HUMAN RIGHTS MYANMAR

IPCM

How the military blocked independent media during the 2025-6 elections

How the military blocked independent media during the 2025-6 elections

March 2026

Executive Summary

Several hours before the military launched the February 2021 coup, it raided the offices of telecommunications companies, ordering them to shut down internet access and restore it only once a comprehensive set of digital blocks had been implemented. The military's targets included social media networks and many of the country's independent media outlets. Five years later, during the military's 2025–26 sham elections, these blocks became the cornerstone of the regime's digital election strategy.

This report reveals the evolution of these blocks, tracking their intensification during the elections. As the first in a series of investigations which will later cover journalists' experiences, this report exposes the military's weaponisation of internet infrastructure to systematically censor the media and deny the public their fundamental right to access information.

Key Findings

- The military significantly increased its website blocking during the elections, obstructing 93% of public attempts to access the large independent media websites.
- The blocks increased according to each outlet's criticism of the military with those most critical facing over 90% obstruction compared to 0% for those complying with the military's narrative.
- To stop people evading the blocks, the military increased blocks on encryption and circumvention tools to 97% and 93% while simultaneously

unblocking unencrypted platforms in an attempt to funnel the public into a more heavily surveilled digital space.

- The military tried to gaslight the public, classifying blocks as State secrets, threatening telecommunications companies (telcos) with severe imprisonment for leaks, and concealing 98% blocks as technical failures.
- All telcos failed in their responsibility to respect human rights and have become active enforcers of the military's blocking regime, including State-owned telcos MPT and Mytel which have led the crackdown with near-100% blockades of the media.

Contents

The International Programme for the Development of Communication

This report was delivered with the support of the UNESCO International Programme for the Development of Communication.

Introduction

Following five years of systemic human rights atrocities, the military regime tried to finalise its coup objectives by holding long-promised elections phased between December 2025 and January 2026. The polls were widely condemned as a sham by the international community and failed to gain recognition from regional bodies, including ASEAN. [1]

The illegitimacy of the electoral process was rooted in the military's deliberate attacks on the information ecosystem. By blocking significant portions of the internet, the military denied prospective voters the ability to exercise their right to seek and receive the information necessary for informed decision-making. Since the 2021 coup, blocking as an act of mass censorship has functioned as a digital barrier between the public and the truth.

The military did not just seize the streets during the coup; it also captured the digital infrastructure

This report investigates the military's media blocking prior to the election cycle and analyses the subsequent ratcheting up of blocks during the critical three-month countdown from September to December 2025. By evaluating these changes during the campaign period, the report demonstrates how technical interference was leveraged to manipulate the electoral outcome and secure regime survival.

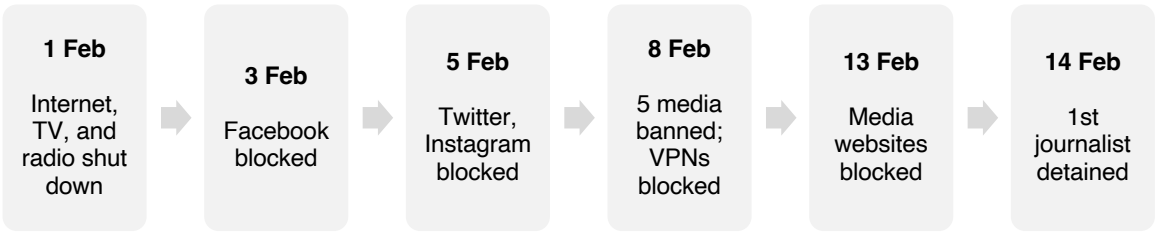
Analysing the military's blocking regime

The architecture of the digital coup was established at 3:00 AM on 1 February 2021.[2] Soldiers forcibly entered the offices of telecommunications companies (telcos), television stations, and radio broadcasters, demanding immediate service shutdowns. In the chaotic days following the coup, the public's only viable link to the outside world was through foreign SIM cards, an avenue that was eventually identified and systematically shut down too.[3]

While total internet shutdowns characterised the early weeks of the coup, the military eventually transitioned to a more surgical strategy of targeted internet blocks. The military first ordered the blocking of large social media platforms including Facebook, followed by X (formerly Twitter) and Instagram. This was followed by blocking of the websites of the country's largest independent media

[1] AP (2026), "ASEAN does not recognize Myanmar's elections, which military-backed party claims to have won".
[2] Free Expression Myanmar (2021), "Military violations of free expression timeline".
[3] Reuters (2022), "A year after Myanmar coup, growing surveillance threatens lives".

outlets, eventually expanding to include local media outlets reporting from Myanmar's ethnic states and regions.



The blocks remain five years after the coup. This report is focused on the blocks in place in this electoral year and is based on a robust data set of 198,000 internet network measurements and 1.8 million indicators collected across Myanmar between January 2025 and January 2026.[4] Each measurement tested if a desired website was accessible via a particular operator, such as MPT or MyanmarNet, and, if not, determined both the presence and type of block. Within this framework, network measurements are treated not merely as technical data, but as evidence of interference with the right to seek, receive, and impart information as guaranteed under Article 19 of the International Covenant for Civil and Political Rights (ICCPR) and the Universal Declaration for Human Rights (UDHR), which establish human rights obligations for the military. These network measurements allow the disaggregation of the data by time, location, and individual telco to expose the mechanics of the digital coup in the countdown to polling day.

The blocking regime relies on total secrecy enforced by the military. Only 2% of the blocks were transparent with declaratory pages or known censorship DNS. The remaining 98% were effectively secret blocks hidden by technical anomalies such as TCP resets or DNS tampering, which made websites appear broken or a connection appear slow.[5]

In 98% of cases, the military hides its censorship behind technical anomalies, gaslighting the public into believing that the truth is simply broken

However, by comparing these technical anomalies against error rates, control data, and the anomalies faced by pro-military platforms, it becomes clear that they were predominantly intentional, military-directed interference. This deliberate ambiguity is designed by

[4] Network measurements were collected by the Open Observatory of Network Interference (OONI).
[5] These anomalies include DNS tampering, TCP/IP blocking, HTTP blocking, and TLS based interference.

the military to gaslight the public, obscuring censorship under the guise of technical failure. Such censorship can for example be seen in the blocks facing media websites.

Blocking targeted at the independent media

By the time the 2025–26 elections were officially announced on 28 August 2025, the military had spent five years trying to isolate the vast majority of the public from the free information ecosystem online. Prior to the start of the election campaign, the military-controlled infrastructure already obstructed 79% of all of the public's direct attempts to access the websites of Myanmar's largest independent media. Given that there were approximately 24 million people in Myanmar with internet access, this represents many thousands of attempts to reach the independent media blocked daily.[6]

For the public, circumventing these blocks became a high-risk, high-cost endeavour. Maintaining access to the independent media required the regular download and installation of new VPNs in a constant game of whack-a-mole with the censors blocking the different applications as they became popular. It also required the payment of exorbitant data charges doubled by the military after the coup with the immediate effect of widening the digital divide.[7] Furthermore, in addition to the technical difficulty and cost, the physical risk of accessing the independent media was also high. Security forces at checkpoints routinely violated privacy rights by searching devices for evidence of independent media access to extort bribes or justify arbitrary arrests.

This environment of suppression also placed independent media outlets in a situation of permanent crisis. Most media, operating from exile on shoestring budgets, were forced to divert precious editorial resources toward larger IT teams and technical workarounds simply to ensure their content could reach a fraction of their audience.

Blocking escalation during the election countdown

During the three-month countdown to the election, the blocking of large independent media websites surged from 79% to 93%. A 14% increase over three months suggests that millions of additional people were affected, losing access to the

[6] Reliably quantifying affected individuals requires accurate visitor numbers for each outlet. Approximately 44% of the 54 million population have the capacity to access the internet and it is likely that many check the news daily. Freedom House (2025), "Myanmar".
[7] Free Expression Myanmar (2021), "Military violations of free expression timeline".

independent media. This spike occurred precisely when voters required access to investigative reporting to vet candidates, identify election intimidation, and monitor overt influence campaigns. By engineering this spike, the military undermined the deliberative phase of the election and increased the likelihood of hiding any electoral manipulation.

While the previous 79% blocks was already significant, it was not total information control as it still allowed some access. By increasing the independent news vacuum during the elections, the military ensured that its own propaganda, disseminated via State-controlled media, faced less digital competition.

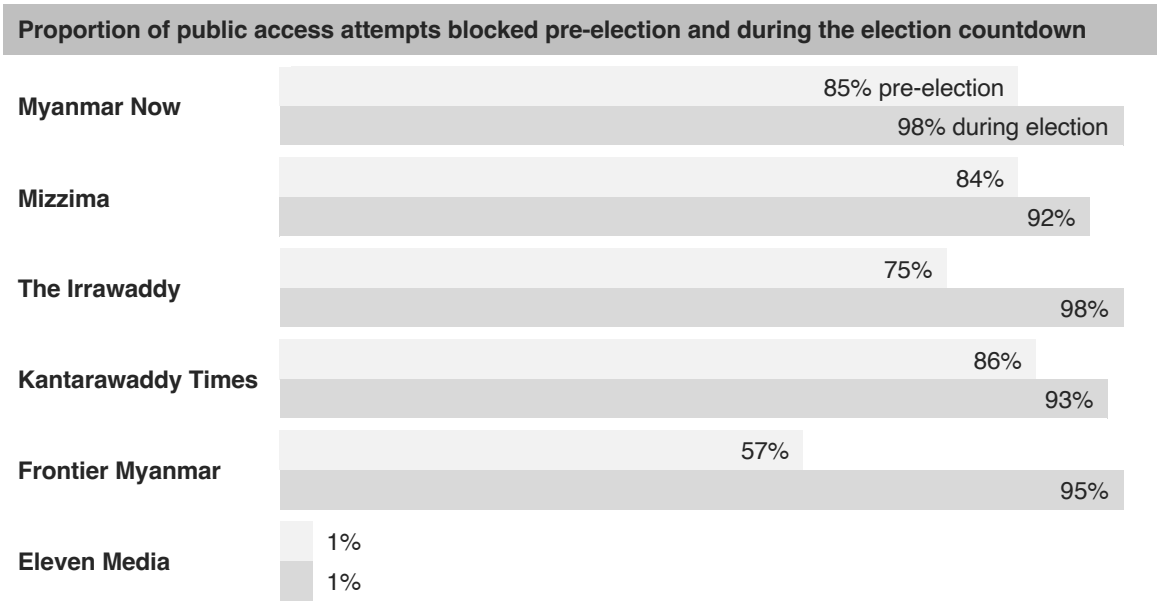
By increasing media blocks from 79% to 93% during the elections, the military ensured that the most critical phase of the election occurred in an information desert

Following the election, the blocking rate marginally declined from 93% to 85% after the end of January 2026. This drop suggests that once the military's electoral objectives were secured, the high levels of campaign-period interference were no longer deemed as necessary. This fluctuation confirms that network interference is a dynamic tool of political control, calibrated to the military's calendar.

Precision blocks against critical media

The blocks have not been applied uniformly since the coup, but focused against the most credible threats to the military's narrative. Media known for uncovering military atrocities and corruption faced the most severe website blockades. Before the election, the media outlets Myanmar Now, Mizzima, and The Irrawaddy faced the highest blocking rates of 85%, 84%, and 75% respectively. During the election countdown, these rates escalated to 98%, 92%, and 98%, rendering their websites virtually invisible to the domestic public without adequate circumvention tools.

Local, small and medium-sized media outlets have been similarly targeted since the coup, particularly those reporting from conflict zones where the military was conducting systematic human rights abuses. Myitkyina News Journal, covering Kachin State and the military's attacks on the Kachin Independence Army (KIA), faced blocking rates of 76%. Narinjara News, reporting in Rakhine State on fighting between the military and the Arakan Army (AA) faced 73% blocks. Karen Information Centre, covering military attacks on the Karen National Union (KNU) in Karen State faced 69% blocking.



Once the election countdown had begun the blocks on small and medium media increased. Kantarawaddy Times, which reports from Karenni (Kayah) State where the Karenni Army (KA) is fighting the military, saw increases from 86% to 93% blocking.

The military's intensified focus during the elections also included a more diverse range of media than before. Frontier Myanmar, an outlet focused on analytical and human rights reporting and with an audience primarily made up of English-language speakers and internationals, saw its blocking rate rise from 57% to 95% during the elections. All these increases demonstrate that the military was strategic in its targeting, aiming to censor the most critical voices and denying information to influential audiences.

Removing blocks to reward compliant media

Media that comply with the military's demands are rewarded through the blocking regime. Outlets like Eleven Media, which operate in Myanmar under the regime and practice significant self-censorship, maintained a 0% to 1% blocking rate. Certain localised pro-regime outlets were similarly left unblocked, creating a curated digital environment where only inaccessible or non-threatening voices remained audible.

This 90% gap in accessibility between compliant and independent media is a stark example of how infrastructure is used to reward subservience and punish editorial independence. It forces independent newsrooms into an impossible choice between adopting the military-vetted narrative or facing digital extinction.

The military's 90% access gap is a digital bribe: it rewards self-censorship with visibility while punishing journalism with digital extinction

For the public, this disparity creates a false sense of normal. Some people without the technical expertise or financial resources to circumvent censorship may assume that independent outlets have simply ceased to exist, while the accessible, military-compliant websites appear to represent the totality of the national conversation. This manipulation of perception is as damaging to the right to information as the blocks themselves.

Restricting socials to block media

In Myanmar, social media platforms serve as the primary gateway to the internet for most people. Because the social media apps are more accessible than browsers to those with limited technical skills and were historically subsidised through zero-rating data plans, the platforms remain the most vital distribution channels for independent media and the most common spaces for civic discourse.

Blocks on Facebook surged from 72% to 98% during the election

Social media platforms also provide a lifeline for media sustainability, allowing journalists to reach sources and, in some cases, generate advertising revenue. By targeting these platforms with blocks, the military did not just censor media content but also attacked the financial and operational foundations of the independent media.

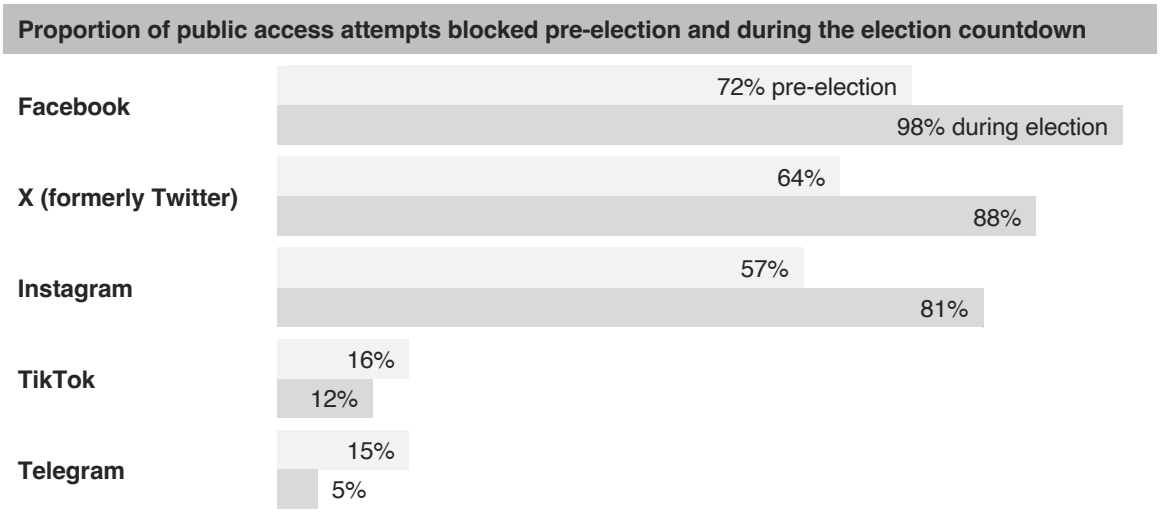
Prior to the election, 72% of attempts to access Facebook were blocked, alongside 64% for X (formerly Twitter), and 57% for Instagram. If successful, many of these attempts would have enabled people to view the media. During the election campaign countdown, these blocks reached near-total levels: Facebook blocks surged from 72% to 98%, X from 64% to 88%, and Instagram from 57% to 81%. These social media blocks essentially severed the primary artery of election-related information for the vast majority of the population.

Rewarding friendly social media

In sharp contrast to the USA-based social media platforms, the military has maintained minimal blocks on Chinese-owned TikTok and Russian-founded Telegram.[8] During the election countdown, the blocking rates for these platforms actually decreased: TikTok dropped from 16% to 12%, while Telegram fell from 15% to 5%.

The military targets accessibility based on its own geopolitical calculations, favouring platforms it links to States that offer the regime diplomatic or military backing. Furthermore, unlike Facebook and Instagram, other platforms have not implemented sanctions against military accounts to the same degree, allowing the military to use them more freely for its own election propaganda and recruitment.

This fragmentation of the digital space will have a profound effect on the audience. By blocking informative platforms while leaving entertainment-heavy apps like TikTok open, the military effectively pushes the public toward distraction and away from substantive civic engagement. This forced digital displacement fragments the media's audience and subdues public resistance through a diet of curated entertainment.



Coercing the public into surveillance

The military's targeted blocking also functions as a surveillance funnel for the media and the public. End-to-end encrypted tools that prevent the military spying on what the public is viewing and saying have been almost completely blocked since the coup

[8] TikTok is owned by ByteDance, a company founded by Chinese entrepreneurs and headquartered in Beijing. Telegram was founded by two Russians who have since left Russia.

began. Signal had a 98% blocking rate, WhatsApp a rate of 97%, and Messenger was blocked 98% of the time.

The military was trying to coerce the public into using less secure environments and tools where the military can more easily intercept communications, including access to the media. Telegram and TikTok do not offer end-to-end encryption by default and were blocked only 5% and 12% respectively during the election countdown.[9]

The military is funnelling the public away from encrypted apps and into a digital trap designed for surveillance and the exposure of whistleblowers

This is also a direct threat to the safety of journalists and their sources. Without access to encrypted channels, journalistic activities are exposed to military monitoring, placing whistleblowers and journalists at immediate risk of detention or violence. The blocks are therefore not just a barrier to information but also a mechanism to enable surveillance.

Blocking circumvention routes to the media

The Myanmar public have shown that they want unrestricted access to the internet. After the military started blocking access, the public quickly turned to circumvention tools to bypass the military blocks. Virtual Private Networks (VPNs) and other circumvention tools became essential for exercising the right to information, allowing people to bypass military-directed blocks and access independent reporting.

Before the elections, prominent circumvention tools were blocked on average 57% of the time. However, tools popular within Myanmar faced even more aggressive targeting by the military. Psiphon, a tool combining VPN, SSH, and HTTP proxy technologies, faced an 88% blocking rate. During the election countdown, average blocking increased to 65%. Popular tools like Proton VPN surged from 82% to 93% blocking during the campaign.

The double lock strategy ensures that even when people find a way to bypass the blocks, the military is already there

This demonstrated a double lock strategy by the military in an attempt to censor the media. It simultaneously blocked media websites and blocked the circumvention

[9] ESET (2025), "Breaking down Telegram's privacy promise: What's protected and what's not". TikTok (2026), "Direct Messages".

tools needed to reach them. The strategy ensured that even the most determined and tech-savvy members of the public were met with significant barriers, reinforcing the information vacuum during the country's most sensitive political window.

The role of telcos in blocking the media

Implementation of the blocking regime required the active or coerced participation of telecommunications companies (telcos). In Myanmar, the internet network is owned and run by about 120 licensed telcos, half of which are consumer-facing and half infrastructural.[10] A few telcos are State-owned operating under direct military control including MPT, which owns much of the national infrastructure and runs a large mobile phone service, and Mytel, a mobile phone telco. The majority of telcos are privately-owned, some of which are led by individuals with close ties to the military leadership commonly known as "cronies". Regardless of ownership, the military requires all licensed telcos to implement its orders including blocking demands.

The military keeps its blocking regime extremely secretive. Military orders are issued as directives through the Ministry of Transport and Communications (MoTC) and are protected by the Official Secrets Act which includes severe prison terms for anybody caught whistleblowing.

Differences between State and private telcos

Telcos have been transformed from connectivity providers into the enforcers of State-sponsored isolation

Network measurements show that there were some differences in the telcos' implementation of military orders. While the average rate of blocking large independent media during the election countdown was 93%, some telcos blocked more. State-owned and military-controlled MPT maintained a 100% blockade and military-owned Mytel reached 98%. This indicates that telcos are not neutral infrastructure providers but have become active participants in the military's suppression of fundamental rights.

In general, private telcos enforced the military blocks to a similar extent as the State-owned telcos. However, several individual telcos may have interpreted the orders

[10] This does not include those telcos operating in the opposition-held territories of Myanmar such as Starlink.

using less restrictive technologies, allowing their customers slightly more digital freedom. For example, a telco may have implemented blocks at the DNS level, which was easily bypassed by tech-savvy users, rather than IP-level filtering. Those individual telcos did not make any public claims to protect their customers' digital rights and therefore their exact motivations are unclear. However, for their security, they will not be named in this report and details of their comparative difference will not be disclosed.

These quiet acts of defending digital rights likely allow many people to access information and maintain a fragile link to the truth. Nevertheless, the overarching reality remains that the majority of Myanmar's telcos act as a direct enforcer of the military's information blockade.

Blocking under international law

Under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR), any restriction on the right to freedom of expression, like a block, must pass the three-part test of legality, legitimacy, and necessity. However, the military's blocking regime failed every pillar of this test.

First, the blocks were not legally sound. The military was not a lawful government and therefore its directives were not lawful too. Even if the government was lawful, the directives lacked transparency, legal precision, legal predictability, judicial oversight, and avenues for appeal.

Second, the blocks were not necessary to achieve the legitimate aim of protecting national security (assuming that is what the directives claimed). The blocks were targeted at websites like the media that do not threaten the existential security of the country but rather only threaten the military's control of the State. National security claims cannot be invoked to protect authorities from embarrassment or to conceal illegal acts (like a coup).

"National security" is not a license for regime survival. The systematic blocking of the media is a violation of international law

Third, the harm caused by the blocks was not proportionate to any potential benefit. Blocking entire social media platforms and media websites with their millions of users and pages of information was a blanket measure that far exceeds any real localised security requirement.

There was no legitimate justification under international law for the scale and nature of the military's blocking as documented in this report. The blocking regime was therefore not a security measure, but a gross violation of international law designed to preserve a military dictatorship through the systemic closure of civic space online and the erasure of the independent media.

Responsibilities of telcos

Under the UN Guiding Principles on Business and Human Rights, telcos have an independent responsibility to respect human rights, regardless of State pressure.[11] While the military employed coercion and threats of violence, telcos operating in Myanmar were not merely passive victims. By implementing clandestine blocks that used technical anomalies rather than transparent block pages, telcos were failing their human rights due diligence.

This lack of transparency prevents people from identifying and challenging censorship, effectively making these telcos complicit in the military's regime of secrecy. To meet their international obligations, telcos choosing to operate in such environments must take all possible steps to mitigate the harm of authority directives, including providing maximum transparency to their customers and resisting the use of deceptive blocking technologies.

Conclusion

The military's blocking regime has become the cornerstone for its systematic violation of the public's digital rights, including their rights to freedom of expression, association, assembly, privacy, and participation in public affairs. It is a regime designed not only to silence the independent media but to manipulate the public into digital spaces where they can be more easily monitored and repressed. By ratcheting up the blocks of independent media during the 2025–26 elections, the military attempted to engineer a campaign period without independent scrutiny. While the blocking regime continues elections can never be free or fair, and Myanmar will remain a global landmark in digital authoritarianism.

This report, the first of three, exposes one element in how Myanmar's independent media was attacked during the elections. Subsequent reports will detail attacks on social media platforms and the resulting toll within the media outlets themselves.

[11] UN OHCHR (2011), "Guiding Principles on Business and Human Rights".

Recommendations

- The authorities must immediately and unconditionally end all internet blocking and network interference, ensuring the public's right to seek and receive information is restored in accordance with Article 19 of the ICCPR.
- Electoral observers, foreign States, and international bodies should recognise that no election in Myanmar can be considered free or fair while the blocking regime remains in place.
- Foreign States and international bodies should expand sanctions regimes targeting those involved in the design and implementation of the blocking regime, including the leadership of the Ministry of Transport and Communications.
- Telcos must implement robust human rights due diligence processes to identify, prevent, and mitigate the harm caused by military directives, providing the public with transparency reports and serving users with transparent block pages rather than deceptive technical anomalies.
- Civil society, responsible businesses, and donors should increase financial and technical support for diverse and multi-platform independent media outlets, including television and radio, and the development of robust, high-availability circumvention technologies for the Myanmar public.

With financial support provided by