

Myanmar's Legal Framework For Cybersecurity Needs To Be Built To International Standards

May 10, 2021

UPDATE

On 15 February 2021, the State Administration Council (SAC) adopted an amendment to the 2004 Electronic Transactions Law (as amended 2014) which added an aim of 'protecting personal data' to the existing law. It included provisions on personal data (Article 27-bis) taken from the draft Cybersecurity Law (see below). It also added penalties concerning failure to protect personal data, spreading misinformation, and committing cyberattacks ([see consolidated version of the Electronic Transactions Law, as amended](#)).

There was no further news of the draft Cybersecurity Law until **26 April, when in SAC meeting 9/2021**, it was mentioned that there would be measures 'to add required provisions in the cyber law'. No further detail is available.

In February, a [draft 'Cybersecurity Law'](#) (English translation to follow) was sent by some Ministries to certain types of business in Myanmar (ICT, banks) for urgent comments by 15 February.

The military State Administration Council appears to intend rapidly to adopt this law. MCRB has prepared [a document analysing elements of the law](#) from the perspective of human rights, including the rights privacy and freedom of expression which are both contained in Myanmar's constitution, as well as international practices, in support of organisations who intend to do advocacy on the draft law.

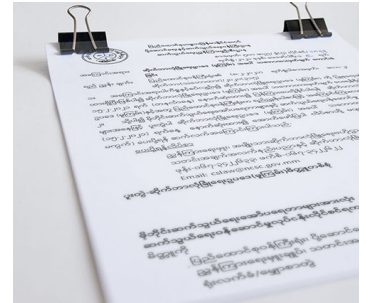
Democratic oversight by the Parliament elected in November 2020 is not possible due to the military's declaration of a State of Emergency. [Over 150 civil society groups](#) have expressed their opposition to the legitimacy of such a wide-ranging law being adopted the SAC, and particularly one which fails to adhere to the state duty to protect human rights.

Adopting a cybersecurity law in the form currently proposed will not only impact on civil society. It will greatly increase the risk for companies in Myanmar, to the extent that some responsible international investors, particularly in the ICT sector, may exit the market altogether, or delay or terminate plans to invest or supply services.

The law's focus on 'data localization' i.e. storage of data in sites determined by the government (Article 28) will also increase the vulnerability and reduce the competitiveness of Myanmar companies, such as banks, e-commerce providers and any other type of company operating in Myanmar making significant use of data, since they will be unable to make use of the security and efficiency offered by international cloud-based service.

Myanmar's chances of creating jobs and becoming a location for offshored data-based services such as call centres or shared services centres will be undermined as this law is incompatible with international data protection regulation such as the EU's General Data Protection Regulation (GDPR).

Finance sources such as private equity, international finance institutions, and banks, will also identify this cybersecurity law, if adopted, as a major ESG risk. If they are unable to mitigate it, they will be unwilling to fund companies in Myanmar at a time when businesses badly needs investment to recover from the COVID recession.



The military State Administration Council to intend rapidly to adopt this law.

Thompson Chau
@tchau01

10 foreign business & industry groups their concerns about #Myanmar's late cybersecurity law.

The statement warns that criminalising usage etc "disrupts the free flow of in & directly impacts businesses' ability to operate legally & effectively."

2:17 PM · Jan 28, 2022

188 Reply Copy link

[Read 24 replies](#)

Further Reading:

[Junta cyber bill has Myanmar business up in arms](#)

Asia Times, 28 January 2022

[Civil society, businesses up in arms over junta's draft Cyber Security Law](#)

The draft law has been criticised by:

- the [Myanmar Computer Federation/Myanmar Computer Industry Association/Myanmar Computer Professionals Association](#)
- [the Union of Myanmar Federation of Chambers of Commerce and Industry \(UMFCCI\)](#)
- [a large number of foreign chambers of commerce/business associations](#) in Myanmar including EU, France, Germany, UK, Italy, Greece, New Zealand
- [AmCham](#)

The [Asia Internet Coalition \(AIC\)](#), whose members include Facebook, Grab, Google and Twitter, is deeply concerned with the devastating law consequences. Individual companies have spoken out including [Telenor](#), and a number of banks.

In 2016 MCRB published a [ICT Sector Wide Impact Assessment](#) which covered many of the human rights risks in the existing Myanmar legal framework. These were updated in 2019 in an [MCRB Policy Brief: The Legal and Policy Framework for Information Communication Technology \(ICT\) In Myanmar: Implications For Human Rights](#).

MCRB's 2019 [Policy Brief on Cyber Security and Cyber Crime](#) identified specific issues for Myanmar and policies which would build an effective cybersecurity framework compatible with international standards:

1. Establish a cyber security framework rather than one law in isolation
2. Prioritise protecting and defending individuals, devices, and networks as the core objective of any cyber security strategy / policy
3. Adopt and implement a comprehensive data protection law – with further detailed address in a separate policy brief on how to achieve a Myanmar [Data Protection Law That Protects Privacy](#)
4. Identify and prioritise the security of the country's critical infrastructure
5. Establish incident response teams
6. Undertake a proper threat assessment and develop recovery plans

These studies and briefs highlighted that of particular concern for privacy is the existing lack of human rights safeguards for surveillance or 'Lawful Interception', currently only addressed in vague powers in Article 75 of the Telecommunications law. As Annex 1 of the recommendations of the 2016 ICT SWIA, MCRB proposed a [Rights-Respecting Lawful Interception Framework](#). The provisions in the SAC's draft cybersecurity law sections 47-50 fail to meet any of the elements of this framework:

47. The State Administration Council shall grant the right to the relevant person or organization in order to intercept as prescribed in any existing law.

48. The companies and organizations providing services as prescribed in the Telecommunication Law shall make arrangements and preparations in advance so that the relevant person or organization authorized under Section 47 can intercept.

49. A relevant person or organization authorized to intercept subject to Section 47 shall conduct any of the following interventions without interfering the fundamental rights of the citizens:

- 1** *Preventing any actions that can harm the sovereignty and territorial integrity of the State;*
- 2** *Performing any acts for the defense and security of the State;*
- 3** *Performing any acts for the rule of law and public order;*

Frontier Myanmar

Frontier Myanmar, 11 February 20.

DOWNLOAD THE MYANMAR ICT S

Full Report (284 pages/5.35mb)

Executive Summary and Recomm

Executive Summary & Recomm
(Burmese)

Chapter 01: Introduction

Chapter 02: ICT Government Insti
Policies & Legal Frameworks

Chapter 03: Sector-Level Impacts

Chapter 04: Operational-Level Im

4.1: Freedom of Expression

4.2: Hate Speech

4.3: Privacy

4.4: Surveillance

4.5: Cyber-Security

4.6: Labour

4.7: Land

4.8: Groups at Risk

4.9: Stakeholder Engagement and
Grievance Mechanisms

4.10: Security and Conflict

Chapter 05: Cumulative-Level Imp

Annex: Background On SWIA Me

Linked Initiatives on ICT/Human R
Myanmar

- 4 *Investigating crimes;*
- 5 *Issues approved under any existing laws; and*
- 6 *Act of safeguarding and protecting public life, property and public welfare.*

50. A Related Ministry or a department and organization which is assigned by the Ministry may investigate, and supervise any services being operated and processed at the online service provider and may request them to provide written records if it is necessary for the country's protection and security purposes and public interest.

On 25 January 2019, MCRB participated in a consultation of Ministries and other interested stakeholders to discuss a draft 'Cyber Law' prepared by Singapore based consultancy TRPC (TRPC.biz) with World Bank funding in response to ToRs provided by the Myanmar's Ministry of Transport and Communications (MoTC). MCRB is making this [January 2019 draft](#) available to improve transparency and address some confusion which has arisen over the origins of the Feb 2021 draft Cybersecurity Law. The draft Cyberlaw was accompanied by a paper on '[Policies Related to e-Government, e-Commerce, and Cyber Security](#)' which addressed a number of issues such as 'cloud first', data classification, etc.

At the 25 January meeting, MoTC and TRPC received feedback that the scope of the draft law was too wide, and that it should be divided into individual laws on issues such as Cybercrime, Data Protection etc. It was also pointed out that the E-Commerce provisions should be covered in a unified law, together with the Ministry of Commerce who was also working on this issue. MCRB also questioned the approach of the draft law, in which important issues were being left to the decision of various Committees. This kind of approach reduced transparency, accountability and legal certainty for businesses and other stakeholders. As a result of dissatisfaction with draft, the planned public consultations in Q1 2019 were not held, and the WB/TRPC assistance came to an end without further extension.

In 2020 the MoTC developed an internal 'zero draft' 'Cybersecurity Law' which took a different approach to the January 2019 draft. This zero draft (see above) was updated following the assumption of power by the 1 Feb 2021 military government.

[Facebook](#)
[LinkedIn](#)
[Twitter](#)

Read also

- [MCRB Submits Input to OHCHR on the Practical Application of the UNGPs to the Tech Sector](#)
- [Update on Draft Cybersecurity Law and its Impacts on Digital Rights and the Digital Economy](#)
- [Why Data Protection Matters: Know what you share!](#)
- [MCRB Provided Comments on Draft E-commerce Strategy for Myanmar and Draft eCommerce Guidelines 2020](#)
- [Recorded discussion panel: "In Privacy and Data Protection We Trust!"](#)
- [Lift the Restrictions on Internet Access](#)



[Previous article](#)

[Next article](#)

[Joint Statement on Mobile Internet Shutdown in Myanmar](#)

[Statement by Concerned Businesses Operating in Myanmar](#)

Funding from governments of UK, Norway, Switzerland, Netherlands, Ireland and Denmark.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Government of
the Netherlands



DENMARK