The Republic of the Union of Myanmar

State Administration Council

Cyber Security Law (DRAFT)[1]

State Administration Council Law No.—/ 2022

Myanmar Year 1382, xxx Month, xxx Day

(2022/ xxx Month/Day)

In accordance with article 419 of the Constitution of the Republic of the Union of Myanmar, the State Administration Council enacts this law.

CHAPTER (1) Name and Relations

1. This Law shall be called "Cyber security law".

2. Provisions in this law shall relate to the following matters.

(a) Offences committed by – anyone residing in the country or vehicles and aircrafts registered in accord with any existing law; or a Myanmar citizen: or a foreigner temporarily or permanently residing in Myanmar; or offences committed locally and internationally.

[(b) deleted: "Arrangements, agreements, contracts and covenants made for local and outbound communications; matters related to economy or specific type of electronic information including exchange or storage of information."]

(b) Any matters of communications made with anyone either directly or indirectly with regards to the cyber resource within the national cyber space; or between national and other cyber spaces.

CHAPTER (2) Meaning

3. The following expressions contained in this law shall have the following meanings:

(a) State means the Republic of the Union of Myanmar.

[1] This document is based upon an anonymous unofficial translation received. The translation has been edited and some parts changed to remove errors or clarify meaning.

[(b) deleted: "'State Administration Council' means a national administration council formed under order 9/2021 by the Office of Commander-in-Chief, in accord with Article 419 of the Constitution of the Republic of the Union of Myanmar."]

(b) Central Committee means a Central Committee on cyber security formed by the Union Government.

(c) Steering Committee means a steering Committee on cyber security formed by the Central Committee.

(d) The Ministry means the Ministry of Transport and Communication.

(e) Relevant Ministry and Organisations mean the Ministry of Defense and Ministry of Home Affairs. That word also includes departments or union ministries that are regarded by the Union Government to be related to any issues of cyber security.

(f) Department means the Information Technology and Cyber Security Department.

(g) Investigation Unit means a task force for conducting investigation established by Steering Committee with the approval of the Central Committee.

(h) Cyber Security means the prevention of any actions that includes destroying, disclosing, accessing, sending, distributing, using, transforming and impeding information, cyber resource, electronic information, the critical information infrastructures without approval or agreement.

(i) Information means Data, Text, Image, Voice, Video, Code, Software, Application and Databases;

(j) Cyber source means a computer, computer system, computer program or program, network, communication equipment and information. It also includes any other technology and associated devices that are upgraded or advanced based on them.

(k) Electronic information means information created or sent or received or stored by digital electronic technology or electromagnetic wave technology or any other specific technology.

(l) Critical Information Infrastructure means fundamental infrastructures that are described in Article 14. That word also includes any matter declared as 'Critical Information Infrastructure' by the Union Government or the Central Committee or the Ministry.

(m) Data means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed or has been processed in a computer or computer network and it may be, in any form, stored internally in the memory of the computer.

(n) Personal information means any information which has been verified or verified about a person;

(o) Person responsible for maintaining personal information means the person assigned by the government department or the organisation authorised to administer personal information under the existing law or in accordance with the provisions of this Law

(p) Administration means the collection, receiving, transferring, distribution, coordination, prohibition, destruction, recording, maintenance, storing, changing, retrieval of stored data, suggestions, utilisation or disclosures of personal information.

(q) Administrator of Critical Information Infrastructure means a person implementing matters related to the critical information infrastructure.

(r) Electronic or Digital Signature means any symbol or mark arranged personally or on his behalf by electronic technology or any other similar technologies to verify the authenticity of the source of the electronic record and the absence of amendment or substitution.

New (s) Electronic record means a record generated, sent, received or stored by means of electronic, magnetic, optical or any other similar technologies in an information system or for transmission from one information system to another;

(t) Electronics or Digital Certificate are electronic credentials issued to a subscriber by the Electronics or Digital certification authority identifying the relationship between the electronic signature and the electronic data message;

(u) Electronic or Digital Certification Authority means an authorised person to validate the authenticity and integrity of an electronic or digital certificate.

New (v) Subscriber means a person who is by any technologies identified as an authentic signer of an electronic signature in the electronic or digital certificate;

(w) Original Sender means a person by whom or on whose behalf the information purports to have been created, generated or sent. This expression does not include a person acting as an intermediary with respect to electronic information;

(x) Addressee means a person who is intended by the original sender to receive the electronic information. This expression does not include a person acting as an intermediary with respect to electronic information;

[(t) deleted: "'Online service' means any business served via online by using a system similar to the cyber source or materials."]

New (y) Digital Platform Service means any over the top (OTT) service that can provide the service to express data, information, images, voices, texts and video online by using cyber resources and similar systems or materials.

Explanation- Over the top (OTT) means providing services using cyber resources and similar systems rather than the traditional way.

New (z) Digital Platform Service Provider means any individual or any entity providing digital platform service in Myanmar. Apart from Articles 58 and 62, that word does not include companies and organisations that hold telecommunication service licences under the telecommunication law.

(aa) Cyber Security Provider means any individual or entity who is providing any cyber security services by using cyber sources or similar systems or materials with regard to the information technology system.

(bb)Computer means a device capable of receiving, transmitting, storing, processing or retrieving information and records, using arithmetic and logical means by manipulation of electronic, magnetic, optical or any other similar technologies;

(cc) Computer Programme or Programme means a set of instructions a computer follows in order to perform a task;

(dd)Computer System means either any device that can automatically process data by using a program or any set of devices that are integrated or contain connected parts. This expression shall also include any removable storage medium used in computer operation; and any computer program or information stored in this device of a computer system.

(ee)Communication Device means interconnected devices by any technology, their infrastructure, related parts and any telecommunication equipment specified by the Ministry.

(ff) Network means a telecommunication system of interconnection between a communication device, computer or computer-like devices and other related system and devices through the use of cable or wireless or satellite or by any other technologies;

(gg) Access means accessing a specific cyber source either whole or partially.

(hh) Hacking means wholly or partially obtaining data or information communicated by using a network.

(ii) Malware means a malicious code that disrupts or endangers a cyber source.

[(hh) deleted: "'Cyber security' means prevention of obtaining, disclosure, sending, disseminating, usage, interfering, changing or destruction of data, cyber source, electronic information and critical information infrastructures without permission."]

(jj) Cyber Space means an environment in which electronic information can be sent, communicated, distributed and received reciprocally within a network or by connecting networks with the use of cyber source;

(kk) National Cyber Space means cyberspace determined by the central committee or steering committee.

(ll) Cyber Crime means a violation or attempting or encouraging a violation of any prohibition contained in this law or any other existing laws on cyberspace by using any cyber source.

(mm) Information and Communication means utilisation of any online communication including e-government infrastructure, e-commerce infrastructure, forum, blog and social media network within cyberspace or national cyberspace by means of a specific cyber source or internet of Things (IoT) as Information Communication Technology (ICT) either by an individual or an organisation;

New (nn) Cyber fraud means an individual or group or organisation violates any actions described in Chapter (11).

(oo) Cyber-attack means violation of, an attempt, abetment, motivation or acting as a conspirator to violate an attack that targets the executive, finance, economy, rule of law, national security or public safety and property or disrupts and halts the information communication by using a cyber source within cyberspace;

(pp) Member state means any country from international or regional organisations in which the State is a member or ratified to conventions, covenants or agreements related to prevention and coordination of cyber security or cyber-crimes.

(qq) Online Gambling means gambling by using any cyber source to organise luck draws or play a game with or without tolls, that involves an element of skill with the intent of winning money or any property which has money-alike worthiness, or which is agreed to be exchanged into money.

New (rr) Online Financial Service means any financial service transaction such as online payments and online money transfer by using cyber source.

New (ss) Data Classification means the level of security classified in accordance with rules and regulations based on the degree of data importance.

New (tt) Licence means a business licence issued by individuals, departments, or organisations in accordance with this law.

CHAPTER (3) Objectives

4. This law shall serve the following objectives:

(a) To be able to safely and securely use cyber sources, critical information infrastructure and data stored

with electronic technology.

(b) To be able to protect the personal information of the public in accordance with the law

(c) To be able to safeguard and protect from harassing, cyber-attacking and cyber-fraud by using electronic technology to harm the national sovereignty, peace and stability.

(d) To be able to supervise in ensuring that cyber security services are systematically implemented in accord with the law.

(e) To prevent cyber-crimes.

(f) To support the digital economy.

(g) To recognise and legally protect the authenticity and integrity of electronic information in conducting local and international communications using cyber sources.

CHAPTER (4) Formation of Cyber Security Central Committee

5. The Union Government shall

(a) the Cyber Security Central Committee shall be established with the following persons to supervise cyber security matters.

(1) Deputy-Prime Minister of Union Government _ President

(2) Union Minister _ Vice President

(3) Union Minister/Chairmen / Relevant Ministry and Organisations _ Member

(4) A person assigned by the Union Government Secretary

(b) The Central Committee formed under subsection (a) may be reorganised as necessary.

6. The responsibilities of the Central Committee are as followed -

(a) Set policies, strategies and action plans related to cyber security for the development of a good and safe national cyberspace;

(b) Implement cyber security-related policies, strategies and programs and supervise and coordinate to be able to cooperate with foreign countries and international and regional organisations.

(c) Promote the training and development of human resources for the development of cyber

security-related matters.

(d) Promote the development of infrastructures that are necessary for cyber security and the prevention of cyber-crime.

(e) Coordinate and direct among relevant government departments, government organisations and other organisations to ensure the betterment of cyber security; prevent cyber-crimes and support rule of law and judiciary sector.

(f) Instruct relevant ministries to prepare the cyber security plans for the critical information infrastructures.

New (g) Direct to implement necessary policies and systems for the recognition of the authenticity and integrity of electronic information in local and foreign communication by using cyber sources.

(h) Instruct local and international cyber security service providers to coordinate in accordance with the cyber security plans for the critical information infrastructure.

(i) To achieve the objectives of this law, determine the information storage of online communication operators in which the public engages through national cyberspace.

New (j) Permit to establish a national digital laboratory and digital laboratories in accordance

New (k) Announce necessary policy, rules, regulations and directives for online financial services by coordinating and collaborating with the Central Bank of Myanmar.

(l) Execute duties and tasks assigned by the Union Government from time to time.

CHAPTER (5) Formation of Cyber Security Steering Committee and its Responsibilities

7. With the approval of the Union Government, the Central Committee shall form the Cyber Security Steering Committee with the following members:

(a) Union Minister, Ministry _ Chair

(b) Deputy minister/vice-chair / permanent secretary/Relevant Ministries _ Members

(c) Cyber security professionals _ Members

(d) Representatives from Non-governmental organisations _ Members

(e) Director-General/Department _ Secretary

8. The duties and responsibilities of the Steering Committee are as follows:

(a) Coordinates activities to identify, prevent cyber-crimes and cyber security

(b) Implements the cyber security policy, strategies, action plans, information infrastructure and training and development of human resources as laid down by the central committee to better develop cyber security, cyber-crimes prevention and identification matters

(c) Prepares in-time response systems if there are any cyber attacks.

(d) Coordinates with other relevant ministries to ensure national cyber security

(e) Observes and reports to the central committee in accordance with provisions of the cyber security and cyber-crimes related conventions, treaties and agreements so that the state can be a member state.

(f) Implements and cooperates in accordance with the provisions of the cyber security and cyber-crimes related conventions, treaties, and agreements that the state is a member of international

(g) Forms required working groups and assign their responsibilities, with the approval of the central committee, to perform cyber security activities

(h) Announce, inform and present news and recommendations to the general public with regard to cyber security, cyber terrorism and cyber threats

(i) Educates and implements training on cyber security

(j) Supervises the emergency response teams for cyber security breaches in every sector

(k) Appraises and approves the services mentioned in this law in accordance with policy, strategy, action plan and frameworks with regard to the permits, rejects and take action of the service licenses

New (l) Implement in accordance with the policy to acknowledge the integrity and reliability of the electronic information in communications of domestic and international.

(m) Present the progress reports and other necessary reports to the central committee

(n) Implement cyber security duties assigned by the central committee as relevant

(o) Cooperates with neighbouring countries, regional organisations, international organisations with regards to information sharing, investigation, sanctioning, cooperation and scrutiny on cyber security, cyber-attack, cyber threat or cyber crimes

(p) Scrutinises and permits cyber security teams or organisations, sanction on unauthorised cyber security teams or organisations

(q) Implements the regulation to collect information on businesses from the online communication

sector

(r) Scrutinises and approve local-made or imported information technology equipment and devices to ensure they are in line with cyber security policy and standards

9. With the approval of the central committee, the Steering Committee shall form the following working committee to implement the objectives of this law:

(a) Cyber Security Working Committee

(b) Cyber-Crimes Working Committee

(c) Cyber Protection Working Committee

(d) Electronic Communication Supervision Working Committee

(e) Other necessary Working Committees

10. Steering Committee shall form an investigation team with the approval of the central committee if the works outlined in this law require an investigation.

CHAPTER (6) Protection of Personal Information

11. The person responsible for managing and keeping the personal information shall —

(a) systematically keep, protect and manage the personal information based on its types, security levels in accordance with the law

(b) not allow, disclose, inform, distribute, dispatch, modify, destroy, copy and submit as evidence of the personal information of an individual without the consent or the permission in the provision of an existing law to any individual or organisation.

(c) not utilise personal information for managing issues that are not in compliance with the objectives

(d) systematically destroy the personal information that is collected to be used for a period of time after a certain period

12. The investigation team who receives information that includes personal information or the person mandated or instructed on their behalf shall keep the information confidential except disclosing the information in hand in accordance with the law.

13. Personal Information Management shall not include the followings:

(a) prevention, search and enquiry, investigation, submission of evidence in a court by the government

agency, investigation team or rule of law team assigned by the government for cyber security, cyber-attacks, cyber terrorism, cyber misuse and cyber accident, cyber-crimes

(b) search and enquiry, investigation, data collection, prosecution and submission of evidence in a court by the government agency, investigation team or rule of law team mandated to work on criminal issues

(c) enquiry, investigation, data collection and info-sharing and coordination carried out if the cyber security and cyber-crimes issues are of concern to the state sovereignty, stability, national security

(d) when carrying out activities in subsection (c), either the central committee or relevant ministry or department has separate authority and working on it in accordance with those definitions.

CHAPTER (7) Protection of the Critical information infrastructure

14. The important information infrastructures are as follows;

(a) Electronic Government Services

(b) electronic information and infrastructure on finance and budgeting

(c) electronic information and infrastructure on water resources

(d) electronic information and infrastructure on transportation

(e) electronic information and infrastructure on communication

(f) electronic information and infrastructure on public health

(g) electronic information and infrastructure on electricity and energy

(h) electronic information and infrastructure on natural resources

(i) electronic information and infrastructure classified for private use only.

15. The Central committees shall;

(a) Redefine the critical information infrastructure with the approval of the State Administration Council as necessary.

(b) Instruct the ministry to inform the process of identifying and redefining the critical information infrastructure on the specific sectors to the official responsible for managing and maintaining critical information infrastructure.

(c) Set up policies to keep, record and maintain the information on the important information

infrastructure.

16. The Steering Committee shall inspect the readiness of cyber security of critical information infrastructure and give instructions to ensure it meets the specified standards.

17. Concerned ministries and government institutions shall perform the followings;

(a) Drafting action plans on cybersecurity for critical information infrastructure;

(b) Establishing emergency response teams for cybersecurity breaches;

(c) Submitting cybersecurity report to the Steering Committee.

18. The official responsible for managing and maintaining the critical information infrastructure shall;

(a) Keep information related to critical information infrastructure in accordance with regulations, depending on the level of information;

(b) follow the regulations in disseminating, producing, transferring, receiving and saving information on important information infrastructure;

(c) submit the cybersecurity report to concerned ministries and organisations at least once a year.

19. Steering committee shall coordinate with the emergency response team with regard to the cyber security breach to implement protections of critical information infrastructure.

CHAPTER (8) Electronic communication

New 20. The Electronic Certification Authority shall:

(a) A reliable system must be used to prevent hacking and abuse of computer hardware and software systems

(b) A standard level of credibility must be set in the service industry that is relevant to the performance of the intended business

(c) Confidentiality of electronic certificates must be conducted in accordance with security measures

(d) The prescribed standards must be followed

(e) The details of the electronic certificate of electronic communication shall be provided

(f) The actual performance in relation to the issuance of the electronic certificate must be stated.

(g) The credibility of the electronic certificate issued and the factors that may affect the accountability or assurance of its service provider must be mentioned

(h) In case of damage due to the circumstances permitted by the electronic certificate or a computer system malfunction

(1) The person who may cause harm must be notified in any way possible

(2) The electronic certificate shall be complied with in accordance with the specific procedures to be followed in practice for the above circumstances and incidents,

(i) Comply with the rules and regulations set by the Electronic Communications Oversight Committee from time to time.

New 21 (a) When submitting a proposal for an investment permit under the Myanmar Investment Law, the holder of the Electronics Certificate is required to apply to the Myanmar Investment Commission together with the license issued by the Electronic Communications Supervision Working Committee.

(b) The Myanmar Investment Commission may, if necessary, seek the opinion of the Electronic Communications Supervision Working Committee in respect of the application under subparagraph (a).

New 22 (a) Those who want to act as a subscriber must apply to the electronic certification authority in accordance with the requirements to obtain the electronic certificate.

(b) The electronic certification authority may, after scrutinising the application under subsection (a), set the criteria and issue or refuse to issue the electronic certificate.

New 23. The subscriber must

(a) When using a valid permanent certificate with information identifying electronic signature, care must be taken not to allow that information to be misused by others.

(b) Care must be taken to ensure that the personal data and additional information are valid and accurate when using the electronic certificate issued as the electronic signature within the permitted period.

(c) If the confidentiality of the information on the electronic signature is leaked or If in a situation where the confidential information may be leaked, Notice must be given to those associated with the electronic signature without delay according to the procedure arranged by the electronic certification authority or with the appropriate arrangement.

New 24. The subscriber shall be liable for the consequences of failure to comply with the provisions of Article 23.

New 25. Matters that are prescribed by the existing law to be written and signed could be done with the electronics records, electronics information and electronic signatures and such acts shall be legally binding as provided by applicable law.

New 26. The original sender and Addressee receive the electronic record; Sending electronic information and electronic certificates; Receipt and storage shall be carried out in accordance with the prescribed procedures. However, if we have a separate agreement with each other, we can act in accordance with those agreed-upon methods.

New 27. If there is no agreement otherwise, parties entering contracts can use electronic technology in offering, accepting offers or other necessary data.

New 28. An electronic record or electronic information shall be deemed as that of the original sender if it is sent either by the original sender himself or by a person authorised to send on behalf of the sender or through an automatic information system arranged by the sender himself or by a person acting on behalf of the sender.

New 29. The Addressee shall be deemed to receive the information or the electronic record or electronic information from the original sender if;

(a) by means agreed between the Addressee and the original sender; or

(b) the Addressee receives from a person related to the original sender or a person authorised to send on behalf of the original sender by means of original agreements.

New 30. During or before sending the electronic records or electronic information, the original sender or the Addressee;

(a) shall be deemed of having received information for any of the following methods:

(1) The Addressee replying himself or by an automated system or by any other means;

(2) The Addressee displays a sufficient demonstration towards the original sender that he or she had received.

(b) can make a separate agreement to acknowledge the receipt.

New 31. The original sender must confirm the receipt of the electronic record or receipt of the electronic information:

(a) If the acknowledgement of receipt has not been received in the prescribed case, it shall be deemed that the original sender has never sent it.

(b) in the case which is not specified, within the period specified separately; If no time is specified, the original sender may notify the recipient that he/she has not received the acknowledgement of receipt,

even within a reasonable time.

New 32. If there is no separate agreement between the original sender and the Addressee of the sending and receiving time, the electronic record or electronic information shall be:

(a) The time of transmission is the time of entry into the information system beyond the control of the original sender or its agent

(b) The time of reception is as follows:

(1) When accessing a designated information system

(2) When the recipient used the non-defined information system

(3) When the recipient enters the information system if there is no specified information system

New 33. Original sender and Addressee:

(a) If there is no separate agreement, the business location of the sender shall be considered as the place of sending. The business location of the Addressee shall also be considered as the place of receipt.

(b) If a business is operated in more than one place, the main business area; If there is no business location, the place of permanent residence of the person; In the case of an organisation, the place of establishment established in accordance with the law shall be considered as a permanent address

CHAPTER (9) Providing Service

34. The cyber security service providers shall perform the following;

(a) planning and implementing cyber security preventing measures to support the Department and Cyber Security Breach Emergency Response teams;

(b) providing warnings on cyber security risks and preventive guidance;

(c) developing response plans and solutions against malicious codes, cyber-attacks, hacking, or other security breaches.

(d) Immediate implementation of appropriate emergency response, response and notification of stakeholders in the event of a cyber security attack;

(e) Applying cyber security technology and required standards

(f) Prevent leaking, damaging or loss of information of service users.

(g) Immediate report to cyber security breach emergency response team and department in case of emergency.

(h) Payment of prescribed license fees

(i) Submission of business report as prescribed

35. Prevention, removal, destruction and cessation shall be made accordingly in a timely manner, following the provision of information by the department that a digital platform service provider in Myanmar causes any of the following on cyberspace;

(a) Speech, texts, image, video, audio files, signs or other ways of expressions causing hate, disrupting unity, stabilisation and peace.

(b) Misinformation and disinformation

(c) Sexually explicit material that is not culturally appropriate for Myanmar society to see; Photos, Audio files, Videos, Texts, Signs, Symbols and other expressions

(d) Child pornography; Photo, Video, Texts, Symbols and other expressions

(e) written and verbal statement breaching any existing law

New (f) A legitimate complaint of the expression, writing, sending, distribution of speech, text, images, video, sound, symbols and other expressions that damage an individual's social standing and livelihood

New 36. A digital platform service provider with more than 100,000 users in Myanmar shall ensure the following;

(a) Devices holding users' data must be stored in line with data classification rules.

(b) Internet Service providers must be registered in accordance with Myanmar company law.

(c) Taxes must be paid in accord with the provisions set forth in relevant laws if iF is due to claim any tax relating to the business conducted through internet service or similar profitable business.

37. A digital platform service provider in Myanmar shall retain the following information from the service users for up to three years from the first date of use of the service;

(a) Username, Internet Protocol (IP) address, telephone number, identification card number and address of the service users.

(b) User record of the service user.

(c) Other information as directed by the Department.

38. A digital platform service provider in Myanmar may provide all or part of the information contained in Article 37 if the assigned person or authorised organisation is requested under any existing law.

CHAPTER (10) Obtaining License

39. Any individual or organisation from local or abroad willing to operate as an authorised electronic certification issuer must apply to the electronic communication supervision working committee in accordance with the requirements for obtaining a license.

New 40. The Electronic Communications Supervision Committee shall scrutinise the application for a license under Article 39 and, with the approval of the Steering Committee, issue a license or refusal to issue a license to the applicant person or organisation subject to conditions.

41. Anyone wishing to operate a cyber security service in Myanmar must apply to the Department in accordance with the requirements for obtaining a business license.

New 42. The Department scrutinizes and issues licenses in accordance with the stipulations in relation to the application for a license. Refusal to issue a license shall be carried out with the approval of the Leading Committee.

New 43. To obtain a license, an individual or entity must renew the license in accordance with the provisions of the Electronic Communications Supervisory Committee or Department.

New 44. The Electronic Communications Supervision Committee or the Department shall, with the approval of the Steering Committee, issue the license or refuse to issue the license in accordance with the stipulations.

45. Anyone willing to operate a digital platform service shall register at the Department in accordance with the relevant procedure.

46. The Department shall review relevant license application and license renewal pursuant to the stipulations; and shall issue the licenses to applying individual or organisation with the approval of the Steering committee.

CHAPTER (11) Cyber Fraud and cyber crime

47. Any of the following acts performed on a particular cyber source by anyone without the owners' permission

shall be deemed unauthorised access to information;

(a) Changing, modifying, or deleting a computer program or a program or data or information and its related status or properties,

(b) Copying, transferring, or relocating a cyber source to one of the followings,

(1) transferring a computer program or a program or data or information from its original place of storage to either another cyber source, or a device, or a storage device;

(2) transferring a computer program or a program or data or information within the same cyber source or a device or a storage device but to a different location in its system;

(3) Using a computer program or a program or data or information;

(4) Obtaining data from a computer system by running a computer system, or by any other means.

48. If any of the following acts relating to a computer system or computer program or a program or a data is performed without permission, it shall be deemed as an illegal modification of a quality of a particular computer system —

(a) Changing any program or data stored by a respective computer system;

(b) Deleting any program or data stored by a respective computer system,

(c) Putting additional information to a program or data stored by a respective

(d) Any action that can interrupt the regular functions of a computer system.

49. The following acts related to a computer system or computer program or a program or a data shall be deemed as controlling;

(a) Controlling any computer or computer system or network, or similar action;

(b) Controlling and executing any computer or computer system or network by another computer system (software/tool).

50. A computer system or a program or data or information shall be deemed as illegal access to a computer system by a person by any means;

(a) If that person is not the authorised one to oversee the Mitigated context which shall be assessed relevant with any computer system;

(b) If that person is not the one who does not have permission from the responsible person to oversee

the litigated context which shall be assessed relevant with any computer system;

51. Intervention made to a computer system or computer program or a program or a data by a person with any of the following methods shall be deemed an illegal intervention.

(a) If the person is not the authorised person for a specific computer system;

(b) If the person is not the authorised one to decide whether to make the aforementioned intervention or not;

(c) If the person is not the one who has permission from a responsible person to make interventions for a specific computer system.

New 52. Performing the provisions of Articles 49, 50 and 51 with the permission of any existing law shall not be deemed to be illegal.

[42. deleted: "Security cameras shall be installed in crowded places, public places, and where necessary for security in accordance with the specified rules and regulations."]

CHAPTER (12) Protecting and Responding Cyber Crimes and Cyber Attacks

53. Cybersecurity Working Committee, Cyber Crime Working Committee, and Cyber Protection Working Committee shall implement the followings regarding any events of cyber security threats, cyber-attacks or cyber fraud;

(a) Accessing potential impacts or impacts of cyber security threats, cyber-attacks or cyber fraud;

(b) Preventing any other consequences of cyber security threats, cyber-attacks or cyber fraud from occurring;

(c) Preventing cyber security threats, cyber-attacks or cyber fraud from occurring;

(d) To increase the levels of cybersecurity, retrieving, storing, transferring, and monitoring the information which is stored, received, sent, or created in a computer or computer system aiming;

(e) Investigating and taking actions against cyber security threats, cyber-attacks or cyber fraud.

54. The digital platform service provider or the cybersecurity service provider shall coordinate and collaborate to implement the activities prescribed in Article 53.

55. Cybersecurity Working Committee, Cyber Crime Working Committee, and Cyber Protection Working Committee, in implementing activities prescribed under Article 53, can inspect the computer or computer system of the following persons who are considered to be related to any security threats,

cyber-attacks or cyber fraud;

(a) The user or the person suspected as the user who uses any computer or any computer system or any network which are considered to have been related to any security threats, cyber-attacks or cyber fraud;

(b) The person who is related with any person mentioned in subsection (a).

56. Cybersecurity Working Committee, Cyber Crime Working Committee, and Cyber Protection Working Committee shall return the computer or computer systems to the provider systematically after assessing, analysing, and investigating that computer or computer systems.

57. The Union Government can grant a relevant person or organisation the authority to intervene, to conduct interventions prescribed under existing laws.

58. The companies and organisations providing services as prescribed in Communication Law shall arrange and prepare for the relevant person or organisation granted with authority in accord with Article 57 to be able to intervene.

59. A relevant person or organisation granted with authority to intervene as per Article 57 shall conduct any of the following interventions without interfering with the fundamental rights of the citizens;

(a) Preventing issues that can harm the sovereignty and territorial integrity of the State;

(b) Performing acts of State Defense and security;

(c) Performing acts of Rule of Law and public order;

(d) Investigating crimes;

(e) Issues permitted in accordance with the existing law;

(f) Acts to safeguard and protect public life, property and public welfare.

60. The ministry or the department or the organisation assigned by the ministry can visit and check and oversee the site of any digital platform service provision business, and can ask to present labels either to serve the purpose of state defence and security or for the public interests.

61. In the event of a need to act for the public interests, the ministry can conduct the following with the approval of the Union Government;

(a) Temporarily prohibiting any digital platform service provision in Myanmar;

(b) Temporarily controlling the devices related to digital platform service provision in Myanmar temporarily;

(c) Permanently ban any of the digital platform service provision businesses in Myanmar.

New 62. Permission from the Ministry must be sought in line with conditions for the use of VPNs & similar tools to set up, access and use networks that are licensed under the Telecom Law.

CHAPTER (13) Seizing Evidentiary Materials and Submitting Expert's Witness

63. The Inspection Body shall if required to seize evidence, handle and seize them pursuant to provisions under this Law and any other existing laws.

64. The Inspection Body can submit to the court the evidential materials in electric or digital form pursuant to the stipulations after assessing, analysing and studying them.

65. The National Digital Forensic Lab and the Digital Forensic Lab will be established in order that the central committee, the respective working committees and respective departments could implement their duties, and expert witnesses can be submitted to the court in the form of digital evidential materials pursuant to the stipulations.

New 66. If the evidence relating to prosecuting an offence filed under this law is not easy to bring to court, it can be presented with a report or other relevant documentation on how the evidence is kept without going to court. Such submission shall be deemed to have been presented as evidence before the court and may be administered by the relevant court in accordance with the law.

New 67. In the event of any dispute regarding the submission of electronic evidence, it shall be submitted to the National Digital Laboratory for examination. The findings and opinions of the National Digital Laboratory are final.

CHAPTER (14) Online Gambling

68. Regarding online gambling, no one shall, without permission:

(a) claim or collect stakes for gambling;

(b) gamble, encourage or assist someone to gamble, gather or solicit people to gamble.

CHAPTER (15) Administrative Actions

New 69. If the subscriber violates any of the terms of the electronic certificate; If a person is found guilty of

violating any of the provisions of this Act, the person authorised to issue the electronic certificate may issue an administrative order to the person:

(a) Suspension of the certificate for a limited period

(b) Cancellation of the certificate

New 70. If the person authorised to issue the electronic certificate violates any of the license terms; If he is convicted of violating any of the provisions of this Law, the Electronic Communications Regulatory Committee may issue such administrative order to the person:

(a) Applying the prescribed fine

(b) Suspension of license for a limited period

(c) Revocation of license

New 71. The operator of the digital platform service is subject to Article 35; In case of failure to comply with the provisions of Articles 36 and 54, the Department may, with the approval of the Steering Committee, impose any administrative action as follows:

(a) Warning

(b) imposing a fine

(c) Suspension of service in Myanmar for a limited period or suspension of the license for a limited period.

(d) Prohibition or revocation of license in Myanmar

72. If the cyber security service provider fails to comply with the provisions of Articles 34 and 54, the Department may, with the approval of the Steering Committee, impose any administrative action as follows:

(a) Warning

(b) imposing a fine

(c) Suspension of service in Myanmar for a limited period or suspension of the license for a limited period.

(d) Prohibition or revocation of license in Myanmar

73. A company that provides services under the Telecommunications Law; If the organisations fail to comply with the provisions of Article 58, the Department may, with the approval of the Steering Committee,

take the following administrative action:

(a) Warning

(b) imposing a fine

(c) Suspension of service in Myanmar for a limited period or suspension of the license for a limited period.

(d) Prohibition or revocation of license in Myanmar

New 74. The Steering Committee may dissolve any cyber security body or organisation that has not been properly formed.

CHAPTER (16) Appeal

75. (a) if the person authorised to issue the electronic certificate refuses to issue the electronic certificate; A dissatisfied tenant may appeal to the Electronic Communications Supervision Committee within 30 days from the date of the order or decision, even if an administrative order is made under Article 69.

(b) With respect to the appeal filed under subsection (a), the Electronic Communications Oversight Working Committee may, with the approval of the Leading Committee, approve or amend the order or decision issued by the person authorised to issue the electronic certificate.

(c) The order or decision made under subsection (b) of the Electronic Communications Supervision Committee is final.

New 76. If the Electronic Communications Supervision Committee refuses to issue the license or refuses to renew the license or makes a management order under Article 70, the person who is dissatisfied with the issuance of the electronic certificate may appeal to the Central Committee within 60 days from the date of the order or decision.

New 77. If the Leading Committee refuses to issue the license or refuses to renew the license or refuses to register or refuses to renew the registration, Article 71; A person dissatisfied with any of the administrative penalties imposed under Articles 72 and 73 may appeal to the Central Committee within 60 days from the date of the decision or order.

78. The Central Committee may approve or amend the appeal under Articles 76 and 77. The decision of the Central Committee is final.

CHAPTER (17) Offences and Penalties

79. If a person responsible to manage personal data is convicted of failure to manage personal data in with Articles 11 and 12, he or she shall be punishable by imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs kyats or both.

80. Any person, if convicted personal data of a person to another without approval, shall be punishable by imprisonment for a term not exceeding 3 years or a fine not exceeding 50 lakhs kyats or both.

81. If a person responsible to manage critical information infrastructure is convicted of failure to perform his or her duties under Article 10 subheading (b), he or she shall be punishable by imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs kyats or both.

82. Any person who is convicted of interfering, destroying, stealing, harming, illegally sending, modifying or changing electronic information, shall be punishable by imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs kyats or both.

83. Any person who is convicted of interrupting a communication within a network or using data contained in a communication or disclosing data to another person, without the approvals from the original sender and Addressee, shall be punishable by imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs kyats or both.

New 84. If a person is convicted of using a password or electronic signature of someone, without consent or agreement, directly or indirectly to communicate with another person, the person shall be punished with imprisonment for a minimum of one year and a maximum of three years or a fine not exceeding 100 lakhs kyats or both.

New 85. Anyone applying for a certificate If convicted of misrepresenting his identity or license to the person issuing the certificate, either for the purpose of suspending or revoking the certificate, he shall be punished with imprisonment for a minimum of one month and a maximum of six months or a fine not exceeding 50 lakhs kyats or both.

86. If the operator of the digital platform service is found guilty of failing to comply with the provisions of Articles 36 and 37, he shall be punished with imprisonment for a minimum of one year and a maximum of three years or with a fine not exceeding 100 lakhs kyats or both.

New 87. Whoever is convicted of violating the provisions of Articles 47 and 48 shall be punished with imprisonment for a minimum of six months and a maximum of two years or a fine not exceeding 100 lakhs or both.

New 88. Whoever violates Articles 49, 50 and 51, shall be punished with imprisonment for a minimum of one year and a maximum of three years or a fine not exceeding one hundred thousand kyats or both.

89. Any person who commits any of the following acts in bad faith or dishonesty shall be punishable by imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.

(a) Infecting a cyber source with or inserting malware and other elements that can compromise computer functions;

(b) Preventing access of any authorised person to access a cyber source;

(c) Encouraging or assisting access to cyber sources in violation of the regulations prescribed by the law;

(d) Interfering a person by using a cyber source of another person by paying or in any other ways;

(e) Destroying, removing or modifying information in a cyber source; or compromising its usefulness or effects for any reasons;

(f) Stealing, preventing the ability to use, destroying or modifying the source codes from a computer with an intent to destroy it (or) asking someone to do so;

(g) Deceiving through the use of cyber sources;

New (h) Stealing or damaging any money transfer or financial asset made by an online service of a person or organisation using cyber resources.

New 90. No one shall have access to a network using Virtual Private Network (VPN) technology or similar technology on a network licensed under the Telecommunications Law without the permission of the Ministry. If convicted of using the offence, the person shall be punished by imprisonment for a minimum of one year and a maximum of three years or with a fine not exceeding 50 lakhs kyats or both.

91. Any person who is convicted of creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on cyberspace, shall be punished by imprisonment for a minimum of one year and a maximum of three years or with a fine not exceeding 50 lakhs kyats or both.

[65. deleted: "Any person who is convicted of creating a fake account, website and web portal with the intent of causing public panic, loss of trust or social division on a cyberspace, shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both."]

92. Any person who is convicted of cyber violence acts such as preventing or making it difficult to access cyber sources; attempting to hack into a cyber source without permission; using more than permitted; and inserting or installing dangerous malware with the intent to hurt someone; with an intent to threaten or disturb national sovereignty, security, peace and stability, rule of law and national solidarity, shall be punished with imprisonment for a minimum of two years and a maximum of five years or with a fine not exceeding 300 lakhs kyats or both.

93. Any person who commits acts of cyber-attack such as attempts of unauthorised access to and hacking cyber

sources which are kept confidential for nationally, internationally or multilaterally implemented security reasons; and using more than permitted; with the intent of deteriorating the relationship between the country and other foreign countries or for the interests of another foreign country, shall be punished with imprisonment for a minimum of three years and a maximum of seven years or with a fine not exceeding 500 lakhs kyats or both.

94. Any person who is convicted of providing online financial service without being legally registered in Myanmar nor without permission from the Central Bank of Myanmar shall be punished by imprisonment for a minimum of one year and a maximum of three years or with a fine not exceeding 100 lakhs kyats or both.

95. Any person who is convicted of buying and selling illegal currency such as digital currency, cryptocurrency on cyberspace shall be punished by imprisonment for a minimum of six months and a maximum of one year or with a fine not exceeding 25 lakhs kyats or both.

96. Any person who is convicted of electronically sharing sexually explicit speech, image, audio file, video, sentence, sign, symbol and other expressions shall be punished by imprisonment for a minimum of one year and a maximum of two years or with a fine not exceeding 50 lakhs kyats or both.

[69. deleted: "Any person who is convicted of creating, collecting, searching, downloading, announcing, promoting, changing or disseminating obscene, inappropriate and explicit child image, audio file, video, words, sign, symbol and other expressions for sexual purposes shall be charged in accord with the Child Rights Law."]

97. Whoever is convicted of soliciting bets for online gambling without permission shall be punished by imprisonment for a minimum of one year and a maximum of three years or with a fine not exceeding 100 lakhs kyats or both.

98. Whoever is convicted of committing any form of online gambling without permission shall be punished by imprisonment for a minimum of six months and a maximum of one year or with a fine not exceeding 50 lakhs kyats or both.

New 99. Whoever obstructs or prevents or injures the Leading Committee and its assigned working committee or Commission or person, which is carrying out its duties in accordance with this Law, or failing to comply or request to comply with this law shall be punished by imprisonment for a minimum of six months and a maximum of one year or with a fine not exceeding 50 lakhs kyats or both.

100. Anyone who is convicted of violating the prohibitions prescribed under the rules, regulations, notifications, orders, instructions, and procedures of this law shall be punished by imprisonment for a minimum of six months and a maximum of one year or with a fine not exceeding 25 lakhs kyats or both.

101. Anyone who attempts or conspires or abets any offences provided by this law shall be liable to punishments provided by this law.

CHAPTER (18) Miscellaneous

[78. deleted: Existing and ongoing Electronic Identification Permit License (Digital Signature) Services, Online Services and Cyber Security related Services before the enforcement of this law shall register and apply for the license in accordance with this law within one year from the date this law was enacted.]

[79. deleted: Matters not in compliance with the provision of this law are to be adjusted for public interest and to be in compliance with the provisions in this law, necessary adjustments are to be completed in the said period mentioned in Article 78.]

102. Announcements, Orders and Directives issued relating to telecommunication or electronic communication before the enactment of this law shall be applicable unless otherwise contradicting the provision in this law.

103. A member of the central committee or supervision committee or working committee or investigation committee who is not a civil servant while carrying out their activities in this law shall be deemed as such as mentioned in the penal code Article 21.

New 104. (a) The Union Government shall prescribe the Secretariat of the Central Committee and the Leading Committee.

(b) The Secretariat prescribed under subsection (a) shall be placed under the supervision of the Ministry

New 105. The Secretariat is composed of the Central Committee and the Steering Committee:

(a) Expenses shall be borne

(b) To carry out office duties lightly

106. Outstanding fees and fines in this law shall be collected and it cannot be levied in the income tax and considered as outstanding balance.

107. An individual or organisation assigned to carry out duties and responsibilities in accordance with this law in good faith shall not be prosecuted.

New 108. Department

(a) International cyber security organisations may coordinate with regional cyber security organisations in accordance with the guidelines of the Ministry in implementing international and regional cyber security cooperation.

(b) Hold cyber security technology and proficiency tests and competitions in accordance with

international standards and issue certificates.

New 109. According to this law, the prior approval of the Steering Committee must be obtained in litigation

110. The offences in this law are recognised as cognizable offences and can be charged by the Myanmar Police Force.

New 111. The Central Committee or the Steering Committee or the Ministry or the Electronic Communications Oversight Committee:

(a) any government department; With the permission of the Union Government, the permission required under this Law; Obtaining a license and recommendation; It may be exempt from the public interest if fees are required.

(b) Matters related to the State of Emergency; National defence and security issues; In the case of natural disasters, without the prior approval of the Union Government, the necessary permits under this Law; it may be exempted from obtaining a license and a recommendation or having to pay fees if necessary.

(c) Matters exempted under subsection (b) shall be submitted to the Union Government.

New 112. A license that has not expired under the Electronic Communications Act shall be deemed to be a license issued under this Law and shall be valid until the expiration date of that license. If it will proceed when the license expires, a license must be applied in accordance with the provisions of this law.

113. Should an explanation of any technological terms or technical terms in this law be required, the Ministry can issue a notification to explain such lexicons with the agreement from the State Administration Council.

114. In the implementation of this law;

(a) the Ministry, the Ministry of Home Affairs, and the Ministry of Defense can issue rules and regulations with the agreement of the Union Government.

(b) the Ministry, the Ministry of Home Affairs, the Ministry of Defence, and related ministries can issue notifications, orders, directives, and procedures.

(c) the Central Committee, the Executive Committee and related working committees can issue notifications, orders, directives, and procedures.

115. The Electronic Transactions Law (State Peace and Development Council Law No. 5/2004) is repealed by this law.

I hereby sign this law in accord with the Constitution of the Union of Myanmar.

Sign:

Min Aung Hlaing

Chairman,

State Administration Council