HUMAN RIGHTS MYANMAR

Impact of digital surveillance on civic space in Myanmar

Submission to the UN Rapporteur on Freedom of Assembly and Association – November 2025

Introduction

Since the 2021 coup, the military has deliberately constructed a digital dictatorship in Myanmar, using surveillance to undermine the rights to freedom of assembly and association. This report documents the specific technologies deployed, the legal architecture created to legitimise repression, the complicity of private actors, and the devastating, targeted impact this surveillance has on human rights defenders, journalists, civil society organisations (CSOs), and marginalised groups. It shows surveillance is not merely a tool for monitoring but is the core infrastructure of the military's rule by lawfare, designed to atomise dissent and enable crimes against humanity. The report is submitted to the UN Special Rapporteur on freedom of peaceful assembly and of association for her recommendations to the UN Human Rights Council on the impact of digital and AI-assisted surveillance.

Impact of digital surveillance tech on association and assembly rights

The military has deployed a comprehensive and integrated apparatus of surveillance technologies that allows the military to link an individual's physical presence (assembly) to their digital identity and networks (association).

The surveillance apparatus

The military's surveillance tech operates through several key integrated technologies.

First, AI-powered physical surveillance is expanding through a network of "Safe City" CCTVs, including facial recognition and license plate recognition systems, in major cities such as Naypyidaw, Mandalay, and Yangon. This technology, supplied by Chinese firms including Dahua, Huawei, and Hikvision, is explicitly used to watch protesters, identify them by matching surveillance data against national registration card databases, and enable their subsequent arrest and retaliation. This system transforms public spaces, the traditional sites of peaceful assembly, into zones of constant aggression and continuous monitoring.

Second, network-level surveillance is being implemented via a Great Firewall, which the military is building with assistance from the Chinese State-affiliated company Geedge Networks. This system uses Deep Packet Inspection (DPI) to monitor, filter, and block all internet traffic, including encrypted communications, and can decrypt traffic encrypted with SSL/TLS protocols. This technology grants the military unprecedented control over the content of online association and assembly.

In addition, device and communications surveillance is conducted through sophisticated spyware technology acquired from suppliers in China, Russia, and Iran. This allows for the targeted infiltration of devices, intercepting private communications, and tracking the location of human rights defenders, journalists, and civil society members.

Finally, the military is aggressively rolling out a national Electronic ID (e-ID) system. It has a history of collecting biometric data (fingerprints, iris scans, family lineage) during voter registration, including in ethnic minority villages. This data feeds a centralised Personal Scrutinisation and Monitoring System, creating a comprehensive database for repression.

Established in secrecy

Knowledge of this surveillance tech is derived from leaked documents, partner reports, and whistleblower accounts, not from any public announcements or consultation. The rollout of these technologies has been marked by complete opacity. No meaningful consultations were held before the deployment of facial recognition systems. When a draft of the Cybersecurity Bill (2022) was shared with business groups, their widespread condemnation was summarily ignored. The military then circumvented this by quietly incorporating the surveillance provisions into amendments to the Electronic Transactions Law.

Legal justifications

The military's primary justification is national security, public order, and preventing crime. However, this is a façade. The military's first act after seizing power in the 2021 coup was to systematically dismantle existing legal safeguards and replace them with a new legal architecture designed to explicitly authorise and legitimise total surveillance.

This replace-and-repress strategy involved two steps. First, immediately after the coup, the military suspended key provisions (Arts. 5, 7, and 8) of the Law Protecting the Privacy and Security of Citizens (2017), removing all basic protections against warrantless surveillance, search, seizure, and arbitrary detention.

Second, it introduced a new, repressive "legal" framework, including:

1. Amended Electronic Transactions Law: Amended in February 2021, this law grants authorities sweeping powers to access, intercept, and confiscate personal data without judicial oversight. It creates broad, vague crimes for "false news" and information that could "lower dignity" or "destroy unity," effectively criminalising all online dissent.

2. 2025 Cybersecurity Law**:** Adopted in 2025, this law mandates that digital platforms and service providers retain all user data (names, IP addresses, browsing logs) for three years and hand it over to military authorities on demand. It criminalises the establishment of VPNs and allows the military to block any platform at will.
3. Counter-Terrorism Law Bylaws**:** New bylaws introduced in March 2023 grant authorities sweeping powers to intercept communications without a warrant and explicitly designate opposition groups (like the National Unity Government) as "terrorist" organisations.

This is the weaponisation of law to create a legalistic basis for a digital dictatorship. This strategy gives the military's repressive acts a veneer of domestic legality, retroactively legalising the very violations the previous laws were meant to prevent, thereby frustrating international accountability efforts that rely on clear violations of national law.

Private sector complicity

The surveillance apparatus is built and operated through corporate complicity, primarily by two groups.

First, foreign technology suppliers provide the technology for repression. A host of foreign, predominantly Chinese, companies are involved. Geedge Networks (Jizhi) provides the Tiangou Secure Gateway (TSG) and Cyber Narrator, the DPI Great Firewall technology. Dahua, Huawei, and Hikvision supply the AI-powered CCTV and facial recognition systems. The China National Electronics Import and Export Corporation (CEIEC) is involved in providing a location-tracking system. Local brokers, such as Mascots Group, act as intermediaries, facilitating deals for both DPI and location-tracking tech.

Second, domestic telecommunications operators are reportedly complicit in implementing the military's surveillance infrastructure. Mobile network operators and other internet service providers are involved. Mobile operators, Myanma Posts and Telecommunications (military-controlled), Mytel (military-owned), ATOM (formerly Telenor), and Ooredoo (now Nine Communications), have installed Geedge's TSG hardware in their data centres, hosted intercept spyware, and are compelled to hand over user data on demand.

This relationship constitutes a surveillance-as-a-service business model. The military provides the legal demand (repressive laws) and impunity. Foreign firms (like Geedge) provide the technology (DPI, AI). Domestic telcos (like ATOM and MPT) provide the infrastructure and access to millions of internet users. This creates a closed-loop, profitable ecosystem of repression. The telcos, trapped by the military's control, have become the primary data collectors for the military.

Consequences of digital surveillance on the exercise of assembly and association rights

The consequences of this surveillance tech have been severe attacks on the rights to assembly and association.

Criminalisation and dissolution of associations

The military's surveillance tech has been used to identify, target, and neutralise virtually all forms of independent association. Trade unions and CSOs, for example, face an existential threat. Targeted persecution, including surveillance, threatening phone calls, and raids on homes and offices enabled by tracking, has forced them to halt operations or flee. The military has banned most trade unions and imposed a mandatory, complex Organisation Registration Law (2022) to criminalise any organisation that does not submit to its total control. Furthermore, the military has dissolved at least 40 political parties, including the National League for Democracy (NLD), for failing to register under its new repressive law, effectively eliminating all political association.

Criminalisation of assembly online and offline

The deployment of offline assembly tools like AI-CCTVs with facial recognition is a direct response to street protests. It allows the military to identify participants after the fact and retaliate, ensuring that any non-violent assembly leads to arrest. Gatherings of more than five people remain prohibited.

The military now also treats online assembly as a criminal act. Civil society activists have been arrested simply for posting messages on Facebook urging people to join a silent strike. This equates a Facebook post with a physical threat to the state.

Arrest, detention, and prosecution from digital surveillance

Surveillance is the primary tool feeding the military's mass-arrest campaign. As of November 2025, the military has arbitrarily detained almost 30,000 people. The military is conducting large-scale mass arrests for online expression. Thousands of people have been detained for anti-military social media posts after the coup, averaging 60 people every month.

Digital surveillance now constitutes the primary evidence for prosecution, a process that involves the weaponisation of digital evidence. Some individuals are tracked via their IP address and SIM card. Others are arrested after pro-military supporters informed authorities about online criticism of the military. Authorities also conduct random street checks of mobile phones, where people can be arrested for simply possessing photos of protests or having a VPN app installed.

Laws used to prosecute digital dissent

The military uses an interchangeable set of laws to ensure prosecution. The charge is arbitrary. The goal is imprisonment.

The first of these is Article 505A of the Penal Code, which criminalises any statement that causes fear or spreads false news against the military. It is used to jail journalists, activists, and any civilians for critical Facebook posts. The Electronic Transactions Law is also used to prosecute the act of posting.

The most severe law is the Counter Terrorism Law. By designating all opposition (NUG, PDF) as terrorists, the military uses surveillance to find any link, such as sharing news, contacting a PDF, or financing terrorism, to justify life sentences.

This system constitutes rule by lawfare. The surveillance apparatus (IP tracking, DPI) is the feeder mechanism for this system, automatically identifying targets. The repressive laws are the processing mechanism. They are so broad and interchangeable that an arrest can always be legally justified. This creates an automated pipeline of repression, moving a person from an online post to a life sentence with chilling efficiency. The law is no longer a shield for the public but a sword for the State, and surveillance is the hand that wields it.

Legal architecture of digital repression in Myanmar			
Law	**Key repressive provision/action**	**Surveillance method enabled**	**Targeted group and example**
Penal Code, Section 505A	Criminalises incitement and "false news" against the military; speech that causes "fear".	Social media monitoring; phone checks	Activist arrested for a Facebook post urging participation in a silent strike.
Electronic Transactions Law (Amended 2021)	Grants authorities warrantless access to data; broad definitions of "misuse"; criminalises "false news"	Social media monitoring; data interception	Journalist charged under of the Electronic Transactions Law Art. 33(b) and Penal Code Art. 505A.
Counter-Terrorism Law (Amended 2023)	Designates NUG, PDF, and opposition groups as terrorist organisations.	IP/SIM tracking; communications intercept	Journalist arrested via IP/SIM trace, charged under Penal Code Art. 505A & Counter Terrorism Law and given a life sentence.
Cybersecurity Law (2025)	Mandates 3-year data retention; criminalises VPN establishment; allows platform blocking.	Deep packet inspection; VPN blocking; phone checks	Authorities conduct random street checks, arresting and fining people for having VPN apps on their phones.
Law Protecting Privacy (2017)	*Suspended* Sections 5, 7, and 8.	Warrantless search and seizure; AI/facial recognition	Removes legal basis to challenge warrantless surveillance, search, or seizure, enabling all other violations.

Impact of digital surveillance on targeted individuals and groups

The military's surveillance is not indiscriminate. It is focused on specific individuals and groups to maximise fear and control, with a clear intersectional and discriminatory impact.

The high-tech war on women

The military and its supporters conduct a high-tech war on women, using surveillance data as fuel for a coordinated online campaign of fear.

This has a severe impact on well-being and mental health, as women targeted by these campaigns report severe emotional and psychological effects, including living in constant fear, depression, and distress. The tactics are a form of psychological warfare.

It also has a major impact on reputation through sexualised disinformation. Pro-military channels on platforms like Telegram, which has become a hotbed of pro-military activity, systematically target women's rights defenders. They use doxxing (publishing private data like names and addresses) and sexualised disinformation. Women are also falsely accused of being morally corrupt or promiscuous, or are depicted in dehumanising, sexualised imagery. These narratives are often perpetuated and endorsed by official military media, demonstrating State-level coordination.

This harassment is directly linked to offline violence. Doxxing posts explicitly call for the targeted women to be punished offline, including calls for their arrest and seizure of property. Pro-military channels have been seen celebrating news of their arrests, showing a direct link between online targeting and offline security force action.

Finally, it has a devastating impact on relationships. By doxing women and their families, the military breaks down support networks and uses family members as leverage, inflicting maximum psychological trauma.

Targeting of civil society

The military's surveillance has a severe impact on the capacity of CSOs. For CSOs and trade unions, surveillance poses an existential threat. The targeted persecution, including arbitrary arrests, detentions, acts of violence, raids on homes and offices, seizure of equipment, and surveillance, has crippled their ability to operate, forcing them underground or into exile.

This targeting also has an impact on the capacity of journalists. Journalists face constant surveillance, forcing many to operate in exile. This surveillance extends to their sources. The public is now less willing to share information for fear that military officials are scanning news material to hunt them down. This targeted surveillance breaks the ability of journalists to associate with sources, strangling independent media at its root.

For human rights defenders, there is a clear impact on reputation. Defenders are doxed and branded as terrorists. Their data is purposefully used to encourage discrimination.

Discrimination against minorities

A sinister long-term impact of the military's surveillance project is the potential for the creation of an AI-driven system for predictive repression and discrimination. This creates the potential for what amounts to an algorithmic apartheid.

The mechanism for this is clear: the military is collecting biometric data (fingerprints, iris scans, family lineage) in rural villages through processes like voter registration. This data is being fed into centralised systems alongside the new national e-ID project. When this massive biometric database is cross-referenced with surveillance data (CCTVs, online activity) and processed by AI, the military has the capability to develop opaque algorithms.

These algorithms could then be used to assign risk scores based on ethnicity, inferred political affiliations, and biometric characteristics. This would move repression beyond punishing actions (like protesting) to pre-emptively punishing identity. An ethnic minority individual could be algorithmically flagged as a potential opposition supporter, leading to pre-emptive arrest, extrajudicial interviews, or denial of social benefits and public services. This is a digital and AI-assisted system that automates the military's longstanding discriminatory practices against groups like the Rohingya and other minorities.

Chilling effects on civic engagement and democratic debate

The online campaign of fear and the system of mass arrests have generated a profound, society-wide chilling effect.

Collapse of online civic space and public engagement

The primary impact is the atomisation of dissent. Human rights defenders, journalists, and the public are forced to self-censor. This is most starkly documented among women, who retreat from public life as a direct result of coordinated, sexualised doxing campaigns. They are forced to reduce their public presence online, a direct and measurable suppression of their rights to association and expression.

This has also led to a deep erosion of trust. The military's war on informers and its use of pro-military doxers has destroyed social trust. The public is now afraid to associate with anyone (including journalists) who might be under surveillance.

Criminalisation of digital security

The military's strategy has evolved to attack the very capacity for private association. This is a chilling effect by design, achieved by criminalising privacy itself. The escalation is clear: first, the military blocks platforms like Facebook. Then people adapt, using VPNs to bypass blocks and protect their privacy. The military starts to deploy advanced firewalls (DPI) to block VPN traffic. And then the military begins arresting and fining people during random phone checks merely for having a VPN app. This is a direct, deliberate attack on the tools of privacy. The military has legally redefined the act

of seeking privacy as a criminal offence. This makes secure assembly or association online (e.g., in an encrypted chat) a high-risk, prosecutable act.

Clandestine association and high-risk "sousveillance"

The chilling effect has not eliminated association, but forced it into a highly dangerous, clandestine form. CSOs must now dedicate their limited resources to digital safety initiatives and complex security protocols, diverting from their core missions.

In response to the military's attacks, civilian resistance networks have developed sousveillance (surveillance from below). They use publicly sourced digital forms and secure channels to gather and share intelligence on military troop movements, helping resistance groups and civilians avoid harm.

This sousveillance phenomenon is a critical effect of the military's total surveillance. It demonstrates that the chilling effect has forced all association related to resistance to become an intelligence operation. This is a war within a war. While a testament to the resilience of civil society, it proves that the space for free assembly and association is gone. Association has been militarised. To associate freely is to engage in a high-risk counter-intelligence operation where capture via the military's spyware or DPI means torture or a life sentence.

Recommendations to the UN

- The international sale, transfer, and deployment of all AI-assisted surveillance (facial recognition) and network-level surveillance (DPI, spyware) technologies to Myanmar must be immediately suspended. Given the military's abuse of its legal apparatus and the lack of judicial oversight, no effective safeguards exist.
- Member States must impose targeted, coordinated sanctions on military officials and entities responsible for procuring and deploying the digital surveillance apparatus, including the Information Technology and Cyber Security Department.
- Member States must investigate the entire supply chain of repression for complicity in crimes against humanity. This includes sanctioning foreign suppliers like Geedge Networks and local brokers such as Mascots Group.
- Telecommunications providers in Myanmar (including MPT, Mytel, ATOM, and Ooredoo) must conduct human rights due diligence, resist military demands for surveillance data, and transparently disclose all requests. International investors must demand this resistance or begin responsible divestment.
- Social media platforms must invest heavily in rights-based, local-language moderation. Telegram, in particular, must end its use as a platform for violent content, including doxing and sexualised disinformation. Other platforms must also invest in moderation to prevent State-sponsored disinformation.