Protecting Myanmar's HRDs in the digital age

Submission to the UN Office of the High Commissioner for Human Rights – March 2026

Introduction

Since the February 2021 coup, the Myanmar military has systematically constructed a digital dictatorship, a sophisticated ecosystem where emerging technologies are weaponised to dismantle civic space, enforce total information control, and target HRDs with lethal precision. Myanmar currently serves as a global cautionary tale for digital authoritarianism. The country ranks as one of the world's most repressive digital environments. For HRDs in Myanmar, the digital sphere is no longer primarily a tool for liberation but increasingly a theatre of persecution, where a single digital footprint can lead to extrajudicial killing, torture, or life imprisonment.

Legislative and regulatory measures

The military has replaced the rule of law with rule by lawfare, utilising a fragmented, overlapping, and draconian legal framework designed to criminalise every facet of an HRD's digital life.

- **Penal Code Article 505A and the criminalisation of dissent:** Amended immediately after the coup, Article 505A quickly became the military's primary tool for revenge against its critics. By criminalising so-called "false news" and speech that "causes fear" or "disturbs government employees," the military has created an environment where sharing a human rights report or even "liking" a pro-democracy post is a punishable offense. Hundreds of journalists and HRDs have been detained under this provision, often based solely on screenshots of their social media activity.
- **The Counter-Terrorism Law and State terror:** The military has weaponised the Counter-Terrorism Law to designate the legitimate political opposition and HRDs as "terrorists." This designation triggers extreme digital surveillance powers and allows for the prosecution of anyone providing material support, which the military interprets to include digital advocacy, fundraising via mobile money, or even the digital documentation of military abuses. This framework allows the military to exercise State terror while shielding its own atrocities from international scrutiny.
- **Cybersecurity Law (2025) and data sovereignty:** This law represents the final brick in the digital wall. It mandates that all digital platforms operating in Myanmar, including ISPs and social media companies, must retain comprehensive user data (names, IP addresses, browsing logs, and physical locations) for a minimum of three years. Crucially, it empowers the military to demand this data without judicial oversight, effectively making every tech company an involuntary arm of the military intelligence apparatus.

- **Electronic Transactions Law (Amended 2021):** The military's amendments to this law stripped away previous privacy protections, granting authorities sweeping powers to intercept personal data and access accounts without warrants. By criminalising the misuse of information technology, the military provides a thin legal veneer for warrantless digital surveillance and the seizure of devices during random street checks.
- **Organisation Registration Law (2022) as attack on independent CSOs:** This law forces all civil society organisations (CSOs) to register as service providers. Failure to comply leads to heavy prison sentences. This forces HRDs into a binary choice: operate as a State-sanctioned entity with no right to advocacy, or operate illegally in the shadows, where they lack any legal protection against digital or physical targeting.
- **Judicial dependence and absence of rule of law:** The military has dismantled judicial independence, transforming courts into administrative arms of the military. Analysis of the military's "justice" system reveals that judges are evaluated based on their loyalty to the military rather than adherence to legal principles. In cases involving digital dissent by HRDs, fair trial standards, including the right to a public hearing and the right to counsel, are systematically ignored. These puppet courts ensure a 100% conviction rate for HRDs, effectively legalising the arbitrary detention of those who challenge the military's digital control.

Digital communications

The military employs a sophisticated mix of technical blockades and coordinated technology-facilitated attacks to isolate, terrorise, and physically locate HRDs.

- **Targeted blocking and the 2025–26 election crisis:** The military has used website blocking as a cornerstone of its digital election strategy, particularly during the sham elections. Military-controlled ISPs obstructed up to 93% of attempts to access independent media and HRD's websites. This blocking was precision-targeted: media most critical of the regime faced 90%+ obstruction, while pro-military narratives remained untouched. By simultaneously unblocking unencrypted platforms, the military attempted to funnel HRDs and the wider public into a more heavily surveilled digital space where dissent could be easily tracked.
- **Localised internet shutdowns and conflict zones:** The military continues to impose localised internet and mobile shutdowns, particularly in conflict-heavy regions like Kachin, Rakhine, and Chin States. Hundreds of instances of shutdowns have been documented across many townships. These blackouts are strategically timed to coincide with military airstrikes and ground operations, serving to hide atrocities from the international community and disrupt the ability of HRDs to document war crimes in real-time.
- **Economic constraints and the digital divide:** Digital repression is inextricably linked to economic warfare. Since the coup, the military has forced ISPs to double data prices and tripled corporate taxes on providers, costs which are passed to the user. For poorer HRDs such as those in rural areas, mobile data can now cost a significant portion of their daily income. This has forced many defenders to reduce their usage or sell their devices for survival, effectively pricing the most vulnerable activists out of the digital resistance.

- **The dox-to-arrest pipeline:** There is a direct link between online harassment and physical violence. Pro-miliaty monitoring groups engage in systematic doxxing, publishing the private addresses, family details, and live locations of HRDs on digital platforms. Once a target is exposed, pro-military mobs or security forces carry out raids. This pipeline has transformed social media into a real-time tracking tool for the military's punishment lists.
- **Technology-Facilitated Gender-Based Violence (TFGBV):** Women HRDs face a distinct and coordinated campaign of fear. An analysis of social media posts revealed that politically motivated abuse directed at women was many times higher than international baselines. Pro-military Telegram channels in particular use doxxing to share private information and "nudification" tools to create non-consensual sexual imagery of women HRDs. These are used to blackmail activists or "shame" them into silence, often leading to severe psychological trauma and withdrawal from public life.

Digital restrictions on privacy

- **The PSMS national database and integrated policing:** Central to the military's surveillance architecture is the PSMS (Person Scrutinisation and Monitoring System). This national database identifies individuals considered a threat to the military, including HRDs, protesters, and political activists. PSMS is integrated into the daily operations of local police, border authorities, and military checkpoints. By checking IDs against this centralised list, the military has successfully captured and imprisoned countless HRDs during routine domestic travel or attempts to seek refuge.
- **Biometric and facial recognition infrastructure:** Under the guise of Safe City projects, the military has installed AI-driven facial recognition cameras in major cities, including Yangon, Mandalay, and Naypyidaw. These systems, sourced from international vendors allow the military to cross-reference CCTV footage against national databases. This allows them to hunt HRDs who participated in protests months or years prior, making any public appearance a life-threatening risk.
- **The VPN crackdown and deep packet inspection (DPI):** As HRDs turned to Virtual Private Networks (VPNs) to bypass surveillance and the PSMS-linked tracking, the military responded with advanced Deep Packet Inspection (DPI) technology purchased from abroad. These systems can identify VPN use and block it, stopping it working. Possession of a VPN can also lead to extortion or arrest during random phone inspections at checkpoints. This crackdown is a direct attempt to strip HRDs of their last remaining tools for anonymity and secure communication.

Corporate responsibility

International tech companies have frequently failed to meet their obligations under the UN Guiding Principles on Business and Human Rights (UNGPs) regarding the Myanmar crisis.

- **Failure to conduct heightened due diligence:** Despite being a high-risk and conflict-affected environment under the UNGPs, most technology providers operating in or supplying Myanmar

have failed to implement mandatory heightened human rights due diligence. Foreign companies and intermediaries provide the backbone of the military's surveillance State with zero transparency or accountability for the subsequent torture and arrest of HRDs. Digital platforms conduct at best minimal due diligence when planning products and usage. By prioritising market access over human rights safeguards, these firms are directly exacerbating the digital dictatorship.

- **The engagement algorithm and structural violence:** Major digital platforms continue to utilise profit-driven algorithms that are fundamentally unfit for the Myanmar context. These algorithms prioritise high-engagement content, which in a authoritarian conflict zone invariably includes State-sponsored hate speech, dehumanizing propaganda, and disinformation over factual human rights documentation. By failing to adjust algorithmic design for the local reality of mass violence, platforms effectively profit from the amplification of the very content that fuels atrocities.
- **Harmful tech company decisions:** Technology platforms, financial service providers, and service operators increasingly use international sanctions and global criticism as a blanket justification for excluding good actors in Myanmar. Independent media and HRDs, critical for countering disinformation, are frequently denied the ability to monetise their content or access advertising revenue. Communities denied internet access by the military have their satellite internet cancelled following indiscriminate and disproportionate foreign pressure. This over-compliance with sanctions regimes undermines the financial viability of truth-tellers while State-controlled entities often find back-door methods to maintain their digital presence.

Recommendations

HRM urges the OHCHR and UN Member States to take the following urgent actions:

1. **Impose a comprehensive technology moratorium:** Immediately halt the export, sale, and transfer of dual-use surveillance technologies (including facial recognition, DPI equipment, and spyware) to the Myanmar military and its intermediaries.
2. **Protect the right to encryption:** Recognise the use of end-to-end encryption and VPNs as essential life-saving tools for HRDs in repressive environments and condemn any legislation that criminalizes their use.
3. **Mandatory corporate due diligence:** Enforce legislation requiring tech companies to perform and publish human rights impact assessments specifically focused on their operations (or the use of their products) in Myanmar.
4. **Digital evidence preservation:** Support the development of decentralised, blockchain-based, or high-security digital repositories to preserve evidence of human rights violations for future accountability mechanisms, ensuring the military cannot delete the history of its crimes.