

August 6, 2025

Risk Analysis & Insights, Asia-Pacific, Defence & Security

Surveillance and Suppression in Post-Coup Myanmar

By Lara Westra

More than two years after the 2021 coup, Myanmar remains under military rule, with the Junta using surveillance and digital repression to silence dissent and block democratic progress. Despite the appearance of electoral processes in the past, Myanmar’s political structure has allowed the military to maintain unchecked power (King, 2022). The Tatmadaw’s use of technology, including facial recognition, social media monitoring, and disinformation campaigns, reflects a dangerous evolution from traditional authoritarian tactics to a modern surveillance state (Dean, 2017). These practices have not only oppressed civil society and political opposition but have also exacerbated existing humanitarian crises.

A Democratic Façade

Since 2011, Myanmar appeared to undergo a transition toward democracy and a market economy. However, this transition was structurally constrained from the beginning. The 2008 Constitution guaranteed military control over three powerful ministries, defence, home affairs, and border affairs, along with ‘25%’ of parliamentary seats and veto power over constitutional amendments (Hlaing, 2012; King, 2022, P.3).

The landslide victory of the National League for Democracy (NLD) in the 2020 elections deepened tensions between the civilian government and the military (King, 2022). On February 1, 2021, General Min Aung Hlaing and the Tatmadaw (Myanmar’s military) launched a coup, citing unsubstantiated claims of voter fraud (King, 2022). Despite denials by the Union Election Commission and international election observers such as The Carter Center, the military proceeded to dissolve democratic institutions and assert control (King, 2022).

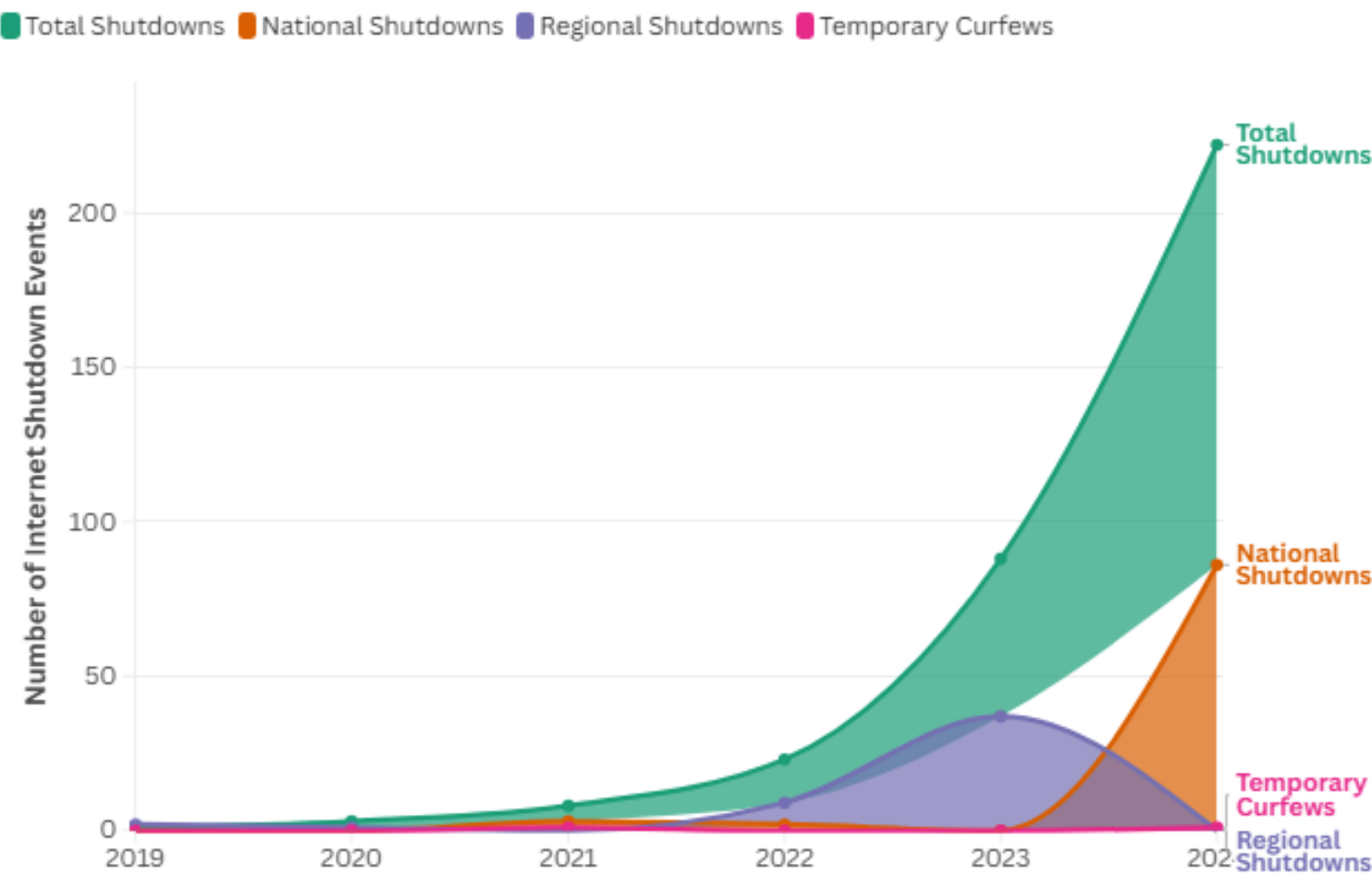
Myanmar’s Internet Weaponisation Tactics

While the military’s repressive methods are not particularly novel, their technological sophistication has grown. In previous regimes, such as the German Democratic Republic (GDR), the Stasi relied on informants, wiretaps, and mail interception to control the population (Domínguez, 2024). Today, Myanmar’s intelligence services use tools such as facial recognition, drone surveillance, internet monitoring, and algorithmic tracking to monitor dissent with far greater reach and efficiency (Htwe, 2025).

The Tatmadaw’s Office of the Chief of Military Security Affairs (OCMSA), in coordination with the Myanmar Police Force (MPF) and its intelligence arms, including the Special Branch and the Criminal Investigation Department, operates a highly coordinated surveillance network (Dean, 2017). These agencies not only collect information but

The Internet is now a major source of information shaping worldviews and political beliefs. Weaponisation involves using information, true, false, or biased, in ways that cause harm or manipulation (McLoughlin, 2023). Threats can come from individuals, groups, or even AI-powered algorithms and large language models. Digital repression in Myanmar goes beyond passive surveillance. For example, three years since the coup, the Junta have conducted internet shutdowns and telecom jamming ahead of military assaults which fuelled widespread arrests, with thousands of activists, journalists, and civilians arbitrarily detained (Htwe, 2025). In addition, the Junta actively deployed disinformation campaigns through state-controlled and fake social media accounts to discredit opposition movements, distort facts, and justify its grip on power (Htwe, 2025).

Internet Shutdown Events in Myanmar



*Temporary curfews were largely part of regional and national shutdowns with very few stand-alone events.

Currently, mobile internet shutdowns, the arrest of elected officials, and the silencing of independent media have become routine (Selth, 2025). Surveillance systems in major cities now include CCTV cameras with license plate and facial recognition capabilities, further expanding the regime’s ability to monitor and intimidate its population (Selth, 2025). Most recently, the Junta banned major VPN services, cutting citizens off from secure access to blocked apps like Facebook and messaging platforms (Padmanabhan et al., 2021). Authorities also randomly inspect phones under anti-terror laws, seizing VPN apps and detaining users (Padmanabhan et al., 2021). These operations are used below the threshold of war, allowing plausible deniability and making attribution difficult (Coppel and Chang, 2024). Consequently, feedback loops are occurring, where responses are creating secondary threats, leading to echo chambers and escalating tensions.

Civil Conflict and Humanitarian Consequences

Myanmar’s political instability is intertwined with long-standing civil wars, ethnic tensions, and colonial legacies. Military campaigns against ethnic minorities, most notably the ongoing Rohingya conflict that has created a deep-seated humanitarian emergency (Debnath et al.,2022) Additionally, armed clashes in Kachin and Shan states have caused mass displacement, food insecurity, and the erosion of public services (King, 2022).

International actors should expand sanctions on companies linked to the military and restrict military access to surveillance technology. Additionally, support for international legal mechanisms, including the International Criminal Court and UN investigative bodies, is vital to address war crimes and systemic repression. Finally, tech companies should be vetted and held accountable for enabling surveillance and propaganda in authoritarian regimes. Content moderation and platform transparency must improve in Myanmar’s context.

Myanmar today highlights an example of how authoritarian regimes adapt, merging traditional military control with modern digital surveillance to maintain power and suppress dissent. If left unchallenged, the normalisation of these

the evolving nature of authoritarianism and respond with equally adaptive strategies rooted in accountability, protection, and support for democratic resilience.

Reference

Coppel , N. and Chang, L.Y.C. (2024). Weaponising the Internet. Springer eBooks, pp.37–60.
doi:https://doi.org/10.1007/978-3-031-58645-3_3.

Dean, K. (2017). Myanmar: Surveillance and the Turn from Authoritarianism? Surveillance & Society, 15(3/4), pp.496–505. doi:<https://doi.org/10.24908/ss.v15i3/4.6648>.

Debnath, K., Chatterjee, S. and Afzal, A.B. (2022). Natural Resources and Ethnic Conflict: A Geo-strategic Understanding of the Rohingya Crisis in Myanmar. Jadavpur Journal of International Relations, 26(2), p.097359842211203. doi:<https://doi.org/10.1177/09735984221120309>.

Domínguez, P.L. (2024). The State Espionage in the Digital Era: Lessons Learned from the STASI for International Security. Facultad de Ciencias Humanas y Sociales Grado en Relaciones Internacionales, pp.1–60.

Hlaing, K.Y. (2012). Understanding Recent Political Changes in Myanmar. Contemporary Southeast Asia, [online] 34(2), pp.197–216. Available at: <https://www.jstor.org/stable/41756341>.

Htwe, T.M. (2025). The Role of Intelligence Agencies in Repression and Torture by Myanmar’s Military Junta Intelligence and its Human Rights Abuses During the 2021 Revolution. The Journal of Intelligence, Conflict, and Warfare, 7(3). doi:<https://doi.org/10.21810/jicw.v7i3.6849>.

King, A.S. (2022). Myanmar’s Coup d’état and the Struggle for Federal Democracy and Inclusive Government. Religions, [online] 13(7), p.594. doi:<https://doi.org/10.3390/rel13070594>.

McLoughlin, I. (2023). A Framework for Understanding the Weaponisation of the Internet. 2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp.1–7.
doi:<https://doi.org/10.1109/soli60636.2023.10425340>.

Padmanabhan, R., Filastò, A., Xynou, M., Raman, R.S., Middleton, K., Zhang, M., Madory, D., Roberts, M. and Dainotti, A. (2021). A multi-perspective view of Internet censorship in Myanmar. Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet. doi:<https://doi.org/10.1145/3473604.3474562>.

Selth, A. (2025). Spy Versus Spy: Myanmar’s Multiple Counterintelligence Challenges. International Journal of Intelligence and CounterIntelligence, pp.1–34. doi:<https://doi.org/10.1080/08850607.2025.2453723>.

IN THIS SECTION

Risk Analysis & Insights



Search ...

About the Author



Lara Westra

Lara Westra is currently working as a financial compliance professional for a leading US investment bank and holds a BA in International Relations from Nottingham Trent University. Her interests include the intersection of international relations theory, international security, and international political economy.



SIMILAR POSTS



[Risk Analysis & Insights](#), [North America](#), [International Relations](#)

Heavy Oil, Heavy Dependence: How US Refineries Anchor Canada’s Oil Industry

Levente Bartha

As tensions between the US and Canada come to a head, how will the American leverage over the Canadian oil industry give Washington an edge in the rivalry? The bilateral...

[Read more](#)



[Risk Analysis & Insights](#), [Titan](#)

China increases funding for BRI projects under new risk outlook

Gabriel Lane

[Read more](#)



[Risk Analysis & Insights](#), [Titan](#), [Experts](#), [Defence & Security](#), [Global Governance](#), [International Relations](#)

A New Global Security Architecture: Disbanding NATO, Uniting Europe, and Reshaping Global Alliances

Leon Donadoni

For more than seventy years, NATO has been the primary guarantor of Western security, born in the early years of the Cold War to deter Soviet expansion. While it served...

[Read more](#)

Useful links

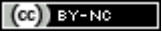
[ABOUT US](#)

[SUBMISSIONS](#)

[CAREERS](#)

Follow us



© Copyright 2025 — Atlas Institute for International Affairs. All Rights Reserved. All content on the website is published under the [Creative Commons Attribution-NonCommercial 4.0 International License](#). 

[PRIVACY POLICY AND TERMS OF USE](#)

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. [Accept](#) [Read More](#)