

PERSPECTIVE

Five Years After Coup, Myanmar's Digital Authoritarianism Enters New Phase

WAI PHYO MINT, DARIKA BAMRUNGCHOK / MAR 13, 2026

Shutterstock

Five years after the coup, Myanmar's junta continues to systematically oppress its own people, carrying out mass arbitrary arrests and killings, imposing internet shutdowns, expanding mass surveillance, enforcing forced conscription, and imposing severe restrictions on both online and offline civic space. Despite these numerous human rights violations, the junta is now seeking legitimacy through military-controlled elections.

By actively adopting and adapting a model of authoritarian rule that weaponizes digital technology and communications infrastructure against its own population, the junta is fueling the normalization of digital authoritarianism, a model that is increasingly replicated across the region and beyond. This is no longer merely a domestic crisis. It has become part of a growing system of transnational oppression and a testbed for the digital authoritarianism ecosystem.

Possibly the worst form of digital authoritarianism

Since February 2021, the Myanmar military has turned the digital space into a battlefield through various oppressive measures such as arbitrary internet shutdowns, seizure of communication infrastructure, conducting mass surveillance, online censorship, data extraction, drone deployment, signal jamming, and the criminalization of digital expression. Those measures are no longer temporary or ad hoc. The use

of advanced digital technologies has become central to an integrated system of the military's authoritarian control designed to govern through fear and technological dominance. The controversial [Cybersecurity Law](#), enacted on January 1, 2025, further entrenches a broad and systematic surveillance regime.

The military has systematically disrupted the country's communications infrastructure, becoming [one of the world's worst offenders](#) of internet shutdowns for the last five years. More than [130 of 330 townships](#) have been placed under prolonged internet blackouts, while [VPNs](#) and [social media platforms](#) have been banned. At the same time, [advanced firewall systems](#) have been installed at national internet gateways to filter, monitor, and restrict online content.

Data from national databases, e-ID systems, sim registration data, financial and banking records, and census programs have been consolidated into a centralized identity system that is systematically used for [surveillance](#), [arrests](#), and [forced conscription](#). Blending traditional tactics, such as legal instruments, human intelligence, and state databases, with a new tool, the so-called "[Person Scrutinization and Monitoring System](#)" (PSMS) functions as a digital screening and tracking system. By integrating with the automated, facial recognition-powered PSMS, it entrenches authoritarian control over both physical and digital spaces.

Although the full impact of the PSMS, linked to national databases, warrant lists, and biometric data, is difficult to unpack and measure, the military has reportedly used it at [roadside checkpoints](#), checking IDs or scanning individuals' irises and arresting those flagged for alleged anti-junta activities. The repressive practices came to support technologies that have already resulted in mass arrests and violations, leaving people living in constant fear.

According to the [latest report](#) from the Assistance Association for Political Prisoners, over the past five years, the military has killed at least 7,761 people, including 1,005 children, and arrested more than 30,426 people, including 631 children, for political reasons. The majority remain in prison today. Among them, hundreds of individuals were arrested solely for their online expression, including changing their profile pictures to black, liking anti-junta posts, commenting in support of resistance activities, or making financial contributions. Data for Myanmar further [reports](#) that as of November 2025, the junta had burned at least 113,054 homes since the coup.

Foreign support and the militarization of technology

These tools and practices form the backbone of digital authoritarianism. Much of this technological infrastructure is not domestically developed but has been used to escalate military repression. Support from foreign governments, particularly [China](#) and [Russia](#), has played a decisive role in enabling this new phase of authoritarian control.

Surveillance infrastructure, cybersecurity systems, support for military owned and/or controlled telecommunications networks, data centers, and data governance models imported from countries such as [China](#), [Russia](#), and [India](#) have provided the military with both the tools, such as the growing use of [foreign advanced drones](#) with night vision cameras and [infrastructure for extensive digital identity systems](#), as well as the blueprint for digital control.

In September 2025, [Justice For Myanmar](#) published an investigative report revealing that the Chinese company Geedge Networks supplied the Myanmar military with a commercial version of China's "Great Firewall," including deep packet inspection (DPI) technology. According to the report, this system enables real-time surveillance and geolocation of Myanmar's 33.4 million internet users, with operational support from 13 domestic telecommunications providers.

OUR CONTENT DELIVERED TO YOUR INBOX.

Join our newsletter on issues and ideas at the
intersection of tech & democracy

[Subscribe](#)

The import of such digital authoritarian technology enabled by legal loopholes in both national and international regulations has strengthened the military regime and deepened its technological sophistication amid shifting geopolitical dynamics. The transfer was reportedly carried out through complex international supply chains.

The regime has shifted from relying only on traditional intelligence networks to adopting imported digital systems and infrastructure. Myanmar stands as a cautionary example and testing ground for how digital authoritarianism can be strengthened through the transfer of technical capacity through authoritarian alliances and the apathy of the international community.

Sham elections are not a democratic reset

The military recently held a month-long national election, conducted in three phases from 28 December 2025 to 25 January 2026, widely regarded as a sham election. Before, during, and after the process, the regime systematically violated digital and civil freedoms, making free and fair elections impossible. Airstrikes continued in townships even as voting was underway. The United Nations reported that at least 170 people were killed with 408 military aerial attacks recorded between December 2025 and the final round of voting.

Despite international condemnation and boycott calls, reported turnout exceeded 50 percent, likely driven in part by fear of repercussions for nonparticipation. In December, 2025, under a new law criminalizing actions deemed to undermine the election, the military announced the arrest of more than 200 people for alleged “sabotage” of the election process, many for social media posts opposing the vote.

Sham elections do not represent a democratic reset or meaningful transformation. Portraying it as a pathway to stability is dangerously misleading. Endorsing or engaging with it risks securing long-term legitimacy for the military, including its use of technology to silence dissent, manipulate information, and force people to give votes. Myanmar's revolution has not ended. Democracy cannot be restored while surveillance replaces accountability, fear suppresses free expression, and technology is used to threaten civilians rather than enable civil participation and empower people.

As the military seeks international legitimacy through this electoral process, greater global scrutiny is urgently needed. The past five years since the coup have shown enough the consequences and deepening humanitarian crisis. This is a critical moment for international attention, not indifference.

A call for regional and global action

As Myanmar's resistance enters its sixth year, the crisis carries both regional and global implications. The country has become a testing ground for digital authoritarianism globally. The military's reliance on imported sophisticated technologies illustrates how authoritarian regimes learn from one another, reinforce repressive practices, and build interconnected systems of control.

At the regional level, this is a critical mission for ASEAN in implementing a Myanmar-led solution to the crisis. The Five-Point Consensus, adopted in April 2021 in response to the Myanmar military, has failed. Although ASEAN has not recognized the military's elections, the regional bloc with 11 member states remains divided. Meanwhile, big companies across the ASEAN region and beyond continue to do business with the military, providing a significant source of funds, equipment, and technology.

The Special Rapporteur on the situation of human rights in Myanmar called on states to focus on cutting the flow of weapons, aviation fuel, and funds that enable the military's campaign of violence and repression.

If the Myanmar military's digital authoritarianism is allowed to persist unchecked and gain international recognition, it will send a dangerous signal: that governments can dismantle fundamental rights and still be treated as legitimate actors.

The international community should respond with principled and coordinated action. This means resisting the normalization of technology-enabled repression in Myanmar and refusing to legitimize the results of sham elections or fraudulent political processes. Governments and private companies that enable these systems — through financing, technological support, political endorsement, or silence — should be held accountable. International partners should also strengthen coordinated mechanisms to resist the military's expanding digital repression and invest in technologies that help people in Myanmar circumvent censorship, counter internet shutdowns, and sustain independent information ecosystems.

Resisting digital authoritarianism in Myanmar is not only a strategic necessity — it is a moral obligation. The future of digital freedom, democratic governance, and human rights in the region and beyond depends on it.

AUTHORS



WAI PHYTO MINT

Wai Phyto Mint is an Asia-Pacific Policy Analyst at Access Now. Wai Phyto has been working as a digital rights advocate in Myanmar for over eight years, and has previous experience in political advisory, media, and communications. Wai Phyto has served as one of the leading persons in Myanmar organizin...



DARIKA BAMRUNGCHOK

Darika Bamrungchok is the Asia Pacific Policy Analyst at Access Now. She has been working as a digital rights advocate and digital security trainer in Thailand and the broader Southeast Asia region for over a decade.

RELATED

Fourth Year Under Myanmar Military’s Digital Iron Curtain: A Reflection on Digital Repression and the Path Forward

MARCH 4, 2025

Myanmar Cannot Wait: Only Coordinated Global Pushback Will Stop Escalating Violence and Repression

AUGUST 17, 2023

PERSPECTIVE

The Tech Arms Race is Reshaping Our Lives — and Threatening Democracy

OCTOBER 22, 2025

Venezuela: Digital ID As a Tool of Oppression

SEPTEMBER 10, 2024

PERSPECTIVE

When Device Security Becomes State Control

FEBRUARY 16, 2026

TOPICS

Cybersecurity

Human Rights

A nonprofit media and community venture intended to provoke new ideas, debate and discussion at the intersection of technology and democracy.



About

Donate

Privacy Policy

Articles

Podcast

Contributors

Fellowships

Contributor Guidelines