



Digital & Telecoms Risk

Myanmar Telecom Risk, Part 1 of 4: Surveillance and the Law

Sep 21, 2026 | Share     

The Bottom Line

Myanmar ranks at the bottom of Freedom House's global internet freedom index, tied with China at a score of 9 out of 100.¹ Since the military took power in February 2021, the authorities have rebuilt the country's networks around three capabilities. Operators can intercept calls and messages; the international gateways inspect and filter traffic; and registration rules tie each SIM and handset to a named individual. The Cybersecurity Law, which took effect in July 2025, gives that arrangement a statutory basis.

Our advice to anyone connecting in Myanmar is based on three working assumptions. Traffic on a local network can be read, any phone can be inspected, and the authorities can obtain a company's



device registration, and Part 3 covers social media and practical security guidance. Part 4 compares Myanmar with other countries and with the data collection practices of the large technology platforms.

Interception at the Operator

The interception capability predates the takeover by several months. In late 2020, the Ministry of Transport and Communications and the Ministry of Home Affairs pressured all four mobile operators to install lawful intercept equipment. This equipment allows the security services to listen to calls, read messages, and track a subscriber's location without going through the operator each time.² The Israeli firm Cognyte won the tender for the interception gateway at state-owned MPT in December 2020.³

Telenor had installed a gateway made by Utimaco of Germany but said it never activated it. In September 2021, it cited pressure to activate the equipment as a main reason for leaving.⁴ When the sale closed in 2022, the gateway passed to military-linked Shwe Byain Phyu, which now operates the network as ATOM, along with call records for more than 18 million subscribers.⁵ Ooredoo agreed to its own sale in September 2022 and completed the exit in May 2024. That network now trades as U9.⁶ Mytel is a joint venture between the military and Viettel of Vietnam. With those two departures, no independent foreign operator is left in the market.⁷

Filtering at the Gateway

The filtering system was supplied from China. Documents leaked in September 2025 show that Geedge Networks, a company linked to the designer of China's Great Firewall, sold Myanmar its Tiangou Secure Gateway. Trials ran from June to November 2022, and the rollout was completed by July 2024. The equipment is installed in 26 data centers belonging to 13 operators and internet service providers, and it is operated from command centers in Yangon and Nay Pyi Taw. It copies traffic for inspection and blocks more than 1,000 applications based on their behavior on the network. It can also locate a subscriber in real time by matching activity to a cell identifier.^{8,9}

Justice For Myanmar lists the hosts as the four mobile operators, along with Frontiir, Campana, StreamNet, China Unicom (Myanmar), Golden TMH, MBT, MTN, Global Technology Group, and IM-Net.⁸ Because the contract provides for Geedge engineers on site and monthly updates, we expect the system's performance to continue improving.

Cameras and Checkpoints

Chinese suppliers also provide camera networks. In December 2020, 335 Huawei cameras with facial and license plate recognition began operating in Nay Pyi Taw as part of the Safe City project. Huawei says it supplied standard infrastructure equipment and did not supply the recognition technology.¹⁰ Our assessment, [The Security Systems Watching You](#), examines the exposure that Chinese-made security equipment creates for companies.¹¹ Dahua and Hikvision systems followed



At checkpoints, the military uses what it calls the Person Scrutinization and Monitoring System (PSMS), which combines database queries, facial recognition, and national ID validation. Its use has been reported at road checkpoints, at Yangon and Tachileik airports, and on express trains. It is also used at hotel check-in, where it became mandatory in June 2026 under the Guest List Information System.¹³

The Monitoring Committee

The monitoring relies on both people and equipment. On 28 April 2026, the government formed a committee to monitor the internet around the clock. Its chairman is Deputy Home Affairs Minister Major General Min Thu, a former head of the Military Intelligence IT department. It draws members from the communications, legal affairs, and information ministries, the Central Bank, and Military Intelligence. The law obliges telecommunications operators and banks to cooperate with it. By the government's own count, 21,369 online users were targeted between 2024 and May 2026, and almost 20,000 of them were prosecuted on counter-terrorism charges.¹⁴

Shutdowns remain a routine instrument, and Access Now logged 95 in Myanmar in 2025, the highest figure for any country. It attributed 76 to the military.¹⁵ Some areas of Kachin, Sagaing, and Rakhine have had no service for over a year.¹³

The Cybersecurity Law

The State Administration Council enacted Cybersecurity Law No. 1/2025 on 1 January 2025, and Notification 113/2025 brought it into effect on 30 July 2025.¹⁶ An earlier 2022 draft proposed prison terms of up to three years for individual VPN users. That penalty does not appear in the final text, which is otherwise broader in scope than the draft, and four of its provisions merit attention.

Extraterritorial reach. The law applies to offenses connected to Myanmar wherever they are committed, meaning Myanmar citizens living abroad can be charged.¹⁷

VPN services. Setting up or providing a VPN service without ministry approval carries a prison term of one to six months and a fine of MMK 1 million to 10 million. Organizations face a minimum fine of MMK 10 million. The text does not make individual VPN use an offense.^{16,18}

Platform registration. A digital platform with more than 100,000 users in Myanmar must register locally, retain user data for up to three years, and provide it to authorized bodies upon written request. Failure to register exposes the platform to fines starting at MMK 100 million and to blocking.^{16,17,18}

Licensed security providers. Only Myanmar-registered companies may provide cybersecurity services under licenses valid for three to ten years.¹⁷

In practice, the older laws still do most of the work. In February 2021, the military suspended the privacy safeguards in the 2017 Law Protecting the Privacy and Security of Citizens and inserted Section 505A into the Penal Code. It also amended the Electronic Transactions Law to criminalize



Cybersecurity Law, and the implementing rules and licensing procedures had not been issued.

Two measures adopted in 2026 send more data to the state. The Anti-Online Scam Law, enacted in late July 2026, allows banks to freeze a suspect account within 15 minutes. It also creates a central database linking bank accounts, SIM cards, IP addresses, and phone records.²⁰ Digital rights monitors interpret it as also obliging operators to archive subscriber location data and call records for official access.¹³ A March 2026 amendment to the Anti-Money Laundering Law empowers the Ministry of Home Affairs to intercept and disconnect communication lines.²¹ The government describes both as anti-fraud measures, but their practical effect is to widen what the authorities may lawfully collect.

Risk Snapshot

Personal risk. Calls, messages, and unencrypted traffic on every Myanmar operator are vulnerable to interception without judicial oversight, and cell data gives authorities a subscriber's location in real time. Arrests under Section 505A and the counter-terrorism law have followed Facebook comments, TikTok captions, and private messages, and documented cases number in the thousands. The Cybersecurity Law continues to apply to Myanmar citizens even after they leave the country.

Business risk. State interception or filtering equipment is present on the networks of all four mobile operators and nine ISPs, so a company cannot avoid it by choosing a different carrier. A corporate VPN has no route to approval and therefore operates unlicensed. Platforms with more than 100,000 Myanmar users are required to register and retain data for three years, but no regulator is yet in a position to accept this. Banks and operators are legally bound to assist the monitoring committee, which places financial and call records within easy reach of the state. Doing business with the named operators is lawful, though it carries reputational exposure and should be covered in sanctions monitoring.

Safety measures. Treat the mobile network as hostile and prefer end-to-end encrypted messaging over trusted Wi-Fi for any traffic sent through a registered SIM. Keep material critical of the military off every device entering the country. Ensure local staff understand that the law applies to them abroad, and do not ask them to take risks on the company's behalf. Send sensitive corporate traffic through infrastructure outside Myanmar, and keep as little data in the country as possible. Encrypt what remains, following the detailed guidance in Part 3.

Sources

1. Freedom House. *Myanmar: Freedom on the Net 2025*. November 2025.
<https://freedomhouse.org/country/myanmar/freedom-net/2025>
2. Reuters via Al Jazeera. *Months before the coup, Myanmar army ordered intercept spyware*. 19 May 2021.
<https://www.aljazeera.com/economy/2021/5/19/months-before-the-coup-myanmar-army-ordered-intercept-spyware>



[acquired-spyware-from-cognyte-new-docs-reveal/00000185-b415-d2c1-afe7-fc37abf40000](#)

4. Reuters. *Norway's Telenor says Myanmar unit sale plan followed junta's pressure on surveillance tech*. 15 September 2021.

<https://www.reuters.com/world/norways-telenor-says-myanmar-unit-sale-came-after-juntas-pressure-surveillance-2021-09-15>

5. Justice For Myanmar. *Military-linked company Shwe Byain Phyu has taken control of Telenor Myanmar*. 16 May 2022.

<https://www.justiceformyanmar.org/press-releases/military-linked-company-shwe-byain-phyu-has-taken-control-of-telenor-myanmar>

6. Ooredoo Group. *Ooredoo Group H1 2024*. 30 July 2024.

https://www.ooredoo.com/en/media/news_view/ooredoo-group-h1-2024

7. ARTICLE 19. *Engaging Tech for Internet Freedom: Myanmar*. September 2024.

<https://www.article19.org/wp-content/uploads/2024/09/ETIF-Myanmar-0924.pdf>

8. Justice For Myanmar. *Silk Road of Surveillance: The role of China's Geedje Networks and Myanmar telecommunications operators in the junta's digital terror campaign*. 9 September 2025.

<https://jfm-files.s3.us-east-2.amazonaws.com/public/Silk+Road+of+Surveillance+EN.pdf>

9. InterSecLab. *The Internet Coup: A Technical Analysis on How a Chinese Company is Exporting The Great Firewall to Autocratic Regimes*. 9 September 2025.

<https://interseclab.org/research/the-internet-coup/>

10. Human Rights Watch. *Myanmar: Facial Recognition System Threatens Rights*. 12 March 2021.

<https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights>

11. SEARCH. *The Security Systems Watching You*. 13 September 2026.

<https://www.search-risk.com/insights/security-systems-watching-you>

12. Reuters. *Exclusive: Myanmar's junta rolls out Chinese camera surveillance systems in more cities*. 10 July 2022.

<https://www.reuters.com/world/asia-pacific/exclusive-myanmars-junta-rolls-out-chinese-camera-surveillance-systems-more-2022-07-10/>

13. EngageMedia and Myanmar Internet Project. *Myanmar Digital Coup Quarterly: May 2026 to July 2026*. 18 August 2026.

<https://www.engagemedia.org/2026/myanmar-digital-coup-quarterly-may-2026-july-2026/>

14. The Irrawaddy. *Regime Launches Committee to Monitor Myanmar's Internet 24/7*. 30 June 2026.

<https://www.irrawaddy.com/news/burma/regime-launches-committee-to-monitor-myanmars-internet-24-7.html>



16. Tilleke & Gibbins. *Myanmar Cybersecurity Law Takes Effect*. 1 August 2025.
<https://www.tilleke.com/insights/myanmar-cybersecurity-law-takes-effect/>
17. Baker McKenzie. *Myanmar: Cybersecurity Law enacted on 1 January 2025*. 28 March 2025.
<https://connectontech.bakermckenzie.com/myanmar-cybersecurity-law-enacted-on-1-january-2025/>
18. Hogan Lovells. *Myanmar's Cybersecurity Law Comes into Effect: Key implications for international stakeholders*. 7 August 2025.
<https://www.hlc.com/en/publications/myanmars-cybersecurity-law-comes-into-effect-key-implications-for-international-stakeholders>
19. Human Rights Watch. *Myanmar: Post-Coup Legal Changes Erode Human Rights*. 2 March 2021.
<https://www.hrw.org/news/2021/03/02/myanmar-post-coup-legal-changes-erode-human-rights>
20. Anadolu Agency. *Myanmar passes anti-online scam law with death penalty, rapid bank freezes*. 29 July 2026.
<https://www.aa.com.tr/en/asia-pacific/myanmar-passes-anti-online-scam-law-with-death-penalty-rapid-bank-freezes/4012400>
21. EngageMedia and Myanmar Internet Project. *Myanmar Digital Coup Quarterly: February 2026 to April 2026*. 28 May 2026.
<https://engagemedia.org/2026/myanmar-digital-coup-quarterly-february-2026-april-2026/>

Other Insights

Myanmar risk, updated daily.



[See more Insights](#)

Let's talk



Organization *

Company / Agency

Your role e.g.

Country Director

Enquiry type

Select — AEGIS demo / Travel / Physical / DD / Media / Other

Message *

Briefly describe what you're working on. Please do not include sensitive operational details — we'll share a secure channel on response.

☐ I consent to the processing of my personal data for the purpose of responding to my enquiry, in accordance with applicable data protection laws

Submit



Navigation

[About](#)

[Services](#)

[AEGIS](#)

[Insights](#)

[Privacy Policy](#)

Operational Base

Yangon, Myanmar

Registered Office

Tampa, Florida, USA

General Enquiries

info@search-risk.com

AEGIS Enquiries

aegis@search-risk.com

Uncompromising integrity.

© 2026 South East Asia Risk & Research Consulting LLC

info@search-risk.com | [search-risk.com](https://www.search-risk.com)

