

Gender equality, the digital space and AI in Myanmar

Submission to the UN Working Group on Discrimination Against Women and Girls - October 2025

Introduction

Since the 2021 coup, the military has systematically weaponised digital technology and Artificial Intelligence (AI) as core components of its strategy to silence dissent and consolidate power. This "digital coup" has resulted in a significant collapse of civil and political rights, with women and girls facing unique and disproportionately severe harms. The digital sphere in Myanmar is not a neutral space but a battlefield where fundamental rights are under constant and deliberate assault. This submission to the UN Working Group on Discrimination Against Women and Girls shows that the military's digital repression is inherently gendered, exploiting and amplifying pre-existing patriarchal norms to create a climate of fear designed to silence women and erase them from public life.

Women's rights in an era of new and emerging technology

Digital technology and AI presents many opportunities but is also being used to undermine the rights of women and girls in Myanmar. The military has constructed a comprehensive architecture of digital control that has systematically dismantled the rights to privacy, freedom of expression, association, and assembly. This system is a "digital dictatorship" designed to prevent people from learning about, objecting to, and organizing against the military's abuses, with severe and gendered consequences.²

Freedom of expression, assembly, and association

The military has transformed the digital sphere into a space of control, impacting on freedoms of expression, assembly, and association. The military repeatedly imposes internet shutdowns to coincide with protests and military operations, crippling the ability of people, particularly women activists, to organise, communicate, and document atrocities. Myanmar leads the world with hundreds of internet shutdowns. The military has also blocked major social media platforms (Facebook, X, Instagram) and news sites, forcing people to try to use blocked VPNs to access information. This

https://freeexpressionmyanmar.org/surviving-myanmars-digital-coup/

² https://freeexpressionmyanmar.org/surviving-myanmars-digital-coup/

³ https://www.ohchr.org/en/stories/2022/08/activists-internet-shutdowns-violate-human-rights

 $^{^{4}\,\}underline{https://humanrightsmyanmar.org/myanmar-freedom-on-the-net-2024/}$



creates an information vacuum filled by state propaganda. The military ordered mobile data prices to be doubled, making internet access prohibitively expensive.⁵ This disproportionately affects women, who already face a significant digital divide due to lower income and digital literacy, further limiting their ability to exercise their rights online. The military amended Article 505(a) and added Article 505A to the Penal Code to criminalise any speech that could "cause fear" or spread "false news," and has used it to prosecute hundreds of journalists and activists for online expression.⁶

Privacy

The military has undercut the right to privacy and rule of law to enable the collapse of all other civil and political rights. The 2025 Cybersecurity Law grants the military sweeping, unchecked powers to monitor online activity, force service providers to hand over user data without judicial oversight, and criminalise dissent under vague terms like "disinformation". Shortly after the coup, the military suspended key sections of the 2017 Law Protecting the Privacy and Security of Citizens, removing fundamental protections against warrantless surveillance and seizure. The expanding network of AI-powered CCTV cameras from Chinese companies like Huawei, Dahua, and Hikvision in major cities creates a pervasive public surveillance infrastructure. This allows the State to monitor people's movements and relationships on an unprecedented scale, turning public spaces into open-air prisons where every action is potentially recorded and analysed. This has a profound chilling effect on women's willingness to participate in public life and peaceful assembly.

Transnational effects

The military's digital repression is enabled and exacerbated by transnational factors. The military is actively procuring advanced AI-powered surveillance systems from international suppliers. It is rolling out Chinese-built surveillance cameras equipped with AI-driven facial recognition from companies such as Huawei, Dahua, and Hikvision in multiple cities. This technology is used for political repression, enabling the military to track and target activists, and its importation directly facilitates gross human rights violations. The 2025 Cybersecurity Law also has extraterritorial reach, explicitly targeting activists and citizens residing abroad.

International social media platforms have often failed to adequately address the coordinated, politically motivated abuse targeting women in Myanmar.¹² Pro-military channels often seem to operate with impunity, disseminating doxed information and inciting repression.¹³ This inaction, encouraged by a lack of investment in local language moderation and a failure to act, is fundamentally driven by platform algorithms designed to encourage engagement.

⁵ https://humanrightsmyanmar.org/myanmar-freedom-on-the-net-2024/

 $^{^{6}\,\}underline{\text{https://freeexpressionmyanmar.org/wp-content/uploads/2022/01/505a-act-of-revenge-1.pdf}$

⁷ https://humanrightsmyanmar.org/myanmars-cyber-law-a-serious-threat-to-privacy-speech-and-security/

⁸ https://humanrightsmyanmar.org/privacy-violations-and-discrimination-in-myanmar/

⁹ https://humanrightsmyanmar.org/myanmars-repressive-use-of-ai-to-counter-terrorism/

 $^{{\}color{blue} {\rm https://humanrightsmyanmar.org/myanmars-repressive-use-of-ai-to-counter-terrorism/repressive-use-of-$

 $^{^{11}\ \}underline{\text{https://humanrightsmyanmar.org/myanmars-cyber-law-a-serious-threat-to-privacy-speech-and-security/}$

 $^{^{12}\} https://humanrightsmyanmar.org/meta-facebook-changes-threaten-myanmars-digital-space/$

 $^{^{13}\ \}underline{\text{https://www.info-res.org/cir/reports/digital-battlegrounds-politically-motivated-abuse-of-myanmar-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-online/of-women-o$



Women's leadership in political, economic, social and cultural rights

AI has been weaponised by the military to specifically target, silence, and exclude women from political and public life, violating their fundamental rights to political participation and freedom of expression. The military employs a dual strategy. First, the deployment of AI-equipped cameras with facial recognition in cities like Naypyidaw, Mandalay, and Yangon has a profound chilling effect on women's activism. This technology removes the anonymity crucial for safe assembly. For women, who are already at heightened risk of State violence and sexual assault in detention, this makes appearing at a protest an extreme personal risk, effectively pre-empting their right to assemble. Second, the military enables and encourages technology-facilitated gender-based violence (TFGBV) to destroy women's reputations and drive them from public discourse. This is a deliberate military strategy designed to enforce patriarchal control and crush female-led resistance.

Targeting of women

Online spaces are a primary front for politically motivated attacks against women in Myanmar. These are not random acts but systematic, coordinated campaigns explicitly aimed at silencing women who express political opinions. Analysis of 1.6 million social media posts found that politically motivated online abuse of women was at least five times more prevalent at the end of 2022 compared to immediately after the 2021 coup, and up to 500 times higher than international baselines. The overwhelming majority of abuse is perpetrated by pro-military, male-presenting accounts. Just four pro-military social media channels were responsible for 50% of the detected abusive posts.

The military's primary tactic is doxxing, which is the malicious release of a woman's private information (address, phone number, photos). Women are targeted for doxxing at a higher rate than men. These posts frequently include explicit calls for the military to arrest the woman, and these online calls are often followed by actual arrests, demonstrating a direct link between online mobs and state security forces.

Military campaigns are often characterised by vile, sexualised disinformation depicting politically active women as "morally corrupt" and "promiscuous". These narratives are often amplified by official military media. Women journalists, politicians, and human rights defenders are subjected to a torrent of violent threats, including rape and death threats, intended to terrorise them into silence. Women media professionals face intense and intersecting forms of gender-based violence, forcing many into exile.

Governance of AI and content moderation of AI-generated content

There is a complete and deliberate vacuum of accountability in Myanmar. The absence of redress is not a failure of the system, but a core feature of it. In post-coup Myanmar, the legal framework is designed not for governance but for impunity. The military has erected a legal architecture to codify

 $^{^{14}\,\}underline{\text{https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights}$

 $^{^{16}\} https://free expression myan mar. org/wp-content/uploads/2018/12/daring-to-defy-myan mars-patriarchy.pdf$

 $^{^{17} \, \}underline{\text{https://freeexpressionmyanmar.org/wp-content/uploads/2023/04/surviving-myanmars-digital-coup.pdf} \\$



digital authoritarianism and retroactively justify any action it takes against its opponents. There are no laws or policies that provide for the safe or ethical governance of AI. Instead, the legal framework is designed to facilitate its use as a weapon of repression.

There are no measures in place in Myanmar to encourage or ensure that training data for AI systems reflect Myanmar's diverse populations. The AI systems being deployed, particularly facial recognition technology, are sourced from foreign companies and implemented without transparency or public consultation . It is widely recognised that these systems often have higher error rates when identifying women and individuals from ethnic minorities, which in a diverse country like Myanmar, significantly increases the risk of misidentification and false arrest for women from minority communities. ¹⁸

Private sector

International social media companies have systematic failures primarily driven by global business models and structurally incompatible with protecting women's rights in a high-risk conflict environment like Myanmar. Some platforms are grossly inadequate in moderating seriously harmful content, and may even profit from it. Prolific pro-military channels dedicated to doxxing and harassing women remain active, even when there are clear policy violations. Takedowns are slow and inconsistent. Platforms have often failed to invest in local context and language expertise. Automated systems are easily circumvented, and human reviewers lack the context to identify policy-violating content, leading to false positives and effective censorship. Restrictive data access policies prevent independent researchers from assessing the full scale of abuse, shielding platforms from scrutiny.²¹

Technology-facilitated gender-based violence

We understand technology-facilitated gender-based violence (TFGBV) as any act of violence perpetrated by one or more individuals that is committed, assisted, or amplified by the use of digital technology against a person on the basis of their gender. In the context of Myanmar, TFGBV is not confined to interpersonal violence but is a political and military weapon. It is systematically deployed by military, military proxy, and pro-military actors to silence women, discredit their political participation, and enforce patriarchal control by exploiting and amplifying pre-existing gender inequalities and discrimination. It includes doxxing, death and rape threats, and the dissemination of sexualized disinformation.

In Myanmar, there are no protective policies, practices, or protocols aimed at ensuring women's and girls' safe participation online. On the contrary, the military and its proxies are the primary perpetrators and enablers of TFGBV. The legal framework, such as the Cybersecurity Law (2025), is designed to facilitate surveillance and punish dissent, not to protect users. The online space is actively made unsafe for women by the military as a matter of strategy. The only efforts to combat TFGBV come from civil society organisations and women human rights defenders themselves, who operate at extreme personal risk.

¹⁸ https://sdgs.un.org/sites/default/files/2024-

 $[\]underline{05/Francis_Navigating\%20 the\%20 Intersection\%20 of\%20 AI\%2C\%20 Surveillance\%2C\%20 and\%20 Privacy.pdf}$

 $[\]frac{19}{\text{https://freeexpressionmyanmar.org/wp-content/uploads/2018/12/daring-to-defy-myanmars-patriarchy.pdf}}$



The deployment of AI in Myanmar's conflict context is central to the military's strategy of repression. AI-powered surveillance systems are used to track and target opponents of the regime. The Person Scrutinization and Monitoring System (PSMS) has been used to cross-check hotel guest lists, leading to the arrest of members of the Civil Disobedience Movement, including women nurses and teachers. These systems can be used for predictive threat analysis, algorithmically flagging individuals as potential threats based on their digital footprint, movements, or associations. Women in conflict zones, particularly those from ethnic minorities, are at extreme risk of being algorithmically profiled as supporters of resistance forces, which could lead to their arbitrary arrest, torture, or extrajudicial killing.

Privacy, Autonomy, and Non-Discrimination

In Myanmar, AI technologies are the central pillar in the military's systematic annihilation of the right to privacy. The destruction of privacy is a strategic prerequisite for violating all other civil and political rights. By demolishing this foundational right, the military has caused the entire structure of civil and political rights to collapse. The impact is not gender-neutral; pervasive state surveillance exacerbates the vulnerability of women, infringing on their autonomy and creating a constant state of fear and self-censorship that pushes them out of civic space.⁴

The AI-powered surveillance systems deployed by the military are suspected to be used to gather and analyse sensitive categories of personal data. This includes biometric data such as facial images collected by the nationwide CCTV network; location data that tracks the movements of individuals and vehicles; and political opinions and associations by tracking attendance at protests or analysing online posts, mapping individuals' associations by monitoring who they meet with. This data is then used to target individuals for their perceived political beliefs, constituting a direct violation of the rights to privacy and non-discrimination.

The impact of this surveillance is not gender-neutral. Women in Myanmar, particularly activists, are already subject to intense social scrutiny. Pervasive state surveillance exacerbates this vulnerability, creating a constant state of fear that severely limits their ability to communicate freely, build trust, and participate in public life.

Recommendations

- 1. **Publicly condemn Myanmar's digital coup:** The UN and its member states should publicly condemn the military's use of digital technology and AI as tools of repression, specifically highlighting the gendered impacts.
- 2. **Impose targeted sanctions on technology suppliers:** Member states should impose targeted sanctions on international companies (e.g., Huawei, Dahua, Hikvision) that supply the military with surveillance technology used to commit human rights violations.
- 3. **Hold social media platforms accountable:** The UN should demand immediate and concrete action from social media companies to address the rampant, politically motivated, and



- gendered abuse on their platforms. This must include significant investment in Myanmar-language content moderation and meaningful engagement with local civil society.
- 4. **Support digital security for civil society:** Member states and donors should significantly increase funding and technical support for digital security initiatives for Myanmar's civil society, focusing on women human rights defenders, journalists, and activists.
- 5. **Ensure accountability for digital crimes:** The Independent Investigative Mechanism for Myanmar (IIMM) and other international justice bodies should be resourced to specifically collect and preserve evidence of digital crimes, including state-led surveillance and coordinated online incitement to violence.