March 2023, UN HRC 52nd regular session
27 February -04 April 2023

Myanmar at the UN: Deterioration of human rights in the digital space | *Updates & recommendations as of March 2023*

INTRODUCTION

Since 2021, the Myanmar military has waged a coup both offline and online against the people of Myanmar.[1] As of March 2023, it has consolidated a **digital dictatorship** which buttresses the commission of serious human rights violations across all states and regions, many of which may amount to crimes under international law.[2]

Internet shutdowns facilitate and shroud military attacks on villages, killings, ill-treatment, arson, and other rights violations; while **surveillance technologies and regulatory controls** have been expanded to track and target individuals. The **telecommunications sector** in Myanmar is now completely controlled by the military, and intercept spyware has been activated across national networks. **Hate speech and incitement to violence** are rampant across online platforms and messaging services, and **doxxing** of individuals – particularly on Telegram – has enabled violent attacks on individuals and property by members of the military, military-linked and armed actors.

The United Nations High Commissioner for Human Rights' report in March 2023 on the situation of human rights in Myanmar highlighted the following violations relating to the digital sphere:[3]

- Freedom of expression, especially online, continues to decline: for example, the military included posting "likes" on social media among conduct demonstrating support to anti-military armed groups, and thus punishable by up to 10 years imprisonment.[4]
- Internet shutdowns continue to prevent safe communications and access to life-saving information in violence-affected areas.[5]

---

[1] See statements marking one and two years since February 2021: Access Now, Resist Myanmar's digital coup: International community must dismantle military dictatorship – or reap repercussions, 31 January 2023; Available at: https://www.accessnow.org/myanmars-digital-coup-statement/; Access Now, Resist Resist Myanmar's digital coup: stop the military consolidating digital control, 8 February 2022. Available at: https://www.accessnow.org/myanmars-digital-coup-statement/

[2] UN Special Procedures, Myanmar: UN experts condemn military's "digital dictatorship", Joint statement by Special Rapporteurs on the situation of human rights in Myanmar; the promotion and protection of freedom of opinion and expression; the right to privacy; and the rights to freedom of peaceful assembly and of association, 7 June 2022. Available at: https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship

[3] United Nations High Commissioner for Human Rights, Situation on human rights in Myanmar since 1 February 2022, A/HRC/52/21, 3 March 2023.

[4] Id., para. 54.

[5] Id., para. 55.

March 2023, UN HRC 52nd regular session
27 February -04 April 2023

The unfolding of simultaneous crises around the world has significantly eclipsed the deteriorating condition of human rights in Myanmar but the international community has a cornerstone role to play in holding the Myanmar military to account, and in confronting private businesses that are facilitating the military's commission of human rights violations across the country.

Developed in consultation with key stakeholders from Myanmar, we provide updates and recommendations on four main topics:
(1) internet shutdowns and connectivity;
(2) surveillance and spyware;
(3) hate speech and incitement to violence, including gender-based violence, online
(4) expansion of monitoring tools ahead of military-planned 'elections'

---

(1) INTERNET SHUTDOWNS AND CONNECTIVITY

On 23 June 2022, the now-former High Commissioner for Human Rights launched her highly anticipated **report on internet shutdowns** (A/HRC/50/55).[6] The High Commissioner remained clear in her messaging: "*States should refrain from imposing internet shutdowns and instead maximize internet access and remove barriers in order to facilitate online communication — an essential enabler of human rights in the digital age.*"[7]

In a previous session of the Human Rights Council, Access Now welcomed the resolution on the ***Situation of human rights of Rohingya Muslims and other minorities in Myanmar*** (**Myanmar Resolution**) (A/HRC/RES/50/3), which called on "*Myanmar to lift the shutdown of Internet and telecommunications services fully in all areas of Myanmar, including Rakhine State, and to repeal article 77 of the Telecommunications Act in order to avoid any further cutting of Internet and telecommunications access and the stifling of the rights to freedom of opinion and expression, including freedom to seek, receive and impart information, in accordance with international human rights law*". (OP12)

In March and June 2022, we delivered oral statements to the HRC highlighting shutdowns and targeted communication blackouts by the military junta.[8]
However, internet shutdowns continue to facilitate brutal human rights violations in Myanmar.

---

[6] Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, 13 May 2022. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/55/PDF/G2234155.pdf?OpenElement
[7] UNOHCR, Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights, 23 June 2022. Available at: https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human#:~:text=GENEVA%20(23%20June%202022)%20%2D,not%20to%20impose%20Internet%20shutdowns
[8] 23 March 2022: Access Now's statement on Myanmar at the U.N. Human Rights Council and 29 June 2022: Access Now's statement on Myanmar during the UN Special Rapporteur on the situation of human rights in Myanmar's Oral Progress Report.

On 28 February 2023, Access Now and the #KeepItOn coalition's new report, ***Weapons of control, shields of impunity: Internet shutdowns in 2022***, reveals these key findings:[9]

- **All 330 townships in Myanmar** experienced at least one shutdown in 2022
- **More than 50 townships** will have been **cut off from the internet for more than a year.**
- **The longest shutdown** has been ongoing for **more than 540 days** as of 28 February.
- The junta continues to strategically use shutdowns before and during attacks in areas where resistance is strongest – including in Sagaing, Magway, and Chin. Shutdowns shroud the military's "scorched earth" strategy of killings, torture, ill-treatment, and arrests, as well as widespread arson of property.
- People suffer from ongoing connectivity challenges due to significant price hikes for internet access[10] and expanded regulations for IMEI and SIM card registration.[11]
- Connectivity is now an exception rather than the norm across Myanmar.

RECOMMENDATIONS

1. Strengthen language in resolutions to (1) condemn internet shutdowns; (2) clearly acknowledge and condemn how the military is weaponizing internet shutdowns to facilitate human rights abuses, prevent documentation and cut off humanitarian aid or support and (3) expand connectivity to an open, secure, interoperable, and universally accessible internet;
2. Ensure resolutions do not solely focus on narrowly defined themes, particularly regarding human rights online, at the expense of failing to capture persistent and emerging issues both online and offline;
3. Leverage existing language on internet shutdowns as captured in UN Human Rights Council and General Assembly resolutions as well as regional mechanisms such as the African Union (see e.g. A/HRC/Res/49/21; A/HRC/Res/47/16; A/HRC/Res/47/23; ACHPR/Res.362(LIX)2016);
4. Strategically leverage findings and recommendations from the UN High Commissioner's shutdowns report for bilateral and multilateral engagement on internet shutdowns ordered by the Myanmar military;
5. Issue public thematic and country-specific statements that highlight instances of network disruptions and coordinate through embassies in countries where network disruptions are taking place to jointly urge States to refrain from and cease such measures (see for example the *2020 Joint Statement on Internet Shutdowns in Belarus,* the *2017 Freedom Online Coalition*

[9] 28 February 2023. Available at: https://www.accessnow.org/keepiton-2022-report
[10] Access Now, Resist Resist Myanmar's digital coup: stop the military consolidating digital control, 8 February 2022. Available at: https://www.accessnow.org/myanmars-digital-coup-statement/
[11] Access Now, Myanmar IMEI FAQ: how the junta could disconnect the resistance, 7 July 2022. Available at: https://www.accessnow.org/myanmar-imei/

Joint Statement on State Sponsored Network Disruptions, and the *G7 Foreign and Development Ministers' Meeting Communique*);

6. Since it is clear that human rights violations online enable and escalate offline violence, we recommend that more States prioritize and make explicit recommendations regarding the impact of internet shutdowns in engagement with international mechanisms, including through the UPR and treaty body processes; and
7. Meaningfully contribute to and adequately fund existing and new initiatives that collect information on mandated internet disruptions worldwide and/or provide for interventions, technological or otherwise, which allow affected people and communities to circumvent shutdowns and access the internet.

---

(2) SURVEILLANCE AND SPYWARE

The arbitrary or unlawful use of surveillance technologies violates human rights and causes real-world harm. The rampant abuse and culture of impunity surrounding surveillance technology also contravenes well-established international norms.

Access Now and our civil society partners have previously urged UN Member States to **denounce spyware abuses and mandate comprehensive measures to investigate and prevent further violations linked to the sale, export, and use** of such spyware and cases of targeted surveillance.[12] Since then, some States have made huge strides to combat the arbitrary or unlawful use of surveillance technologies. **Costa Rica** became the first State to publicly call for the *"immediate moratorium on the use of spyware technology until a regulatory framework that protects human rights is implemented."* [13]

In Myanmar, the military continues to build its surveillance infrastructure with the support of private businesses. After Telenor[14] and Ooredoo[15] sold their operations in the country, **all telecommunications companies in Myanmar are now either owned and/or controlled by the military.**

---

[12] Coalition Letter to the 48th U.N. Human Rights Council (HRC) on Pegasus, 30 September 2021. Available at: https://www.accessnow.org/letter-un-hrc-pegasus/

[13] Access Now, Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology, 13 April 2022. Available at: https://www.accessnow.org/costa-rica-first-country-moratorium-spyware/

[14] Access Now to Telenor's Board: Stop the sale in Myanmar, 13 October 2021. Available at: https://www.accessnow.org/telenor-board-stop-the-sale-myanmar/

[15] Access Now, Ooredoo's plans to leave Myanmar hands military full control of nation's telco sector-it must mitigate the human rights risks, 15 September 2022. Available at: https://www.accessnow.org/ooredoo-myanmar-sale/

Intercept surveillance has been activated across networks, a trend which will likely only worsen with military dominance of the telco sector. Recently, it was reported that Israeli company, Cognyte Software Ltd,[16] won a tender to sell intercept spyware to a state-backed telecommunications firm in Myanmar.

Furthermore, the military continues to install **closed circuit television (CCTV) systems with facial recognition technology** all over the country. These technologies are being sold by Zhejiang Dahua Technology,[17] Huawei Technologies Co Ltd,[18] and Hikvision[19] – businesses that have been sanctioned[20] for their products' use in Xinjiang, China, where surveillance[21] has allegedly facilitated crimes against humanity. The two local companies that have won local tenders to implement the Myanmar CCTV camera project, Fisca Security & Communication and Naung Yoe Technologies, have clear links to the Myanmar military. Fisca's Chairman is Soe Myint Tun,[22] a retired Deputy Commissioner of the Myanmar Police Force. Naung Yoe Technologies[23] regularly provides equipment for the military. Both Fisca Security & Communication and Naung Yoe Technologies were just recently added by the US Commerce Department to the Entity List[24] for providing surveillance technology to the military.

RECOMMENDATIONS

1. Strengthen language in resolutions to denounce abuse of surveillance and spyware technologies and mandate comprehensive measures to investigate and prevent further violations linked to the sale, export, and use of such technologies to the Myanmar military;
2. Leverage existing language on surveillance and spyware abuses as captured in UN Human Rights Council and General Assembly resolutions (see for example A/HRC/50/21; A/HRC/RES/45/18; A/76/173; A/HRC/RES/48/4; A/RES/75/176) to publicly denounce the Myanmar military's abuse of surveillance technologies;

---

[16] Reuters, Israel's Cognyte won Myanmar spyware tender before coup, 15 January 2023. Available at: https://www.aljazeera.com/news/2023/1/15/israels-cognyte-won-myanmar-spyware-tender-before-coup
[17] Zack Whittaker for TechCrunch, US government agencies bought Chinese surveillance tech despite federal ban, 02 December 2021. Available at: https://techcrunch.com/2021/12/01/federal-lorex-surveillance-ban/
[18] Rita Liao for TechCrunch, Tech stocks slide on US decision to blacklist Huawei and 70 affiliates, 16 May 2019. Available at: https://techcrunch.com/2019/05/15/us-blacklist-huawei-70-affiliates/
[19] Zack Wittaker for TechCrunch, "Always on and watching"" A former Xinjiang prisoner describes life inside China's detention camps, 14 April 2022. Available at: https://techcrunch.com/2022/04/13/xinjiang-prisoner-hikvision-china/?guccounter=1&guce_referrer=aHR0cHM6Ly90LmNvLw&guce_referrer_sig=AQAAAJeEy--IM8OcFmLLuuFaqacpGEk-epjzPl9hu7oQwvSNPVh2uN2fhOekqlcTuVqCgWlFokFphAaYGVR57LoYFFo3abF2qn3FrSPvpg7tXluurOAcCDLt9S4zjaLMEKjkmCboXZaadwnv-ZAZXFVs-yrdl8WqitDMDdub9tUHPL8B
[20] Access Now, Track and target: FAQ on Myanmar CCTV cameras and facial recognition, 03 August 2022. Available at: https://www.accessnow.org/myanmar-cctv-cameras/
[21] OHCHR, Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China, 31 August 2022. Available at: https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf
[22] Information last updated on 12 July 2017. Available at: https://opencorporates.com/officers/237160404
[23] Army Recognition, Myanmar Air Defense Vehicles and more appear on social medias, 30 March 2021. Available at: https://www.armyrecognition.com/defense_news_march_2021_global_security_army_industry/myanmar_air_defense_vehicles_and_more_appear_on_social_medias.html
[24] U.S. Department of Commerce, Commerce Implements New Export Controls on Burma and Makes Entity List Additions in Response to the Military Coup and Escalating Violence against Peaceful Protesters, 04 March 2021. Available at: https://www.commerce.gov/news/press-releases/2021/03/commerce-implements-new-export-controls-burma-and-makes-entity-list

3. Join existing State-led initiatives, including the multilateral *Export Controls and Human Rights Initiative*[25] to take spyware threats seriously;
4. Join efforts led by States, such as Costa Rica,[26] to place an immediate moratorium on the use, sale, servicing, and transfer of surveillance technologies produced by private firms until adequate human rights safeguards and regulation are in place.
    a. To support this transition, Access Now and other civil society organizations have developed *13 Principles*[27] to guide law enforcement and policymakers in ensuring respect for human rights in surveillance activities.

---

(3) HATE SPEECH AND INCITEMENT TO VIOLENCE (INC. GENDER-BASED VIOLENCE) ONLINE

Since the coup, military-linked and armed actors have increasingly **abused social media platforms and messaging services to dox people, incite violent attacks against and ill-treatment and killings of individuals – and threaten family, friends** and others in their networks. This has included targeted 'watermelon-suppression' campaigns against junta defectors.[28] Doxxing[29] is the act of publicly sharing someone's personal information online like their phone number, address or private, intimate photos, without their consent and with malicious intent.

In his 13 June 2022 report (A/HRC/49/76), the UN Special Rapporteur on the situation of human rights in Myanmar, reported that *"for decades, the Myanmar military has used sexual violence and other crimes against women as a weapon of war."* Online gender-based violence (GBV) is manifested through debilitating and aggressive acts of doxxing – targeting especially women who actively participate in resistance initiatives against the junta.

A recent CNN report[30] on the prevalence of doxxing on Telegram in Myanmar's context, to which Access Now provided input noted: *"When men are targeted, posts typically insinuate that they are linked to*

---

[25] The White House, Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy, 10 December 2021. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/
[26] Access Now, Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology, 13 April 2022. Available at: https://www.accessnow.org/costa-rica-first-country-moratorium-spyware/
[27] Access Now, Article 19, and others, Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance. Available at: https://necessaryandproportionate.org/principles/
[28] Andrew Nachemson, 'Watermelon suppression': doxing campaign targets pro-democracy soldiers and police, Frontier Myanmar,14 March 2022. Available at: https://www.frontiermyanmar.net/en/watermelon-suppression-doxing-campaign-targets-pro-democracy-soldiers-and-police/
[29] Access Now, How online doxxing is endangering women judges in Tunisia, 24 June 2022. Available at: https://www.accessnow.org/how-online-doxxing-is-endangering-women-judges-in-tunisia/
[30] Pallabi Munsi for CNN, They released a sex video to shame and silence her. She's one of the many women in Myanmar doxxed and abused on Telegram by supporters of the military, 02 February 2022. Available at: https://edition.cnn.com/2023/02/07/asia/myanmar-military-sexual-images-doxxing-telegram-as-equals-intl-cmd/index.html

terrorist groups working to bring down the junta… When women are doxxed, the attacks frequently feature sexist hate speech, often coupled with explicit sexual imagery and video footage of them."

Doxxing by sharing intimate and/or sexual images violates one's privacy and is intended to shame women from further participating in protests and other resistance actions. Releasing personal information endangers the lives not only of victims but their family members and friends, who become targets for violence and harassment in violation of their rights to security, freedom from ill-treatment and life.

RECOMMENDATIONS

1. Strengthen language in resolutions to denounce all forms of gender-based violence in Myanmar, including online elements of such violence, such as doxxing, especially when this is used as a weapon against dissent;
2. Strengthen language in resolutions to denounce the proliferation of hate speech and incitement to violence online and abuse of doxxing by all actors – including members of the military, military-linked and others – in Myanmar, resulting in serious violations of, including but not limited to, the rights to life, security, freedom from ill-treatment, expression, and association;
3. Strengthen language in resolutions to ensure technology companies and platforms comply with their responsibility to respect human rights, including to address adverse human rights impacts of the abuse of their platforms and services to propagate hate and violence offline.

---

(4) EXPANSION OF MONITORING TOOLS AHEAD OF MILITARY-PLANNED 'ELECTIONS'

As the Myanmar military plans for an 'election'[31] in 2023, it is systematically expanding[32] all tools – regulatory and non-regulatory – to **track and monitor all digital information** relating to people in Myanmar. These measures are ostensibly aimed **to railroad subservient voting** at the 'elections'.

The military is bolstering a national database to track and monitor individuals' location and networks. It has forced **SIM re-registration** by January 2023, deactivating all cards not registered with a Myanmar National Registration Card (NRC) – an earlier re-registration drive saw the military deactivate

[31] Emma Farge for Reuters, U.N. rights envoy warns that Myanmar's election will be a 'fraud', 22 September 2022. Available at: https://www.reuters.com/world/asia-pacific/un-rights-envoy-warns-that-myanmars-election-will-be-fraud-2022-09-22/
[32] Dhevy Sivaprakasam on Context News, Myanmar election will seal military's digital domination, 12 December 2022. Available at: https://www.context.news/surveillance/opinion/myanmar-election-will-seal-militarys-digital-domination

more than 34 millions SIMs[33] for "improper" registration. SIM re-registration drives are crucial to link mobile devices to NRCs – which provide information on people's names and addresses and are connected to other information, such as familial relationships, property, and bank accounts. This is supplemented[34] by newer regulatory measures, including **mandatory registration[35] of all International Mobile Equipment Identity (IMEI) numbers** for mobile devices which will link physical phones – which hold information on a person's location and communications – with SIMs and NRC records. Ongoing expansion of surveillance across the country will reinforce tracking of people's communications, networks, and locations.

Meanwhile, the military is also **deliberately cutting off access to the internet** for millions of people, to undermine communications, hinder documentation of violations, and block support, including through online financial transactions, for groups actively opposing the regime. **Prices of mobile data have been significantly hiked**,[36] and a **draft Cybersecurity law**[37] plans to introduce unprecedented requirements on internet service providers and operators which will undermine the rights to privacy, security, freedom of expression and association of their customers in Myanmar.

Access Now (https://www.accessnow.org) defends and extends the digital rights of people and communities at risk around the world. *For more information, please contact:*

Wai Phyo Myint | Asia Pacific Policy Analyst| waiphyo@accessnow.org
Golda Benjamin | Asia Pacific Campaigner | golda@accessnow.org
Dhevy Sivaprakasam | Asia Pacific Senior Policy Counsel | dhevy@accessnow.org

[33] Myanmar Now, Telecoms Ministry says it has deactivated more than 34 million SIM cards. Available at: https://myanmar-now.org/en/news/kia-launches-investigation-into-killing-of-civilians-accused-of-belonging-to-rival-ethnic-army
[34] Access Now, Track and target: FAQ on Myanmar CCTV cameras and facial recognition, 03 August 2022. Available at: https://www.accessnow.org/myanmar-cctv-cameras/
[35] Myanmar Business Today, IMEI number of mobile phones required to be registered, 21 May 2022. Available at: https://mmbiztoday.com/imei-number-of-mobile-phones-required-to-be-registered/
[36] Andrew Haffner for Al Jazeera, Myanmar's internet gets pricier for dissenters, apolitical hike, 11 February 2022. Available at: https://www.aljazeera.com/economy/2022/2/11/myanmars-internet-gets-pricier-for-dissenters-apolitical-alike
[37] Access Now, Analysis: the Myanmar junta's Cybersecurity Law would be a disaster for human rights, 27 January 2022. Available at: https://www.accessnow.org/analysis-myanmar-cybersecurity-law/