5.0 Myanmar Cyber Security Law

On 1 January 2025, Myanmar Cyber Security Law (No. 1/2025-"Law") enacted by Myanmar's State Administration Council, regulates the digital platforms or space including digital communications and protects critical information infrastructures that seek to support the development of the digital economy based on secure cyber resources. The law comprises 16 chapters and 88 sections; this law marks a significant step toward ensuring national security and fostering a resilient digital economy. The Law has yet to come into effect. Its effective date will be announced in a notification by a Presidential proclamation. The legislation is designed to safeguard the secure use of cyber resources, protect national sovereignty from cyber-attacks, support the development of cyber security services, and promote a thriving digital economy. It also introduces mechanisms for investigating and prosecuting cybercrimes while ensuring accountability across the digital ecosystem.

5.1 Overview

The Law states its objectives as the following:

• Ensuring the safe and secure use of cyber resources, critical information infrastructures ("CII"), and electronic information;

• Protecting and safeguarding the sovereignty and stability of the State from cyber security threats, cyber-attacks, or cyber abuse using electronic technologies;

• Systematically developing cyber security services; • Effectively investigating and prosecuting cybercrimes; and

• Supporting a digital economy based on cyber resources.

"Cyber security" is defined as the protection of information, cyber resources or electronic information from unauthorized access, disclosure, transmission, distribution, use, interference, modification or destruction, or of critical information infrastructure from unauthorized use, disruption, modification, destruction, and attempts to do so. The Law has extraterritorial reach, providing

that any Myanmar citizen residing abroad who commits an offence under the Law remains within its remit and will be subject to the penalties set out therein.

A Cyber security Central Committee ("CCC") will be established to implement the Law's stated objectives. The CCC will further establish a Steering Committee which will in turn assign tasks and responsibilities to relevant Ministries.

5.2 Critical Information Infrastructures (CII)

The Law defines CII as electronic information infrastructures relating to national defense and security, the electronic government service system, finance, transportation, telecommunications, health, electricity and energy, and other such infrastructure as may be determined by the CCC. "Electronic information" is defined as information created, transmitted, received or stored with electronic technology, including fax and e-mail, electromagnetic wave technology or any other technology.

The CCC shall direct the relevant government departments to develop cyber security plans for CII, establish cyber security incident response teams, appoint a person to be responsible for the management and maintenance of CII, and submit a cyber-security report to the Steering Committee established by the CCC on an annual basis.

5.3 Licensing and Registration of Cyber Security Services

The Law provides for licensing and registration for cyber security service providers and digital platform service providers as set out below.

The Law defines "cyber security services" as services using cyber resources or similar technology and related equipment or other services determined by the relevant Ministry. Persons or organisations providing cyber security services are required to be licensed as a cyber-security service provider. To be eligible to provide cyber security services, a provider must be a company registered in accordance with the Myanmar Companies Law ("MCL").

In Section 19, it specifies that licenses can range from three to ten years. Section 20 requires cyber security service providers to register under the Myanmar Companies Act and apply to the relevant department for a business license. Section

22 further mandates that providers seeking to continue operations must apply for license renewal at least six months before expiration.

Similarly, the Law defines “digital platform services” as services that enable its users to display, transmit, distribute or use information online using cyber resources or similar technology and related equipment. In Section 24, it requires digital platform providers with over 100,000 users in Myanmar must register under the Myanmar Companies Law and obtain the necessary approval.

The license and registration for providers of both cyber security and digital platform services will be valid for a minimum of three years to a maximum of 10 years. Both types of providers must apply for a renewal of their license or registration six months prior to the expiration of the license or registration period in Section 26.

Penalties for Licensing and Registration:

- Section 62 states that providing cyber security services without a license can result in imprisonment for one to six months, fines ranging from one to ten million kyats, or both. Companies found guilty face a minimum fine of MMK ten million kyats

- Section 63 imposes fines of up to MMK five million kyats for continuing operations without renewing a license.

- Section 64 prescribes fines of at least 100 million kyats for unregistered digital platform providers with over 100,000 users.

- Section 65 imposes fines starting at MMK 50 million kyats for failing to renew registration.

5.4 Digital Platform Service Providers

The Law states that digital platform service providers are required to have adequate measures in place to identify relevant information and cyber resources in the event of certain circumstances, including where information on their service “disrupts unity”, is “false news”, or is information not suitable for public viewing.

• Section 31 mandates that platforms implement measures to identify and address harmful content, including fake news, child exploitation materials, incitement to violence, and activities that violate existing laws. Platforms must also manage complaints related to copyright infringement or content intended to cause social or economic harm.

• Section 33 requires digital platform providers to retain user information, including personal data and usage records, for three years.

• Section 34 allows authorized entities to access this information upon written request, ensuring compliance with legal investigations and regulatory frameworks.

5.5 VPN Service Providers

The Law defines virtual private networks ("VPNs") as a system that is set up as a separate network within the original network using specific technology to ensure security when connecting to a network.

• Section 44 of the law regulates VPN services, mandating that anyone wishing to establish or provide VPN services within Myanmar must first obtain approval from the Ministry. VPN service providers must obtain permission to establish a VPN or provide VPN services within the national cyberspace.

Penalties for VPN Service Providers:

• Section 70: Unauthorized VPN operations are penalized with imprisonment of one to six months or fines of MMK one to ten million kyats.

• If an individual: Imprisonment for a term of not less than one month and not more than six months, or a fine of not less than MMK 1,000,000 and not more than MMK 10,000,000, or both. The evidence relating to the case shall be confiscated as property of the State;

• If a company or organization: A fine of not less than MMK 10,000,000. The evidence relating to the case shall be confiscated as property of the State.

This provision aims to prevent the misuse of VPNs for illegal activities or circumventing cyber security measures, ensuring secure and lawful internet usage.

5.6 Seizing of Cyber Resources

The Law allows for the seizure and analysis in a digital laboratory of cyber resources from individuals who are believed to be implicated in any cyber security threat, cyber-attack or cyber abuse incident. It is noted that support will be provided as necessary to companies and organization providing telecommunications services according to the Telecommunications Law for conducting data analyses and dispatches to a digital laboratory for examination. A digital laboratory is a technology-assisted laboratory that can identify, retrieve, process, analyse and report data stored electronically.

The relevant Ministry is further empowered to temporarily suspend digital platform services or electronic information, temporarily control materials relating to digital platform services and close digital platform services or declare them unfit for public use.

5.7 Offenses and Penalties

The Law sets out penalties for unsolicited communications, cyber misuse, online theft or mischief, and unapproved online gambling. The penalties for these offences range from imprisonment (the maximum stipulated is for a term of seven years for online theft or mischief) and fines (the maximum prescribed is MMK 20 million).

With regard to unapproved online gambling, the Law provides that if the offender is a corporation or organisation, the minimum fine is MMK 20 million and the illicit proceeds will also be confiscated. The Law does not specify how online gambling platforms can obtain official approval. • Section 71 outlines penalties for unlicensed online gambling, including imprisonment for six months to one year or fines ranging from MMK five to twenty million kyats.

5.8 Summary of Myanmar Cyber Security Law

The Cyber Security Law establishes a structured and transparent approach to securing Myanmar’s digital environment. Through its emphasis on licensing, data retention, and clear obligations for service providers, it fosters accountability and trust in the nation’s cyber infrastructure. The framework supports the country’s vision for a secure digital economy while enhancing its readiness to address the challenges of the digital era. The Cyber Security Law 2025 represents a pivotal

advancement in Myanmar's digital governance. By regulating cyber security services, safeguarding critical infrastructures, and promoting responsible online practices, the law sets the foundation for a secure and dynamic digital future. Its comprehensive approach ensures that Myanmar is well-positioned to thrive in an increasingly interconnected world.