardless of their legitimacy. **106**

Self-censorship is particularly common in discussing or reporting on the Rohingya. **107** For example, some journalists and media outlets have opted to use terms such as "Muslims" in order to lessen potential backlash online. The discriminatory term "Bengalis" is sometimes used, in an attempt to link the Rohingya to Bangladesh. **108** Pro-Rohingya activists have largely relied on social media and the international media to distribute information about violence and discrimination in Rakhine State, partly because few domestic media outlets are willing to take the security and financial risks of violence and boycotts associated with reporting on the crisis. **109** The online defamation charges laid against Reuters—one of the world's largest media companies—and the convictions of two of their journalists have underlined the seriousness of the threat (see C3). **110**

Self-censorship on gender issues is also widespread online among journalists and human rights defenders. **111** Women discussing sex and women's bodies online are often abused and harassed. **112** For example, while the global #MeToo campaign gained initial traction in Myanmar, some activists claim that survivors of sexual violence now often self-censor, having seen the intimidation faced by other women who have spoken out. **113**

**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 government and the military continue to dominate public discourse and have sought to control information domestically. Despite years of affirming their desire for media freedom, once in power, the ruling National League for Democracy (NLD)

party resolved to retain state-run media, [114] in order to control publicly available information. [115] As a result, the government and the military still control the entire broadcasting sector and a significant portion of print media, including those outlets' online publications, either directly through the Ministry of Information or via joint ventures with private companies. [116] Hopes that the NLD would increase the editorial independence of state-controlled media and joint-venture media outlets have evaporated. [117]

The government sometimes claims to use the Facebook pages of the Ministry of Information, [118] the State Counsellor Office, [119] and the Information Committee, [120] to provide the public with "unbiased" information to combat "fake" reports from international media, often relating to the Rohingya people and conflict.

Manipulated progovernment content has become pervasive online, particularly on Facebook. [121] The military published inflammatory content regularly on Facebook before being banned by the platform in 2018 (see B2). [122] According to multiple sources, nearly 700 military officials were involved in a systematic campaign of disinformation for five years, creating and managing fake Facebook accounts and pages, which were then used to share false, misleading, and inciting content. Organized troll accounts allegedly helped spread the content to reach more users. [123] In 2019, Facebook banned a number of pages and accounts for engaging in "inauthentic coordinated behavior," some of which were allegedly run by persons associated with the military . [124]

Hard-liners who spread derogatory and violent statements about the Rohingya on Facebook, Viber, and WhatsApp, among other social media platforms, have widened their targets to include other marginalized groups. Before being banned by Facebook, the ultranationalist monk Wirathu regularly spread disinformation and false narratives through his posts and videos that were shared by thousands of followers, and which according to critics, have stoked real-world violence. [125] [126] He has compared Muslims to mad dogs and shared images of corpses with text claiming they were Buddhists murdered by Muslims. [127] In 2019 and 2020, false or hateful information has targeted Rohingya, Muslims, women, Rakhine, and others including journalists and activists. [128] Civil society activists are concerned that this will increase

in the run-up to the 2020 general elections. **129**

Alongside propaganda, unintentional misinformation reflecting poor digital literacy or a lack of available and trustworthy information has spread.

**B6** 0-3 pts

| **Are there economic or regulatory constraints that negatively affect users' ability to publish content online?** | **1** / 3 |
|---|---|

A number of laws contain provisions that can place regulatory constraints on users wishing to publish content online. While the provision has not been invoked to date, the 2014 Printing and Publishing Law created a licensing regime for publishing houses, news agencies, and websites, and outlets must register prior to producing content, including for publishing online. **130** The law also contains a variety of vague and overly broad administrative and criminal sanctions for offenses, which include running a website without a license. Licenses can be revoked by the government at any time.

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

**B7** 0-4 pts

| **Does the online information landscape lack diversity?** | **1** / 4 |
|---|---|

Government and military control over public discourse and the media has significantly restricted the diversity of viewpoints online (see B5). Despite Facebook's removal of several official military accounts and pages (see B2), the military's messaging on certain issues, including on the Rohingya conflict and minority groups, have continued to monopolize the online narrative. These viewpoints are presented on state-controlled broadcast media, and then feed into the public narrative on Facebook. Such content is then spread through users with military backgrounds or

other promilitary accounts. **131**

The state's censorship efforts have also affected the diversity of online content produced by independent sources. For example, in 2019 the military requested that the media refrain from saying "civil war" when referring to domestic conflict. **132** In 2017, the government ordered that all media use the term "terrorist" instead of "insurgent" or "militant" when referring to the Rohingya crisis. **133** Also in 2017, the BBC announced that it would end its broadcasting partnership with MNTV after the network repeatedly pulled BBC programs for using "government restricted words," which included the word "Rohingya," according to some analysts. **134** In June 2018, Radio Free Asia (RFA) cancelled its partnership with the Democratic Voice of Burma (DVB) after the government repeatedly attempted to censor the word "Rohingya" on state television. **135** RFA, however, reported that it would still cover Myanmar on social media. **136**

During the reporting period, the most-visited websites in Myanmar were Google, YouTube, and Facebook. **137** However, few people use internet browsers, with most users preferring Facebook apps on their mobile phones. The most popular Facebook pages were all run by media outlets, some of which were foreign and none of which were state-controlled. **138**

**B8** 0-6 pts

| **Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?** | **4** / 6 |
|---|---|

Online tools used to assemble and mobilize remain freely available. Individuals continued to use the internet for activism, some of which has been successful. Many within civil society regard Facebook—more so than the mainstream media—as the best tool to raise awareness about their concerns and prompt a government response. Their efforts have been constrained during the reporting period, however, as Facebook's restrictions on ethnic armed organizations, the military, and ultranationalist groups have impacted public discourse (see B2 and B3).

One of the largest campaigns online during the coverage period was demand for a

proper criminal investigation for Victoria, a child sexually abused in a private nursery in the capital city, Naypyidaw. **139** The grassroots movement grew organically and garnered massive social media coverage, including a large number of users who changed their profile pictures.

During the coverage period, online campaigning under the #StopInternetShutdownMM was combined with offline protests to call for an ending to the shutdowns in Rakhine and Chin States. **140** In February 2020, nine students were arrested for participating in a peaceful, offline protest against the connectivity restrictions that took place without the necessary government permission. **141** In June 2020, after the coverage period, civil society groups organized a virtual protest marking the one year anniversary since connectivity was shut off. **142** Six activists were also arrested in June for their involvement in an offline protest against the shutdown, which included hanging a banner. They were charged under Section 19 of the Peaceful Assembly and Peaceful Procession Law for organizing without notifying the police. **143** In September 2020, one of the activists, Maung Saungkha, was convicted and was fined 30,000 kyats ($22.50) fine, in lieu of spending 15 days in prison. **144**

In 2018, when the military leader Min Aung Hlaing, claimed that the military was more representative of the people than the elected government, a public outcry swept through Facebook with the slogan, "The military doesn't represent me!" **145** After Reuters journalists Wa Lone and Kyaw Soe Oo were imprisoned in September 2018, Facebook profile pictures were replaced with black spots, representing blacked-out websites, and #ArrestMeToo trended on Twitter and Facebook. **146** In another example, the 2017 #SayNOto66d campaign **147** expanded in late 2018 to focus on decriminalizing defamation altogether. **148**

Some of the most significant online activism has been in response to the plight of the Rohingya. Pro-Rohingya digital activists have used social media to strengthen networks within the Rohingya community, including among the diaspora, while simultaneously reaching out to other supporters. **149** Social media has been invaluable for sharing videos, photos, and testimonies of sexual violence, looting, torture, and murder, **150** which mainstream media outlets have largely ignored.

# C. Violations of User Rights

*Criminalization of internet users persisted, including under several criminal defamation laws, while the government has hinted that a draft cybersecurity law could contain provisions punishing online criticism of the government. Intimidation of users remains common, through online surveillance carried out by the government and military. Individuals reporting on or discussing conflicts in Rakhine, Shan, and Kachin States online, and users discussing gender and other so-called "sensitive" issues, experience harassment.*

**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?** | **1** / 6 |

The constitution and other laws in Myanmar fail to protect human rights online. The current constitution, drafted by the military government and approved in a flawed 2008 referendum, states that "enhancing the eternal principles of justice, liberty, and equality" is one of the country's six objectives. **151** The constitution also provides specific—but highly limited—guarantees for citizens to "express and publish their convictions and opinions" **152** and "freely develop literature, culture, arts, customs, and traditions," **153** provided that they are "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." **154** The constitution includes no provisions directly relating to the internet or access to information, although Article 96 and Schedule 1 (8.m) bestow in parliament the authority to establish laws regulating the internet. In February 2019, the government established a joint parliamentary committee to recommend constitutional amendments to address access to the internet and information. **155** Later that year a coalition of civil society organizations put forward their demands relating to freedom of expression. **156** The committee's final recommendations did not include any substantive changes to human rights or internet freedom in particular.

Fair trial rights are often violated in Myanmar's courts: the accused often have no effective representation, they receive limited access to court documents, and judges are inattentive during proceedings. **157** Trials relating to online activity commonly include significant procedural errors, technically unreliable evidence, and deep-seated judicial unwillingness to consult expert testimony. **158** In many cases, courts have been presented with easily forgeable printouts of digital content, or have ruled without testing the authenticity, reliability, or admissibility of evidence. **159**

Judicial independence is impeded by interference. Judges are nominated by the president, and lawmakers can reject the choice only if it is clearly proven that the nominee does not meet the legal qualifications for the post. The courts generally adjudicate cases in accordance with the government's interests, particularly in major cases with political implications.

A number of laws target online media freedom. A 2018 amendment to the Broadcasting Law failed to clarify the country's transfer from analog broadcasting to digital, which created an arbitrary process that could be misused by the government to control broadcasters and online media. **160** In 2018, the Myanmar Press Council, an independent body that settles disputes involving the media, submitted to the government a proposed amendment of the 2014 News Media Law, which regulates digital media. Whether this proposal will positively or negatively affect media freedom is unclear. **161** A draft of a right to information law first proposed in 2017 had not yet passed as of May 2020. **162** Instead, it has been undermined by new information related laws and drafts. In December 2019, the National Records and Archives Law was adopted, limiting access to information and retaining secretive standards for government documents, including electronic documents, while further criminalizing the sharing of them. **163**

**C2** 0-4 pts

| **Are there laws that assign criminal penalties or civil liability for online activities?** | **0** / 4 |
|---|---|

Several laws explicitly penalize online activity and have been used to imprison

internet users. The Telecommunications Law was drafted by the former government in 2013 with the support of the World Bank, **164** and is the primary framework for licensing telecommunications providers, including mobile service providers and ISPs. Although the law was welcomed by many stakeholders as a sign of much-needed change, **165** the former government added a number of troubling provisions, including Article 66(d)—a vaguely worded content provision criminalizing a range of acts online, including defamation—and Article 68, which criminalizes "communication, reception, sending, distribution, or sharing of incorrect information with dishonest intention." **166**

Under public pressure about the number of prosecutions for online activity, the NLD government rushed through an amendment to Article 66(d) of the Telecommunications Law to ameliorate the issue in 2017. However, the amendment was drafted without proper civil society consultation and was roundly condemned as insufficient. **167** Positive changes in the amendment include a reduction of the maximum prison sentence for violations from three years to two years, the opportunity for the accused to be released on bail, and restrictions on who can file a case. However, the amendment did not define defamation and did not alter provisions that outlaw "extort[ing], defam[ing], disturb[ing], or intimidat[ing]" over a telecommunications network. **168** Civil society activists have argued that the amendment has made no discernible impact on cases brought forward after the amendment was enacted. **169**

The penal code can also be used to imprison internet users. Section 505(a) criminalizes speech "with intent to cause, or which is likely to cause, any officer, soldier, sailor or airman, in the Army, Navy or Air Force to mutiny or otherwise disregard or fail in his duty as such." **170** Section 505(b) outlaws speech "likely to cause fear or alarm in the public." **171**

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. **172** The law has been used to prosecute individuals for online activity (see C3).

The previous government amended but failed to repeal the 2004 Electronic Transaction Law (ETL) in 2013, which criminalized "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. The law was routinely used to criminalize internet activism during military rule. In 2014, Thaung Tin, a senior government official, acknowledged the need to address repressive laws like the ETL and the Computer Science and Development Law, which criminalizes unauthorized use of a computer with a "fax-modem card." **173** The government announced plans to revise the ETL in 2014, but no draft legislation has since been announced. **174**

Several draft laws that could affect rights online were considered during the coverage period. In 2019, the government commissioned consultants to assist in developing a new cybersecurity law. **175** Initial drafts of the framework have been shared confidentially with a handful of civil society groups, but the legislation remained at an early stage of development at the end of the coverage period. **176** The government has stated that the new framework will include provisions penalizing those who "insult the country and people and commit crimes over any communications network." **177** Human rights defenders have expressed concern that the framework, like other restrictive laws governing online activity in recent years, would be vague, overly broad, and used to punish a range of online behaviors. **178**

In response to the COVID-19 outbreak, the government put forward a draft Prevention and Control of Communicable Diseases bill in February 2020. The bill includes a provision that imposes fines, and potentially a six-month prison term, for health officials that disseminate certain health information during specified times that could cause fear or panic. **179** Authorities claim the drafted law seeks to prevent causing public panic or the spread of intentionally false information. As of August 2020, the bill remained in draft form.

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 kyats ($3,300). **180** It was adopted alongside the Patent Law and the Industrial Design Law, which also include criminal sanctions for violations. **181** In May 2019, a

copyright law that includes prison terms of up to three years for commercial copying without consent was adopted. [182]

After a series of leaked draft laws criminalizing "hate speech" received significant criticism from civil society, the process of developing a law has largely been done in secret and a bill has not yet been put before parliament. [183] The government claims that consultations with civil society regarding the bill have occurred, [184] but several well-known civil society organizations working on the issue have refuted these assertions and have received no responses to their requests for meetings with parliament. [185] The government issued in April 2020 a Directive on the Prevention of Incitement to Hatred and Violence ordering officials to address the issue of hate speech. [186] The directive came in advance of a reporting deadline set by the International Court of Justice.

**C3** 0-6 pts

| **Are individuals penalized for online activities?** | **1** / 6 |
|---|---|

Internet users are frequently prosecuted in Myanmar's restrictive online environment. In 2019, there were more than 49 criminal cases under the Telecommunications Law and 37 cases under the Law Protecting the Privacy and Security of Citizens, [187] with hundreds of cases being brought in total against social media users. [188] Many plaintiffs in the cases were affiliated with the state, including public officials, NLD party officials, and military officers, while many of the accused were activists, online journalists, or other civil society representatives. [189] Most cases have resulted in guilty verdicts with six-month prison sentences. [190]

In February 2020, Kay Khine Tun, Paing Phyo Min, and Su Yadanar Myint of the poetry troupe Peacock Generation were sentenced to six-months in prison under Article 66(d) of the Telecommunications Law for sharing images of and livestreaming their performance satirizing the military on social media. [191] In December 2019, four members of the group were also sentenced to six months in prison under Article 66(d). [192]

In March 2020, a Yangon court agreed to hear the military's criminal defamation complaint under Article 66(d) against the editor of independent news outlet The Irrawaddy, citing its coverage of clashes between the Arakan Army and the military in Rakhine. **193** The complaint was originally brought in April 2019.

A previous Article 66(d) case against the Myanmar Now editor, Swe Win, filed by supporters of a Buddhist ultranationalist group, **194** was dismissed in July 2019. However, a court accepted an appeal to this dismissal in August 2019, which has had chilling effects. **195** Swe Win was originally arrested in July 2017 for a Facebook post criticizing Wirathu, **196** and was forced to travel 600 kilometers from his home to the court more than 55 times, usually for a session that lasted just minutes. **197**

Internet users were convicted under the penal code during the coverage period. In May 2020, editor Zaw Ye Htet of online news agency, Dae Pyaw, was sentenced to two years imprisonment under Article 505(b), after publishing a story about a COVID-19 death in Karen State, which official numbers from the government contradict. **198** In August 2019, filmmaker Min Htin Ko Ko Gyi was sentenced to one year in prison under Article 505(a) for a series of Facebook posts critical of the Myanmar military. **199** He had been held in detention since April 2019 and was released in February 2020.

Local activists have also identified at least 33 people—including activists, journalists, politicians, and members of the public—who have been charged under the Law Protecting the Privacy and Security of Citizens for posting criticism on social media. **200** For example in November 2019, six ethnic-minority activists were each sentenced to six months imprisonment under the law's criminal defamation provision Article 8(f), for signing a statement criticizing a government official. **201** During the previous coverage period in September 2018, Facebook user Aung Ko Ko Lwin was sentenced to one year imprisonment for Facebook posts criticizing a state chief minister, under Article 8(f). **202** He was originally arrested in January 2018. **203**

In March 2020, chief editor of Voice of Myanmar U Nay Myo Lin was arrested and charged for allegedly violating the country's Anti-Terrorism Law after interviewing a spokesperson for Arakan Army, which was labelled an unlawful and terrorist

organization by the government days before. **204** Police later confirmed they would not pursue the case. **205**

In May 2019, during the previous coverage period, Reuters journalists Wa Lone and Kyaw Soe Oo were pardoned after being imprisoned more than 500 days following their September 2018 convictions for reporting on the massacre of 10 Rohingya men and boys. **206** The journalists had been sentenced to seven years in prison for violating the Official Secrets Act. **207** They were originally detained in December 2017. In June and July 2018, the journalists' defense lawyers informed the court that they had been tortured while in custody (see C7). In March 2020, the military filed and later withdrew a criminal defamation case against Reuters for a January 2020 story citing the military artillery fire that killed two Rohingya women. **208**

In September 2018, during the previous coverage period, Ngar Min Swe, a former columnist for a state media outlet, was convicted of sedition and sentenced to seven years in prison after he posted "abusive" Facebook posts about Aung San Suu Kyi. **209** His posts included sexist remarks about Suu Kyi after she received a kiss on the cheek from former US president Obama when he visited the country.

### C4 0-4 pts

| **Does the government place restrictions on anonymous communication or encryption?** | **3**/4 |
|---|---|

Users' ability to communicate anonymously is limited by the government's enforcement of SIM card registration requirements. **210** Since 2017, subscribers must provide their name, citizenship identification document, birth date, address, nationality, and gender to register for a SIM card; **211** noncitizens must provide their passports. Some subscribers have reported being required by telecommunications companies to include further information beyond the bounds of the regulations, including their ethnicity. **212** Mytel reported in February 2020 that only 30 percent of subscribers had registered. **213** The MoTC order has resulted in over six million SIM cards being suspended or blocked as of February 2020. **214** Amid COVID-19, the MoTC ordered telecommunications providers to bar outgoing calls for the millions of

unregistered SIM cards, starting in April 2020. **215** At the end of June 2020, after the coverage period, unregistered SIM cards were reportedly deactivated, with the corresponding phone numbers expected to be deleted and subscriber money forfeited.

In March 2019, the government also asked mobile service providers to limit each user to two SIM cards in order to protect "personal and national security." **216** It is unclear how this is being implemented by providers.

Over the course of the coverage period, the government indicated its interest in requiring biometric sim card registration. In November 2019, authorities released a tender to create a database that can store up to 70 million records of biometric data received from mobile registration. **217** In June 2020, the government announced that it was continuing with the project and had requisitioned the Universal Service Fund, which was intended to support marginalized areas to access mobile telecoms, to pay for the biometric database. **218**

Although its provisions have not yet been implemented for web-only media outlets, the Printing and Publishing Law (2014) could potentially be used to prohibit anonymously run websites (see B6). **219**

There are no clear restrictions on encryption, although vague provisions in the Telecommunications Law and the Electronic Transactions Law could be interpreted to restrict the practice. Civil society activists are also concerned that the draft cybersecurity law could restrict encryption (see C2). **220**

### C5 0-6 pts

| **Does state surveillance of internet activities infringe on users' right to privacy?** | **2** / 6 |
|---|---|

Despite the fact that Article 357 of the constitution includes protection for private communications, government surveillance remains a serious concern. State surveillance of internet activities using sophisticated technology remains in its infancy in Myanmar because authorities continue to employ more invasive and direct

methods to infringe on users' privacy. The police frequently confiscate the mobile phones of those facing allegations of online criminal activity without a warrant, particularly human rights defenders, political activists, and journalists. **221** The police reportedly demand passwords for social media accounts and other applications from suspects, including in cases where allegations are unrelated to social media use. **222** For example, shortly after Reuters journalists Wa Lone and Kyaw Soe Oo were arrested (see C3), the police were accused of using Wa Lone's confiscated phone to send a WhatsApp message on his account. **223** The police used the Israeli phone-breaching product known as Cellebrite to collect data from the journalists' smartphones. **224** Cellebrite technology has been used by the police since 2016, and although the company ceased selling its products in Myanmar in late 2018, authorities continue to employ the technology. The revelations about Cellebrite also raised concerns about police accessing the journalists' social media accounts. In 2019, FinSpy malware from the German Gamma Group was reported to be in operation in Myanmar. **225** It is unclear who purchased the spyware.

In February 2018, Myanmar's parliament approved the creation of the Social Media Monitoring Team (SMMT), which was later established under the MoTC. **226** The government argued that the SMMT was necessary to counter those causing instability online, including through hate speech and defamation. **227** Public statements by senior government officials in May 2018 articulated that the SMMT's mandate focused narrowly on targeting foreigners and foreign organizations that cause unrest and threaten the country's sovereignty through interference. **228** Other analysts have suggested that, given Myanmar's broader political context, the SMMT was established to surveil foreign activists (including activists from Myanmar who operate outside the country or lack citizenship), foreign media outlets, and international organizations that focus on the Rohingya and other conflicts in Myanmar, as well as the International Criminal Court and other international bodies pushing for accountability for the atrocities against the Rohingya.

The SMMT was widely criticized by civil society organizations. **229** Despite the criticism, the SMMT was awarded an initial grant of approximately $4.8 million, **230** which it has reportedly used to purchase surveillance technology. **231** The scale and sophistication of the technology is unclear, **232** and the government has refused to

reveal from which country the equipment was purchased, citing security concerns. **233** As of May 2020, no information has been shared regarding the SMMT's powers and responsibilities, relationship with law enforcement and the courts, or any potential safeguards such as independent judicial oversight. Little is known about the body's operations or whether there is any oversight. **234**

The MoTC has announced its intention to build a data center that would serve as a secure base for its planned e-government services in Naypyidaw, and in December 2018 the ministry requested that the parliament approve a $95 million loan from South Korea to it. **235** **236** The Mandalay regional government launched its data center in January 2019 to provide e-government services. **237** Concerns have been raised that the data centers will lack adequate privacy and security safeguards. **238**

**C6** 0-6 pts

| **Are service providers and other technology companies required to aid the government in monitoring the communications of their users?** | **1** / 6 |
|---|---|

Service providers are increasingly concerned about protecting private data, given the ease with which the government can request it without proper oversight or appeals mechanisms. **239** International companies have also come under pressure; for example, a well-regarded NLD member of parliament has called for WhatsApp to monitor suspicious messages between users. **240**

The Law Protecting the Privacy and Security of Citizens, passed in 2017, prohibits the interception of personal communications without a warrant, but contains a vague exception allowing surveillance if permission is granted by the president or a government body. **241** The law does not outline clear procedures to prevent data from being collected and stored, nor does it provide for judicial review. Critics argue that the law's definition of privacy is inadequate and inconsistent with international human rights standards. **242** In early 2020, an amendment was proposed that would make certain offenses bailable under the law but it has not yet been adopted. **243** Other privacy-related laws demanded by a range of private sector and civil society stakeholders, including a robust data protection law, have not yet been proposed.

244

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." 245 The provision stating that any interception should not "hurt the fundamental rights of citizens" is an inadequate safeguard against abuse. 246 The Telecommunications Law also grants the government the power to inspect the premises of telecommunications license holders, as well as to require them to hand over documents, for the ambiguous purposes of defending the "security of the state or for the benefit of the people," without safeguards for individuals' privacy and other human rights. 247 A 2018 amendment to the Narcotic Drugs and Psychotropic Substances Law includes a new provision requiring telecommunications providers to disclose user information without due process. 248 There are no requirements for judicial review.

The largest state-owned telecommunications provider, Myanmar Posts and Telecommunications (MPT), has not publicized the number of requests for data they receive from authorities. Telenor announced that in 2019 it received 188 requests for communications data, about triple the number received in 2018, and complied with 88. 249 Mytel stated that it had received over 100 requests from the police for user data during 2019. 250 Both claimed that the majority of requests were related to human trafficking, missing people, and drugs. 251 The content of these requests are unclear. One major provider stated that it initially required three documents before disclosing information, including a letter from a senior police officer and a letter from the PTD, but has in practice dropped the requirement for a court warrant. 252

**C7** 0-5 pts

| | |
|---|---|
| **Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?** | **2**/5 |

*Score Change: The score improved from 1 to 2 due to fewer instances of physical violence reported in retribution for online activities.*

Online journalists, human rights defenders, and political activists continue to report

intimidation and threats of violence. In one opinion survey published in May 2020, most journalists reported that they believed violence against members of the media had increased compared to the previous year. **253** Violence and threats of violence were particularly common for journalists and activists reporting in conflict areas or communicating online about sensitive political issues such as the Rohingya crisis. **254**

Journalists reporting on the Rohingya crisis or covering the Rakhine State and Shan State conflicts feel particularly targeted. **255** During the trial of Reuters journalists Wa Lone and Kyaw Soe Oo, defense lawyers informed the court that the journalists were tortured in detention. **256** 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. **257** He also said that authorities covered his head with a black hood. In 2017, Kyaw Lin, a journalist in Rakhine State who contributes to the Democratic Voice of Burma (DVB) and is the editor-in-chief of the local outlet ROMA Time, was stabbed by two men on motorbikes. **258**

Human rights defenders also face intimidation and violence. The scale and volume of threats against human rights defenders, all of whom use the internet as their principal tool for advocacy, varies depending on the "sensitivity" of the issue they focus on in their work. Pro-Rohingya and peace activists report high levels of intimidation via direct and indirect messages and comments online. **259** Allegations of torture have also been made against police, prison guards, and border guards by student activists, **260** monks, **261** and others. **262** The government has itself perpetuated threats; in February 2019, a member of parliament threatened to take legal action against those who "damage the dignity" of the country by working with the United Nations. **263** In Myanmar, high-profile women and female human rights defenders report regular gender-based intimidation and threats of violence. **264** Common harassment tactics include cyberstalking, phishing, hacking, and attempts to cast doubt on women's credibility, integrity, and character. Many are intimidated through doctored sexual or intimate images, which are sometimes used in attempts to blackmail women.

A significant number of internet users have reported experiencing cyberbullying, particularly those in marginalized groups including young women, religious

minorities, and the LGBT+ community. **265**

**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 are periodically subjected to technical attacks in Myanmar. In 2017, websites for the Ministry of Culture, the Central Bank, and Maubin University, in addition to some private webpages, were hacked and populated with messages saying "Stop Killing Muslims." **266** The hacks were allegedly carried out by Turkish activists raising their concerns about the treatment of the Rohingya. **267**

Human rights defenders, journalists, and political activists continue to report regular, often weekly, remote attempts to hack their email and Facebook accounts. **268** Digital activists in Myanmar note that Google regularly warns them of "government-backed attackers" attempting to hack their Google products. **269** Pro-Rohingya and Muslim activists are among those who report frequent hacking attempts. **270** Police use sophisticated technology to hack into the devices of journalists, including Reuters reporters Wa Lone and Kyaw Soe Oo in 2017. **271** Advanced spyware has been identified in Myanmar, **272** and human rights defenders, journalists, and political activists report the use of spyware installed on their mobile phones (see C5). **273**

Microsoft has raised concerns about the large number of computers and devices in Myanmar that are infected by viruses and malware. **274** Kaspersky reported in 2019 that Myanmar comes in fourth globally for the highest rates of viruses at 60 percent of computers and removeable media. **275** Browser modifiers are twice as common in Myanmar than the global average, and software bundlers are almost three times more common. Microsoft has also raised concerns about the number of infections of the worm Win/Macoute that spreads to USB drives, which are very common in Myanmar, and communicate the drive's content to a remote host. **276**

## *Footnotes*

1 The number of internet users was reported in June 2019 at 18m by Internet World Stats, see "Internet Usage in Asia," Internet World Stats, [n.d.], https://www.internetworldstats.com/stats3.htm; A report on Myanmar in February 2020 by Hootsuite identified that this number had grown to 22m users by the beginning of 2020, see Simon Kemp, "Digital 2020: Myanmar," Datareportal, February 18, 2020, https://datareportal.com/reports/digital-2020-myanmar; 39 percent of the population and a growth of 1m persons over the course of the year.

2 James Barton, "Ooredoo Myanmar and MPT step up 4G offerings," Developing Telecoms, June 6, 2017, https://www.developingtelecoms.com/tech/wireless-networks/7110-ooredoo-....

3 Khine Kyaw, "Myanmar to accelerate 5G development despite risks," Eleven Media Group, December 19, 2018, https://elevenmyanmar.com/news/myanmar-to-accelerate-5g-development-des....

4 One index rates the percentage of the population using the internet as 33.1 percent in 2019 as compared to 51.8 percent for the Asia region, see "Internet Usage in Asia," Internet World Stats, [n.d.], https://www.internetworldstats.com/stats3.htm; Others rate Myanmar as 39 percent, South-East Asia as 63 percent, and Asia as 52 percent, see "The Global State of Digital in 2019 Report," Hootsuite, [n.d], accessed on October 2, 2019, https://hootsuite.com/pages/digital-in-2019.

5 Myanmar is 81st in the world for mobile speeds and 119th for fixed line speeds, see "Speedtest Global Index," Ookla® Speed Test, accessed March, 2020, https://www.speedtest.net/global-index/republic-of-the-union-of-myanmar.

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

**No**

Websites Blocked

**Yes**

Pro-government Commentators

**Yes**

Users Arrested

**Yes**

*In Other Reports*

Freedom in the World 2020

*Other Years*

2022

ADDRESS

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

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org