Malaysia: Draft Cyber Security Bill 2024

April 2024

Legal analysis

Executive summary

In this analysis ARTICLE 19 provides a close look at the Malaysian Draft Cyber Security Bill (the Draft Bill) for its compliance with international freedom of expression standards.

ARTICLE 19 has worked for many years with several civil society organisations to analyse the state of freedom of expression in Malaysia, as well as on cybercrime issues generally. Against the backdrop of an increasingly repressive environment for journalists, human rights defenders, and land rights defenders in Malaysia and of existing censorship under the Communication and Multimedia Act 1998 (CMA), we are gravely concerned that the Bill will be a mechanism for government control over intermediaries. Although posing as a 'cybersecurity' instrument, the Bill will give the government unaccountable control of computer-related activities, as well as nearly unlimited search and seizure powers. Its criminal provisions do not require any actual intent to violate, effectively introducing many strict liability offences. We fear that the broad language of the Bill will likely be abused to further restrict online freedom of expression and dissent in the country. We point out the following issues:

- **The Bill creates a system for broad control of digital services in Malaysia.** Although labelled as a 'cybersecurity' instrument, the Draft Bill fails to be narrowly tailored to address data breaches causing serious harm, and it does not resemble other computer-related legal instruments. It deems "communications", and hence the media, to qualify as "critical information infrastructure" that are potentially subject to disproportionate reporting and regulation under threat of criminal sanctions.

- **The broad scope of key terms under the Bill could capture journalistic activities and target whistleblowers.** The Bill would conflate any disclosure of information in the public interest with the intentional infringement of security measures with dishonest intent. A "cyber security incident" (the definition of which includes the phrase "unauthorized access" to a computer) could criminalise journalistic activities such as reporting on "unauthorized" leaked evidence of corruption provided by a whistleblower. It can even imperil cybersecurity researchers and professionals doing routine penetration testing to actually improve network security. Such a concern is far from hypothetical; journalists in Malaysia have previously faced harassment for publishing evidence from whistleblowers in the public interest.

- **The Bill requires prior licensing of a wide range of expressive activities.** Anyone providing vaguely defined "cyber security services" in Malaysia will require pre-approval under arbitrary standards subject to change or revocation at any time under threat of up to ten years imprisonment. This would require licensing those who exercise their right to expression by publishing or distributing source code online in the public interest, engaging in academic research, or disseminating free digital security tools to journalists and human rights defenders.

- **The Bill provides for search and seizure powers not subject to judicial or other independent review.** So-called "authorized officers" will have the same powers as police, including the ability to execute searches and seizures of persons and places without any need for a warrant if they can show there is "reasonable cause" for not needing one. Further, the "Chief Executive" established under the Bill may issue production demands with no warrant requirement.

ARTICLE 19 believes the Bill to be unnecessary and fatally flawed in its current state. We urge the drafters of the Bill and the relevant committees in charge of scrutinising it to address the shortcomings identified above to ensure the compatibility of any cybercrime legislation with international standards of freedom of expression. We stand ready to provide further assistance in this process.

Key recommendations:
ARTICLE 19 believes the Bill to be unnecessary and flawed in its current state. We urge the government to withdraw the Bill before the royal accent. As such we refrain from making recommendations aimed at editing or modifying it in its current form. However, at a minimum, any framework addressing cybercrime must include the following (non-exhaustive) features:

- Explicit procedural safeguards under international human rights standards;
- Key legal terms that are defined in law and not subject to arbitrary change;
- Public interest provisions that protect the work of digital security researchers, academics, and publishers of code;
- Independent review and oversight over any administrative bodies, including procedural protections such as term limits and criteria for admission and removal;
- Narrowly-defined scope of the meaning of 'cybersecurity' as well as the providers and sectors to be covered under such a framework;
- No police powers without stringent due process protections, transparency, and rights of appeal;
- Limitations of any penalties to administrative measures with robust rights of process and appeal, as well as intentionality requirements prior to the implementation of any sanctions.

Further, ARTICLE 19 repeats the urgent call for Malaysia to renew its commitment to human rights by signing and ratifying the International Covenant on Civil and Political Rights (ICCPR) as well as other major international human rights treaties**.**

In general, too, we repeat our call to the Malaysian government to repeal or amend all laws restricting freedom of expression in Malaysia, including the Sedition Act, Film Censorship Act, Communication and Multimedia Act (CMA), Printing Presses and Publications Act (PPPA), Sections 504 and 505(b), and Sections 298 and 298A (1) of the Penal Code, and to ensure that they comply with international human rights laws and standards.

Table of contents

Introduction

On 25 March 2024, the Cyber Security Bill was tabled at the Lower House of the Malaysian Parliament (Dewan Rakyat) for the first reading[1]. It was passed[2] on 27 March after the second reading at Dewan Rakyat. On 3 April 2024, the upper house of the Parliament (Dewan Negara) unanimously passed[3] the Cyber Security Bill 2024 after the third reading. Next, upon assent by the King (Yang di-Pertuan Agong), the law will take effect once it is published in the Government Gazette.

ARTICLE 19 considers the Bill extremely problematic from the perspective of the international human rights and freedom of expression standards. We have extensive experience in analysing cyber-crime and cybersecurity legislation, as well as various freedom of expression laws. Most recently, ARTICLE 19 has actively participated in several rounds of ongoing negotiations to propose a comprehensive treaty on cybercrime at the UN level, as well as participated in Malaysia's most recent Universal Periodic Review (UPR) in January of this year.[4]

In its submissions to the UPR, ARTICLE 19 and partner organizations pointed out the existing problems of Internet freedom in Malaysia. Specifically, we pointed out problems of investigations and prosecutions under Section 233 of the Communication and Multimedia Act 1998 (CMA), which provides criminal penalties for online communications that are "obscene, indecent, false, meaning offensive in nature with intent to annoy, abuse, threaten or harass a person".[5] 444 cases had been opened under CMA Section 233 from 2020 through January 2023, resulting in 38 cases' prosecutions, 31 convictions, and several ongoing trials.[6] The CMA is often combined with other criminal laws to levy severe criminal sanctions as an intimidation tactic to chill freedom of expression.[7]

There has been an alarming use of police powers against online expression, including against journalists, in recent years. These include:

- In August 2020 authorities raided *Al Jazeera's* office and seized two computers.[8]

[1] Ragananthini Vethasalam, Tarrence Tan and Khoo Gek San, Cyber Security Bill tabled for first reading, The Star, 25 March 2024.
[2] Bernama, Dewan Rakyat Passes Cybersecurity Bill 2024, 27 March 2024.
[3] FMT, Dewan Negara Passes Cybersecurity Bill 2024, 3 April 2024.
[4] Joint submission to the Universal Periodic Review of the Malaysia by ARTICLE 19, CIVICUS World Alliance for Citizen Participation, Komuniti Muslim Universal (KMU) and Sisters in Islam (SIS), 18 July 2023.
[5] *Ibid*., para. 35.
[6] Ministry of Communications and Multimedia Malaysia, 444 cases investigated under Section 233 of CMA since 2020 - Fahmi, 14 February 2023.
[7] ARTICLE 19, Rights in Reverse: One Year Under the Perikatan Nasional Government in Malaysia, 3 March 2021.
[8] Royal Malaysian Police, Facebook post, 4 August 2020.

Numerous journalists of the outlet also faced police questioning and investigation.[9]

- In February 2021, Fahmi Reza was charged twice under Section 233 of CMA for publishing satire; the charges eventually led to acquittal.[10] As part of the investigation, police seized his laptop and smartphone.[11]
- In February 2023, two secondary school students were arrested and detained for criticising history exam papers via a TikTok video.[12]
- In January 2024, two filmmakers, Tan Meng Kheng and Khairi Anwar Jailani were criminally charged for producing the film Mentega Terbang; members of the cast and crew were summoned by the police.[13]

Historically, Malaysia has also seen the CMA be used as a pretext to harass journalists for publishing the disclosures of whistleblowers, as occurred with the Sarawak Report in 2015, which exposed a corruption scandal of legitimate public interest.[14] Since then, others such as investigative journalist Lathiha Kunaratnamm have faced threats for exposing corruption.[15] Indeed, the need to better protect whistleblowers in Malaysia is well-acknowledged and legislative debates are ongoing to reform the Whistleblower Protection Act 2010, although in light of the situation for freedom of expression in Malaysia it is doubtful how meaningful such reforms may be in practice.[16]

Malaysia's Cyber Security Strategy 2020-2024 makes a reference to "respecting the right to freedom of speech".[17] Malaysia also stated in its National Report submitted in October 2023 that it "continues its commitment to create a conducive landscape for FOE [freedom of expression]" by engaging with stakeholders. The government further represented that "Malaysia recognises and values the important role of civil society in facilitating Government's efforts to advance human rights agenda. The Government will continue to engage and involve them in the deliberation of national policies and programmes."[18] However, we remain sceptical of this commitment in light of recent events, and urge the Malaysian authorities to honour it.

The impact of the Draft Cyber Security Bill will be widespread, especially because Malaysia has in recent years seen increasing access to the Internet, particularly in rural areas. However, that infrastructure remains concentrated with providers such as YTL

[9] Al Jazeera, Al Jazeera journalists questioned over Malaysia documentary, 10 July 2020.
[10] ARTICLE 19, Malaysia: Second criminal charge against artist Fahmi Reza this year, 17 February 2022.
[11] Heather Chen, 'Censored' by Spotify and Arrested, a Malaysian Graphic Artist Speaks Out, 27 April 2021,
[12] New Straits Times, Duo detained over viral video of student criticizing SPM History paper, 25 February 2023.
[13] ARTICLE 19, Malaysia: Drop charges against Mentega Terbang filmmakers, 17 January 2024; Arif Zikri, 'Mentega Terbang' director and scriptwriter receive death threats, cars splashed with paint, corrosive substance, Malay Mail, 16 March 2023.
[14] ARTICLE 19, Malaysia: Crackdown on independent voices must end, 5 August 2015.
[15] Malaysia: Media groups condemn the ongoing crusade to silence whistleblowers and journalists, IFEX, 10 January 2022.
[16] Govt considering centralised whistleblower protection agency, Free Malaysia Today, 4 March 2024.
[17] National Security Council, Malaysia Cyber Security Strategy 2020-2024, p. 16.
[18] National report submitted pursuant to Human Rights Council resolutions 5/1 and 16/21, A/HRC/WG.6/45/MYS/1, 31 October 2023, paras. 26-33.

Communications and Telekom Malaysia.[19] This means that digital activities might be effectively controlled by regulating merely a handful of online providers, which could be deemed "cyber security providers" under the breadth of the Bill.

The analysis not only highlights concerns and conflicts with international human rights standards within the Bill but also actively seeks to offer constructive recommendations on how the Bill can be improved. We explain the ways in which problematic provisions in the Bill can be made compatible with international standards on freedom of expression and privacy and set out key recommendations at the end of each section.

ARTICLE 19 further points out that the Draft Bill comes at a moment when nations are debating an international convention on cybercrime at the UN level, in a process Malaysia is actively participating in. It is thus questionable why the Bill is necessary at this point in time, when States are currently attempting to reach a consensus on the international standards that govern both substantive offences as well as investigative provisions that, if passed, would imminently require Malaysia to rewrite any new domestic legislation. To be sure, the Draft Bill does not even reflect the current draft text of the proposed convention, which contains higher thresholds for seizures and involvement of private actors, as well as numerous references to international human rights standards that are absent in the Bill (and which Malaysia is yet to be party to). While ARTICLE 19 and numerous human rights organizations have taken serious issue with the UN negotiations and current draft text of the proposed convention, we note that the Bill falls far short of even that standard.

ARTICLE 19 urges the drafters of the Bill and the relevant committees in charge of scrutinising it to address the shortcomings identified above to ensure the compatibility of the Bill with international standards of freedom of expression. We stand ready to provide further assistance in this process.

[19] Alexander Wong, DNB's 5G network goes live, TM and YTL first to offer 5G services in Malaysia, SoyaCincau, December 15, 2021.

Applicable international human rights standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments. It is enshrined in particular in Article 19 of the **Universal Declaration of Human Rights (UDHR)**[20] and Article 19 of the **International Covenant on Civil and Political Rights (ICCPR)**.[21]

We note that Malaysia has not signed or ratified the ICCPR. Nevertheless, we consider the obligations set out in the ICCPR to largely reflect customary international law, and should therefore guide the interpretation of guarantees for freedom of expression in Article 10(a) of the Malaysian Federal Constitution, as well as other international human rights instruments to which Malaysia is a State party.[22]

Additionally, **General Comment No 34**,[23] adopted by the UN Human Rights Committee (HR Committee) in September 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[24] In other words, the protection of freedom of expression applies online in the same way as it applies offline. State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[25]

Similarly, the four special mandates for the protection of freedom of expression have highlighted in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[26] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

We note that Malaysia has not signed or ratified the ICCPR, despite accepting several recommendations to do so during its last Universal Periodic Review in 2018.[27] Nevertheless, the obligations set out in the ICCPR largely reflect customary international law. The ICCPR

[20] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[21] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[22] See, for example: Convention on the Rights of the Child, at Article 13; Convention on the Rights of Persons with Disabilities, Article 21.
[23] Human Rights Committee, General Comment No. 34, CCPR/C/GC/3, adopted on 12 September 2011.
[24] *Ibid.*, para 12.
[25] *Ibid.*, para 17.
[26] Joint Declaration on Freedom of Expression and the Internet, June 2011.
[27] Human Rights Council, Report of the Working Group on the Universal Periodic Review: Malaysia, A/HRC/40/11, 7 January 2019.

should therefore guide the interpretation of guarantees for freedom of expression in Article 10(a) of the Malaysian Federal Constitution, as should other international human rights instruments to which Malaysia is a State party.[28] Malaysia must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of the ICCPR as interpreted by the HR Committee and that they are in line with the special mandates' recommendations.

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. The determination of whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

- **Be prescribed by law**: this means that a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[29] Ambiguous, vague or overly broad restrictions on freedom of expression are therefore impermissible;

- **Pursue a legitimate aim:** exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals. As such, it would be impermissible to prohibit expression or information solely on the basis that a speaker casts a critical view of the government or the political and social system espoused by the government;

- **Be necessary and proportionate**. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[30]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[31]

[28] See for example, Convention on the Rights of the Child, Article 13; and Convention on the Rights of Persons with Disabilities, Article 21.
[29] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
[30] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[31] General Comment 34, *op.cit.*, para 43.

Freedom of expression online and intermediary liability

At the international level, several human rights bodies and mechanisms have developed soft law guidance on freedom of expression online and intermediary liability.

The UN Human Rights Council (HRC) recognised in 2012 that the "same rights that people have offline must also be protected online."[32] The HR Committee has also made clear that limitations on electronic forms of communication or expression disseminated over the Internet must be justified according to the same criteria as non-electronic or "offline" communications, as set out above, while taking into account the differences between these media.[33]

While international human rights law places obligations on States to protect, promote and respect human rights, it is widely recognised that business enterprises also have a responsibility to respect human rights.[34] In meeting their obligations, States may have to regulate the behaviour of private actors in order to ensure the effective exercise of the right of freedom of expression.

Importantly, the UN Special Rapporteur on freedom of opinion and expression (Special Rapporteur on freedom of expression) has long held that censorship measures should never be delegated to private entities.[35] In his June 2016 report to the HRC,[36] the Special Rapporteur on freedom of expression, David Kaye, enjoined States not to require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extra-legal means. He further recognised that "private intermediaries are typically ill-equipped to make determinations of content illegality,"[37] and reiterated criticism of notice and takedown frameworks for "incentivising questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation," i.e. the danger of "self- or over-removal."[38]

The Special Rapporteur on freedom of expression recommended that any demands, requests and other measures to take down digital content must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under Article 19(3) of the ICCPR.[39]

[32] HRC Resolution 20/8 on the Internet and Human Rights, A/HRC/RES/20/8, June 2012.
[33] General Comment No. 34, *op cit*., paras 12, 39, 43.
[34] Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex. The UN Human Rights Council endorsed the guiding principles in HRC resolution 17/4, A/HRC/RES/17/14, 16 June 2011.
[35] Report of the Special Rapporteur on freedom of expression, 16 May 2011, A/HRC/17/27, paras 75-76.
[36] Report of the Special Rapporteur on freedom of expression, 11 May 2016, A/HRC/32/38; paras 40-44.
[37] *Ibid*.
[38] *Ibid*., para 43.
[39] *Ibid*.

The international freedom of expression mandates have further expressed concerns at "attempts by some governments to suppress dissent and to control public communications through […] efforts to 'privatise' control measures by pressuring intermediaries to take action to restrict content."[40] Their 2017 Joint Declaration emphasises that:

> [I]ntermediaries should never be liable for any third party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.

They also outlined the responsibilities of intermediaries regarding the transparency of and need for due process in their content-removal processes.[41]

Surveillance of communications

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[42] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right to private communications is strongly protected in international law through Article 17 of the ICCPR[43] which states, *inter alia*, that no one shall be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. In **General Comment no. 16** on the right to privacy,[44] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place when provided for by law, which itself must comply with the provisions, aims and objectives the ICCPR. It further stated that:

> [E]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[45]

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the

[40] 2017 Joint Declaration, *op. cit.*
[41] Manila Principles on Intermediary Liability.
[42] *Ibid*, para 84.
[43] Article 17 states: "1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks."
[44] HR Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).
[45] *Ibid.*, para 8.

right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test:

> Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.[46]

In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of the scope of legitimate restrictions on the right to privacy in the following terms:

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[47]

The Special Rapporteur on FOE has also observed that:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[48]

Anonymity and encryption

The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. A fundamental feature enabling anonymity online is encryption.[49] Without the authentication techniques derived from encryption, secure online transactions and communication would be

[46] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009, para 17.
[47] *Ibid.*, para 21.
[48] Report of the UN Special Rapporteur on Freedom of Expression, Frank LaRue, A17/27, 17 May 2011, para 59.
[49] Encryption is a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" that protects the confidentiality of content against third-party access or manipulation; see e.g. SANS Institute, History of encryption, 2001.

impossible.

The right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FOE, published his report on encryption and anonymity in the digital age.[50] The report highlighted the following issues in particular:

- Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[51]

- Anonymous speech is necessary for human rights defenders, journalists, and protestors. Any attempt to ban or intercept anonymous communications during protests is an unjustified restriction on the right to freedom of peaceful assembly under the UDHR and the ICCPR.[52] Legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications.

Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[53] Laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. Strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction.[54]

The Special Rapporteur's report also addressed compelled 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with Governments, creating serious challenges that implicate individual users online."[55] The report stipulated that such orders should be

- based on publicly accessible law;
- clearly limited in scope and focused on a specific target;
- implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets; and
- only adopted when necessary and when less intrusive means of investigation are not available.[56]

[50] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye A/HRC/29/32, 22 May 2015.
[51] *Ibid.,* paras 12, 16 and 56.
[52] *Ibid.,* para 53.
[53] *Ibid.,* para 56.
[54] *Ibid.,* paras 31-35.
[55] *Ibid.*, para 45.
[56] *Ibid*.

Cybercrime

No international standard on cybercrime exists; but of the regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has been the most relevant standard.[57] Although Malaysia is not a signatory to the Convention, it provides a helpful model for states seeking to develop cybercrime legislation.

The Cybercrime Convention provides definitions for relevant terms, including definitions for computer data, computer systems, traffic data, and service providers. It requires State parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data. These procedural requirements require independent review.

Finally, and importantly, the Cybercrime Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

[57] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004. As of May 2015, 46 states have ratified the Convention and a further 8 states have signed the Convention but have not ratified it.

Analysis of the Draft Cyber Security Bill 2024

Overall, ARTICLE 19 recommends withdrawing the Draft Bill in its current state. If it progresses for further approval, it must be brought in line with international human rights standards. Below we set forth fundamental concerns, although these should be understood as indicators of key problems with the Bill rather than as an endorsement of the Bill even if these issues are addressed.

Overbroad definitions of key terms, subject to change at will, or missing entirely

ARTICLE 19 observes that several key terms of the Draft Bill are incredibly broad, circular, or subject to revision at will. For instance, "cyber security incident" can include *any* "act or activity" that is done "on or through" a system without "lawful authority". To qualify as such an incident, the activity must merely "jeopardize or adversely affect" the "cyber security" of a computer or computer system. The lay understanding of the term 'cyber security' might appear to encompass the infringement of technical security measures. Looking to the term "cyber security" leads to a similarly vague definition; it is simply described as a "state" in which a computer or system is "protected from any attack or unauthorized access" and the "confidentiality" of information is maintained.

At the outset we observe that the phrase "cyber security" is not defined under international law, and instruments such as the Budapest Convention do not contain this term. The closest analogue to the concept of 'security' may include criminal offences named under the Budapest Convention, such as illegal access in Article 2 of that instrument, which require the intentional access to the whole or any part of a computer system without right. Importantly, the latter framing has an intentionality requirement, whereas an "incident" under the Bill need not be the result of any ill intent.

Read literally, a "cyber security incident" could thus capture an instance where a whistleblower provides evidence of corruption or violations of law to a journalist. Such reporting on primary documents would be the result of "unauthorized" access that fails to preserve "confidentiality" of information. As set forth below, this whistleblower activity (and subsequent reporting) would trigger numerous affirmative obligations on part of providers as well as overreaching investigatory provisions that would interfere with journalistic activities. It can even imperil cybersecurity researchers and professionals doing routine pen testing to actually improve network security.

Other standards of the Draft Bill are open-ended, with numerous 'definitions' containing clauses allowing for re-definition as fit. Some examples include:

- The definition of "national critical information infrastructure entity" may be expanded at will under Articles 17 and 18;

- A “cyber security service” is defined as whatever the Minister “may prescribe” under Article 27(2);
- Article 28(a) provides that requirements for licenses are “as may determined by the Chief Executive”;
- Conditions for such under Article 31(1) are subject to “conditions as the Chief Executive thinks fit to impose”;
- An “authorized officer” may be “any public officer authorized under section 36”.

As currently drafted, the following are just a few (non-exhaustive) examples of terms appearing in the Bill which are either undefined, or so vague as to be nearly meaningless: “cyber security,” “cyber security service,” “cyber security provider,” “national critical information infrastructure entity,” “unauthorized access,” “lawful authority,” “reasonable cause,” or “moral turpitude.”

By nature, such an absence of legal definition fails the first test of legality under the three-part test of international law where those definitions may impact the exercise of freedom of expression or other rights online.

Recommendation:

- Strike any cross-references of definitions that allow for government modification of terms. Key terms that are relied upon in measures imposing criminal liability must be defined explicitly and with legal precision.

Requirement of prior licensing for wide range of legitimate activities in the public interest

One of the primary aims of the Draft Bill is to create a “licensing” system as laid out in Part VI. Article 27(1) makes it a crime to “provide any cyber security service” or even hold oneself out to do so, without first obtaining a license. Doing so is subject to a fine of 500,000 ringgit or imprisonment of up to a staggering ten years.

As ARTICLE 19 outlined above, it is difficult to even ascertain the scope of this provision because the basic definition of “cyber security service” is overbroad. Further, Article 27(2) gives the Minister the blanket authority to “prescribe any cyber security service”, meaning the scope of the license is subject to change at will. In the context of media, mandatory licenses are never justified for simply exercising expression online.

At a minimum, we predict that the following actors or entities would fall under the broad scope of requiring licenses:

- Publishers of digital security tools, including developers of free and open source software (FOSS);
- Academic researchers conducting security testing;
- Internet intermediaries or social media platforms;
- Human rights activists or journalists sharing digital security tools.

The administrative burdens of such a license are completely subject to government discretion. For instance, Article 28(a) provides that requirements of a license are "determined by the Chief Executive", and its period under Article 29(4) is "valid for a period as specific in the license". Conditions of such a license, pursuant to Article 31(1), are contingent on whatever the Chief Executive "thinks fit to impose", which can be varied or revoked at will. Violating any of these arbitrary conditions is a separate offence subject to two years imprisonment or a fine of 100,000 ringgit. A license also carries an obligation to produce nearly limitless information "as the Chief Executive may direct" pursuant to Article 32(2)(c). While Article 53 appears to provide a right of appeal, this appeal is made directly to the Minister rather than any independent external review.

ARTICLE 19 notes that requiring government pre-approval, under threat of criminal penalty, for activities such as publishing or the use of digital security tools is by nature a restriction on freedom of expression. As a result, the licensing scheme set forth by Part VI must be analysed under the three-part test of international law, and if it fails this test, it is incompatible with international standards. As set forth above, these articles routinely fail the test of legality, as a number of key terms and procedural requirements contain no definition at all, or are subject to change at will. Such a system provides no legal notice of the underlying conduct subject to restriction.

Further, imposing such a licensing restriction on broad sectors of society, for expressive activity, is neither a necessary nor a proportionate means to achieving any legitimate aim under international law. Therefore, the licensing system fails the three-part test. Outside the scope of the limitations on expressive activity, it is unclear why such a licensing system (and accompanying penalties) is necessary or appropriate to further cybersecurity in Malaysia. The only time a licensing system might be appropriate or proportionate in the context of media is where there is a limited number of broadcast frequencies requiring some degree of administrative regulation due to scarcity. That, however, is not the case here nor what is contemplated.

Recommendation:

- Strike the licensing system of Part VI in its entirety.

Lack of independence or external oversight of the National Cyber Security Committee

The Draft Bill established, in Part II, a "National Cyber Security Committee" (Committee) that suffers from numerous fatal problems as a body with significant authority and procedural powers. Most importantly, the Committee lacks any independence at all. It is comprised primarily of government ministers, its most prominent member being the chair, the Prime Minister. The addition of other members is limited to two. The Chairman (Prime Minister) has significant procedural discretion under Article 7, and basic procedures are undefined and up to the Committee to determine. There are no term limits on the Committee, no external

oversight or opportunity to challenge or review its composition or decisions, and no mechanisms to remove members who engage in misconduct. As such, the work of the Committee can be viewed as a direct extension of the Prime Minister.

Chief Executive may demand production without a warrant

This lack of independence is particularly problematic as the Committee and its Chief Executive possess significant police powers. For instance, Article 6(1)(g) contains a catch-all provision granting the Committee the power to "do such other things" that are "arising out of or consequential" to the Bill. The next provision, Article 6(2), provides for powers "necessary for, or in connection with, or reasonably incidental to" the performance of the Bill. This provides latitude for a wide range of measures, the limit of which is unclear. However, as other articles specifically provide for police powers with criminal penalties, the aforementioned broad provisions may be read as reasonably intending to accomplish the same.

The Committee maintains a "Chief Executive" who is granted a wide range of enumerated powers in Article 10, including the same language as appears in Article 6(2). Supplementing that broad provision are numerous sweeping investigatory and search powers. This includes the power to issue written notices under Article 14 to "any person" to demand the production of information, documents, or electronic media on a schedule "as specified" or otherwise determined by the Chief Executive. If the recipient of such a demand does not possess the demanded information, Article 14(2) requires them to assist by identifying who may have custody. Failure to comply may lead to up to three years imprisonment. These notices are not subject to any external review process and are entirely up to the discretion of the Chief Executive in substance and procedure.

Disproportionate burdens on nearly any entity in the private sector, including media

Part IV provides the Committee the power to designate any person or entity as belonging to "national critical information infrastructure", a cumbersome concept that appears over 200 times in the Bill and grants nearly limitless control over any designee. This phrase (herein labelled NCII) is cross-referenced via a Schedule attached at the end of the Bill, and provides a number of "sectors" of society that are determined to be of heightened critical information. However, we observe that the list contains 11 items that seem to cover every aspect of society beyond what would commonly be understood to be critical for defence, energy, or disaster relief. These categories include everything from transportation to information and communication, healthcare, energy, agriculture, trade and industry, and technology. We note with grave concern the inclusion of "communication" which would appear to capture media.

Article 15(1) allows the Minister to appoint any "person" or government entity to be a NCII sector lead. Article 18(1) further grants the Chief Executive this authority with minimal requirements, and again, not subject to any independent oversight or review. A NCII sector lead may accordingly appoint a NCII entity, which then is held to an onerous number of

requirements and obligations under strict criminal penalty for noncompliance. Some of those include, under Articles 20(1)-20(3):

- A duty to provide information "relating to" the NCII upon request;
- A duty to provide information on any new computers or computer systems obtained; and
- A duty to provide notice of any "material" changes to computers or computer systems of the NCII.

Importantly, a single violation of these provisions carries a steep criminal penalty of up to two years imprisonment and a fine of 100,000 ringgit, and no intent is required. NCII entities are also expected, pursuant to Articles 22-24, to conduct risk-assessments, cyber-security exercises, and provide active notification of any "cyber security incident". Failure to comply also carries steep penalties, and in the case of failing to actively disclose a "cyber security incident" may be punished by up to ten years imprisonment without any intentionality.

ARTICLE 19 finds that the lack of clear definition or guidance makes the scope of these provisions unclear, but the explicit inclusion of the "communication" sector would suggest that media or broadcast organizations are contemplated to be subject to being designated as NCII entities. Upon such a designation, a media or broadcast organization would have active obligations to report on all computer-related activities and would be liable for the aforementioned violations. Similarly, social media companies are reasonably part of the sector, and may be expected to comply with unreasonable demands to surveil all digital activities that occur on their systems. The designation and subsequent demands would not be subject to external review or meaningful rights of appeal.

Recommendations:

- Any administrative bodies must be subject to basic procedural protections such as term limits, qualifications for admission or removal, and opportunities for independent oversight;
- Article 14 is especially incompatible with fundamental principles of proportionality, as any police powers must be subject to minimal due process protections;
- NCII entities must not be subject to criminal penalties, especially without any intentionality requirements;
- NCII entities in any regulatory framework must be limited to those strictly necessary, and not include sectors such as "communication" which may draw in media and broadcast organizations as well as social media platforms.

Significant police powers without independent review or oversight

Part VIII pf the Draft Bill sets forth numerous law enforcement powers; we observe that these powers are not simply limited to police officers, but may be issued to any "authorized officer" on the determination of the Minister. In effect, any person who is not a police officer may be granted, under Article 38(2), "the powers of a police officer of whatever rank as provided for under the Criminal Procedure Code" for investigating any offence under the Bill.

Of important note is that while certain powers are granted, there is no mention of accompanying limitations or due process rates with respect to these officers. It is hence unclear whether this part effectively creates a new police designation that operates with the powers of police without the accountability. Neither are authorized officers required to undergo any training or possess any meaningful qualification.

Searches and seizures do not require warrants

The authorized officers are not required to adhere to warrant requirements in conducting searches. While Article 39 sets forth criteria to apply to a Magistrate for a warrant before conducting a search, Article 40 complete subsumes this by offering a blanket exception to any warrant requirement. A warrant is not required if "an authorized officer is satisfied" that "he has reasonable cause to believe" that obtaining a warrant would cause an investigation to be "adversely affected". All an officer must do is claim there is "reasonable cause", and they will subsequently have all powers as if a traditional warrant were obtained. There is no mechanism to monitor or otherwise review the self-determination of the officer.

Further, the standard of "reasonable cause" is the exact same standard that must be articulated to a judge in Article 39, meaning that an officer does not need to satisfy any heightened legal standard to skip the warrant requirement. This would appear to make the Article 39 procedure pointless, and means that for practical purposes warrants are not required under the Bill.

Officers may compel decryption

Article 46(2) allows any authorized officer to demand passwords, encryption or decryption codes, and software or hardware to access information. We note that under international standards, encryption facilitates the exercise of free expression and privacy, and restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law. It is often the case that service providers do not even possess the technical capacity to decrypt end-to-end communications that pass through their systems; such providers should not face criminal penalty or contempt if this is the case.

Recommendations:

- Warrant requirements cannot be subject to exception unless in narrow situations of emergency, and still must be subject to immediate judicial review and right of challenge or appeal;
- Persons cannot be forced to decrypt information or otherwise provide technical assistance in unlocking communications.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. We have produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19, you can contact us by e-mail at legal@article19.org. For more information about ARTICLE 19's work in Malaysia, please contact Nalini Elumalai at nalini@article19.org.