ARTICLE 19

Hong Kong: Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure

July 2024

Legal analysis

Executive summary

In this legal analysis, ARTICLE 19 evaluates Hong Kong's Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure, released on 2 July 2024, for its compliance with international human rights standards.

According to the drafters, the Proposal aims to enhance the protection of critical information infrastructure systems against cyber threats. This initiative responds to a growing global concern over cyber-attacks that disrupt essential services, as evidenced by recent incidents, including a ransomware attack on Union Hospital in Hong Kong. The proposed legislation seeks to establish a robust regulatory environment to safeguard critical infrastructure, including sectors such as energy, finance, healthcare, and communications.

ARTICLE 19 finds that while the Proposed Framework aims to bolster national security and public safety, it raises significant human rights concerns. The existing National Security Law in Hong Kong has already faced criticism for curbing civil liberties, and similar concerns are echoed in this new proposal.

To align the proposal with international human rights standards, we believe it is crucial that the definitions of critical infrastructure, particularly in the IT sector, are clearly articulated to avoid ambiguity. Additionally, we recommend that the legislation should incorporate strict safeguards to prevent arbitrary enforcement and ensure that any restrictions on freedom of expression are narrowly tailored and proportionate to prevent misuse and ensure compliance with international human rights obligations.

We urge the drafters of the Proposed Framework to carefully consider our recommendations and ensure that the rights of individuals are not compromised in the pursuit of cybersecurity.

Table of contents

Introduction

On 2 July 2024, the Security Bureau of the Hong Kong Government released a legislative proposal to the Legislative Council, along with a paper summarising the legislative background and stakeholder consultations. The proposal, titled the Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure (Proposed Framework),[1] was prepared by the Security Bureau, Office of the Government Chief Information Officer, and the Hong Kong Police Force. It marks an attempt to secure critical information infrastructure systems in Hong Kong and protect them from attacks that can disrupt their functioning and impact essential services for society.

ARTICLE 19 observes that in recent years, there have been increasing disruptions to the functioning of critical infrastructure worldwide caused by a range of external cyber threats such as ransomware or distributed denial of systems attacks.[2] Examples include the forced suspension of scheduled hospital surgeries,[3] disruption of electricity grids,[4] and disruptions of oil transportation pipelines through ransomware attacks.[5] As recently as April 2024, the Union Hospital in Hong Kong was the victim of a ransomware attack that "caus[ed] the computer system to malfunction and affect[ed] medical services."[6]

The increase in attacks stems naturally from the increased digitisation of the infrastructure designed to deliver essential services. For instance, forensic analysis of the disruption to Mumbai's electricity grid in October 2020 suggests that this was caused by malware inserted into an electricity despatch centre which was then transmitted into a dozen critical nodes.[7] In other cases, however, human error or a failure to observe standards on part of the entity operating critical infrastructure was the primary vulnerability. In 2021, the Colonial Pipeline in the USA was the victim of a ransomware attack that was enabled by the leaked password of an old employee's account.[8]

[1] Security Bureau, Legislative Council Panel on Security Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure, LC Paper No. CB (2) 930/2024 (03).
[2] Andraz Kastelic, International cooperation to mitigate cyber operations against critical infrastructure: Normative expectations and emerging good practices, UNIDIR, 2021.
[3] Helen Livingstone, New Zealand hospital faces second weak of disruption after major cyber attack, *The Guardian*, 24 May 2021; BBC, Hospitals cyber attack impacts 800 operations, *BBC*,14 June 2024.
[4] David E. Sanger and Emily Schmall, China appears to warn India: Push too hard and the lights could go out, *New York Times*, 27 September 2021.
[5] Laila Kearney, US electric grid growing more vulnerable to cyber attacks, regulator says, *Reuters*, 5 April 2024.
[6] The Standard, Union Hospital confirms cyber attack; sources say hackers want US$10m ransom, *The Standard*, 20 April 2024.
[7] David E. Sanger and Emily Schmall, *New York Times, op.cit.*
[8] William Turton and Kartikay Mehrotra, Hackers breached Colonial Pipeline using compromised password, *Bloomberg*, 5 June 2021.

This increase in attacks has prompted governments to cultivate standards which ensure that entities operating critical infrastructure shore up resilience. A slew of legislative and policy measures has been implemented in the past five years. The briefing paper refers to Mainland China's Cybersecurity Law (2016) and Regulation for Safe Protection of Critical Information Infrastructure (2021); Macao SAR's Cybersecurity Law (2019); Australia's Security of Critical Infrastructure Act (2018); UK's Network and Information Systems Regulation (2018); Singapore's Cybersecurity Act (2018) and the EU Directive on the measures for a high common level of cybersecurity across the Union 2022.

Thus far, Hong Kong has tackled threats to critical infrastructure through non-legislative measures. The Office of the Government Information Officer set up the Internet Infrastructure Liaison Group in 2005. Further, the Cyber Security Centre of the Hong Kong Police force conducts cyber audits of critical infrastructure in the key sectors of government, banking, finance, communications and public utilities.

ARTICLE 19 recognises that legislative provisions that compel critical infrastructure operators to comply with standards and protocols to boost cyber resilience and hold them accountable in instances of non-compliance could potentially secure these essential services for the public. However, we are aware that legislation imposed to ostensibly attain general national security goals or specific cyber security goals could also enable violations of international human rights law and the right to freedom of expression.[9] This is particularly the case in Hong Kong, where the National Security Law has been criticised for stifling freedom of expression both online and offline and curbing press freedoms.[10] In particular, legislation with vague provisions that give discretionary powers to the state violates the principle of legal predictability.[11]

In this analysis, ARTICLE 19 therefore evaluates Hong Kong's proposed legislation from the lens of international human rights law and highlight instances where provisions may not be in conformity with international human rights standards. While the intention behind the proposed legislation is to enhance cybersecurity for critical infrastructure in Hong Kong, the implications for human rights standards are significant.

Importantly, in this analysis, we do not undertake a comprehensive analysis of the Proposed Framework. In light of our expertise, the analysis is focused on the application of international standards on freedom of expression and related privacy concerns. The omission of any provisions from this analysis does not mean that ARTICLE 19 endorses them or finds them in compliance with international law.

[9] Carolina Rossini and Natalie Green, Cybersecurity and Human Rights, Global Partners Digital.
[10] Michael Caster, A year of creeping darkness under the National Security Law in Hong Kong, 29 June 2021.
[11] See UN Human Rights Committee, General Comment No. 34 on freedoms of opinion and expression (Article 19 ICCPR).

We urge the drafters of the Proposed Framework to carefully consider our recommendations and ensure that the rights of individuals are not compromised in the pursuit of cybersecurity.

Applicable international freedom of expression standards

The protection of the right to freedom of expression

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) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).

Additionally, General Comment No. 34 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.[12] 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.

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, which stipulates that the restrictions must: [13]

- **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. Ambiguous, vague or overly broad restrictions on freedom of expression are therefore impermissible.

- **Pursue a legitimate aim:** These are 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.

- **Be necessary and proportionate to the aim sought:** Necessity requires that there must be a pressing social need for the restriction, which must have a direct and immediate connection to 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

[12] General Comment No. 34, *op.cit.*
[13] *Ibid*.

> individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.

The protection of the right to privacy

The right to privacy complements and reinforces the right to freedom of expression. It is essential for ensuring that individuals can freely express themselves, including anonymously, 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 which states, *inter alia*, that no one shall be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. The Human Rights Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law.[14] Interference authorised by States can only take place when provided for by law, which itself must comply with the provisions, aims and objectives of 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.[15]

Restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test, similar to the one under Article 19 of the ICCPR. This means that 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.

Hong Kong is a party to the ICCPR as the United Kingdom extended treaty protections to the territory in 1976. In 1997, China allowed these protections to remain in force. The protection of human rights in Hong Kong is enshrined in the Basic Law. Article 39 of the Bill of Rights Ordinance and Basic Law puts the ICCPR into effect. Therefore, any legislation passed by the Legislative Council must be in conformity with ICCPR provisions.

[14] Human Rights Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).
[15] *Ibid.*, para 8.

ARTICLE 19's comments on the Proposed Framework

Summary of the proposal

The Proposed Framework is divided into four parts:

- The first part is a Background Paper that provides legislative background to and seeks to justify the legislative proposals.

- Annex I sets out a list of obligations, proposed offences and penalties on Operators of Critical Information Infrastructure (CIOs).

- Annex II sets out the main investigative powers of the Commissioner's Office Annex III sets out a "Code of Practice" that operators of Critical Infrastructure need to comply with.

- Annex IV summarises the main recommendations of the proposed legislation.

The Security Bureau will establish a Commissioner's Office to administer the legislation. The Commissioner's Office will designate Operators of Critical Infrastructure (CIOs) and critical computer systems (CCS). A broad range of sectors that may be construed Critical Infrastructure are indicated in the legislation.

Once designated as a CIO, an organisation will have to comply with the following obligations:[16]

- *Organisational*: CIOs must provide information to the Commissioner's Office regarding an address and office in Hong Kong, report any ownership changes and establish a dedicated security management unit;

- *Preventive:* CIOs must keep the Commissioner's Office informed on any changes or updates to the Critical Computer Systems including changes to the design, configuration and security operation;

- *Incident reporting and response:* CIOs must formulate and submit an emergency response plan, participate in drills organised by the Commissioner's Office and notify the Commissioner's Office of any security threats.

The Commissioner's Office has a number of powers to investigate non-compliance under the legislation. There are hefty financial penalties ranging from HK$500,000

[16] Annex IV, para 8.

(USD 64,050) to HK$5 million (USD 640,490) and additional daily fines of HK$50,000 (USD 6,405) or HK$100,000 (USD 12,810) for persistent non-compliance of certain offences.[17] Rightfully, there are no criminal penalties.

ARTICLE 19's analysis

Broad scope of entities covered by the Proposed Framework

Section 2 of the proposal identifies two major categories of critical infrastructure sectors.

Category 1, "infrastructures for delivering essential services in Hong Kong," includes energy, information technology, banking and financial services, local transport, air transport, maritime, healthcare services and communications and broadcasting. On its face, this categorisation makes practical sense. All of these categories are understood in jurisdictions across the world to fall within the ambit of "critical infrastructure." Further, in Hong Kong, all of these sectors except "Information Technology" are well defined under sectoral regulations.

However, ARTICLE 19 notes that the concept of "information technology" is a broad and ambiguous category that could potentially include a wide range of organisations. Without a clear definition of this sector, businesses remain unclear on whether the stringent requirements of the forthcoming legislation might be applicable to them. Further, the inclusion of this vague category could pave the way for entities such as popular messaging companies or internet exchange points to be treated as CIOs and subjected to the heightened investigative powers enabled by this legislation. This violates the principle of legal predictability and could be misused by the state to impose compliance costs on businesses that are working on issues critical of the government.

We also observe that other jurisdictions have gone about regulating the "Information Technology" critical infrastructure sector more judiciously. For instance:

- The United States policy framework put out by the National Coordinator for Critical Infrastructure, Security and Resilience includes "information technology" as a critical infrastructure sector.[18] In its definition, it has included a range of functions within its ambit including the provision of IT Products and Services; Incident Management Capabilities, Identity Management and Trust Support Services, Internet based content, information and communications services, internet routing, access and connection services. However, unlike in Hong Kong proposal, the United States has not imposed statutory obligations on all entities

[17] Annex IV, Point 15
[18] National Security Memorandum on Critical Infrastructure Security and Resilience, 30 April 2024.

carrying out these functions and instead only proposed sector level strategic plans to further cyber resilience.

- The UK's Network and Information Security Act delineates the "digital infrastructure" sub-sector to include Top Level Domain Name registries, DNS resolver services and IXP operators who cross certain thresholds such as volume of usage within the UK or market thresholds.[19] While the UK does impose statutory obligations, it specifies the range of entities that might need to comply with such statutory obligations.

ARTICLE 19 believes that Hong Kong should also precisely stipulate specific kinds of entities that fall within the "information technology" sector. Content delivery platforms should be explicitly excluded as the imposition of compliance costs on these platforms could pose significant business costs to their functioning and potentially compel them to exit the market. This could deny users an online platform to exercise their right to freedom of expression.

In addition to the eight sectors included in Category 1, the legislation proposes a vague Category 2 that includes "other infrastructures for maintaining important societal and economic activities." The Background Paper provides an illustrative set of examples of entities that would fit into this second category including "major sports and performance venues, research and development parks, etc."[20]

We note that this illustrative list is also too broad. In particular, we find that subjecting research institutions and performance venues to these onerous compliance requirements could end up hindering innovation and the freedom of expression. With academic and research freedom in Hong Kong already in jeopardy,[21] this legislation could be used to further impose onerous compliance burdens on entities and restrict research.

Further, we observe that the unclear nature of this list also allows the Commissioner to designate sectors such as the media as "essential services" and subject them to the enhanced investigation powers and compliance requirements of this legislation, thus constraining resources available to conduct research or report. Therefore, this ambiguous categorisation could enable the further suppression of online media freedom in Hong Kong.

We are also concerned that apart from the ambiguous categorisation described above, the legislation does not stipulate thresholds for organisations to be notified as CIOs. The Background Paper states that operators to regulate will "mostly be

[19] Network and Information Security Regulations 2018, Article 10.
[20] Background Paper, para 11.
[21] Yojana Sharma, Academic freedom a top concern as new security law looms, University World News, 8 March 2024.

large organisations, small and medium enterprises and the general public will not be affected."[22]

We observe, however, that this intent is not reproduced in the "Main Recommendations" outlined in Annex IV. Even if this line were to be incorporated into the legislation, there is no clarity on the threshold (either in terms of revenue or scale of operations) for a business to be considered a "large organisation." Further, the text suggests that the legislation would "mostly" be applicable to large organisations without providing any guidance on the circumstances when small or medium businesses and individuals may fall within its ambit.

ARTICLE 19's recommendations:

- The Proposed Framework should define clearly the term "information technology" sector as relevant to the proposed legislation and provide a specific category of entities that could fall within this category. Content delivery platforms should specifically be excluded in the legislation.

- Category 2 should be removed from the Proposal in its entirety as it is vague and provides unfettered discretion to the Commissioner's Office.

- The legislation should clarify thresholds by sector for entities (based on revenue, market share, users and potential impact) for potential entities to be designated as CIOs.

Potential conflicts with the Privacy Regulator

The vague wording of the legislation also risks potential conflict with Hong Kong's privacy regulator, the Privacy Commissioner for Personal Data.

ARTICLE 19 observes that while the Background Paper excludes personal data from the ambit of the legislation, the legislative proposal mentions the potential harms of "data leakage" from an entity as one of the factors for it getting designated as a CIO.[23] If 'data leakage' is a potential harm the legislation wants to guard against, then logically any "personal data leakage" should be reported to the Commissioner's Office under this legislation. However, the Commissioner's Office is tasked with dealing with critical infrastructure from a national security or public order perspective and does not have the resources or procedures in place to notify victims of said personal data leakage.

ARTICLE 19's recommendation:

[22] Background Paper, para 11 (b).
[23] Background Paper, para 17 (a).

- A *non obstante* clause should be added to the legislation, clearly stipulating that the Privacy Commissioner for Personal Data will be tasked with addressing and remedying cases where personal data has been leaked.

Carte blanche government exemption

The proposed legislation provides a carte blanche exemption for government entities that may be CIOs.[24] Instead, the background paper stipulates that government entities need to continue complying with the less onerous Government Information Technology Security Policy and Guidelines, which are not statutory obligations.

ARTICLE 19 finds that this exemption is poorly thought out for two reasons.

- First, critical infrastructure run by government entities are subject to the same threats and vulnerabilities as the private sector. Exempting them from more stringent regulation vitiates the purpose of the legislation as Hong Kong's critical infrastructure is still vulnerable to disruption. If compliance with the guidelines is enough to ensure that critical computer systems run by government operators are secure and resilient, it is unclear why the same guidelines are not adequate for private sector operators.

- Second, exempting government entities while exposing private entities to enhanced investigation powers and compliance requirements suggests that the government may use this legislation to clamp down on the rights of private sector entities as and when required while not being held accountable for its own genuine statutory violations.

ARTICLE 19's recommendation:

- The exemption for government entities should be removed from the Proposed Framework. The legislation should clarify that government entities running critical infrastructure will also be designated as CIOs.

Need to disclose excessive information to the Commissioner's Office

Under the organisational and preventive requirements of the proposed legislation, designated CIOs need to reveal excessive amounts of information to the Commissioner's Office.

ARTICLE 19 finds it concerning that apart from leading to unwarranted surveillance, a possible security risk is posed by the Commissioner's Office storing unnecessarily large quantities of information that could be accessed by potential attackers.

[24] Background Paper, para 20.

In particular, we find the compelled disclosure of three categories of information problematic for the following reasons:

- First, sharing the design, configuration and security operations of computer systems could amount to disclosing the trade secrets of a commercial entity to the government.[25]

- Second, it is unclear why changes in "ownership" or "operatorship" of the CI need to be communicated every time if the organisation remains the same. The Background Paper suggests that liability falls on organisations and not individuals.[26]

ARTICLE 19's recommendation:
- Requirements to mandatorily disclose design, configuration and security operations of computer systems as well as the 'ownership' and 'operatorship' of a CI should be removed from the Proposed Framework.

Excessive investigation powers provided to the Commissioner's Office

The proposed legislation authorises the Commissioner's Office to require the production of any "relevant information" if it suspects that an offence under the legislation has occurred.[27] This production can be compelled without a Magistrate's warrant.

ARTICLE 19 finds that this wording provides exceptionally broad scope for discretion to the Commissioner's Office provides no clarity on what information "relevant" to an offence under the legislation may be. Without any guidelines or exemptions, this power could be used to compel disclosure of trade secrets of the business or personal data of employees or other individuals that the operator may be storing.

Going by the present wording, the Commissioner's Office could also demand sensitive details including encrypted data and passwords. There is no principle of data minimization that obliges the Commissioner to collect the least amount of data necessary to conduct the investigation.

We highlight that apart from violating the right to privacy and providing an opportunity for government surveillance, unrestrained procurement of information could also become a honeypot for potential cyber attackers if not secured effectively.

While the Commissioner's Office has significant powers to request for information or documents, there are no prescriptions binding the Commissioner's Office on how to

[25] Annex IV, para 8 (II).
[26] Background Paper, para 33.
[27] Annex II, Table II.

secure the documents or information from unwarranted or unauthorised interference or damage. While the legislation proposes to not tamper with personal data, it stipulates no provisions on how to separate personal data from data relevant to the investigation under the legislation or how to deal with personal data if authorities accidentally access it.

Further, we note that the proposed Appeals mechanism included in the proposal is very limited. It only allows an entity to appeal against a designation as a CIO[28] but does not enable the entity to challenge an investigation that is conducted in violation of standards established in the ICCPR or the Act itself.

ARTICLE 19's recommendations:

- The legislation should clarify what "information" the Commissioner's Office can seek from an entity when it suspects an offence has occurred. Personal information or trade secrets should be exempt unless there is a magistrate's warrant.
- The legislation should clearly stipulate that the Commissioner's Office is obliged to take appropriate and proportionate measures to securely store and prevent unwarranted access or interference with any document or information it seizes during an investigation. A code of conduct for the Commissioner's Office should separately be notified.
- The appeals procedure to appeal against an illegal investigation conducted by the Commissioner's Office should be amended.

Core issues delegated to subsidiary legislation by the Executive

According to the legislative proposal, core issues, including the clarifications to some of the vague and ambiguous questions referred to earlier in this Brief have been passed onto subsidiary legislation that will be issued by the Secretary for Security. By its very nature, subsidiary legislation does not require assent from the legislature and may not involve consultation with other stakeholders at all.

ARTICLE 19's recommendations:

- The primary legislation should include provisions on
  - The types of essential services that may be designated as critical infrastructure;
  - Information that may be required by the Commissioner's Office;
  - Any information, including material changes to Critical Computer Systems, that is required to be reported to the Commissioner's Office.

[28] Annex IV, para 17.

Conclusions

Organisations (both in the private and public sector) operating critical infrastructure should ensure that they have internal and external processes to both prevent and respond to cyber-attacks. Legislation stipulating these statutory obligations is an important step towards securing critical infrastructure in any country, including Hong Kong.

However, as ARTICLE 19 highlighted in this analysis, the proposed legislation includes a range of vague and broad provisions that reduce clarity and certainty, consequently having significant impacts on the freedom of expression and the protection of personal data.

Excessive discretion to the Commissioner's Office provides the government access to vast swathes of information that is not directly relevant to protecting critical infrastructure. This excessive access not only violates the right to privacy but also poses a security risk by itself as it provides a honeypot opportunity for potential attackers.

The recommendations presented outline specific provisions that need to be removed or clarified to ensure that the proposed legislation is in compliance with international human rights standards that are also part of Hong Kong's domestic law.

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 on Hong Kong and Global China, please contact Michael Caster at michael.caster@article19.org.