Hong Kong General Chamber of Commerce
香港總商會1861

香港總商會
香港金鐘道統一中心廿二樓
Hong Kong General Chamber of Commerce
22/F United Centre,
95 Queensway, Hong Kong
Tel (852) 2529 9229
Fax (852) 2527 9843
Email chamber@chamber.org.hk
www.chamber.org.hk

Helping Business since 1861

19 October 2022

Mr Allan Leung
Chairman
Sub-committee on Cybercrime
The Law Reform Commission
4th Floor, East Wing, Justice Place
18 Lower Albert Road
Central
Hong Kong

Dear Mr Leung,

Re: Consultation on Cyber-dependent Crimes and Jurisdictional Issues

The Hong Kong General Chamber of Commerce welcomes the opportunity to express our views on the subject consultation.

We support the Commission's proposals to introduce a bespoke cybercrime law that addresses the five types of cyber-dependent offences as stated in the consultation paper. Such a law, if so enacted, would demonstrate Hong Kong's determination to combat technology-induced crimes, which represent a clear and present danger to the business community especially against the backdrop of widespread digitization. The foregoing notwithstanding, we suggest that the proposed legislation should be designed in such a way that in safeguarding the public interest care and consideration would also be given to legitimate business needs.

Our comments on the consultative proposals are as detailed in the attached.

We hope you will give our comments your due consideration.

Yours sincerely,

George Leung
CEO

Encl.

The Law Reform Commission of Hong Kong Sub-Committee on Cybercrime
Consultation Paper "Cyber-dependent Crimes and Jurisdictional Issues" (Issued in June 2022)

Submission by The Hong Kong General Chamber of Commerce (HKGCC)

1. Introduction

1.1. HKGCC welcomes the opportunity to present its views on this consultation paper ("the CP").

1.2. Cybercrime presents a huge risk and potential cost to businesses. It requires them to incur costs in protecting themselves through technology and expertise, costs which SMEs in particular can ill-afford. Where (in spite of such protective efforts) a cyber-attack occurs, it can cause substantial disruption to normal business operations, resulting in extra costs and loss of revenue. Where it results in a data breach (the loss of personal data and confidential business information), additional costs may be incurred in regulatory or litigation proceedings, and the business's reputation may be damaged, resulting in lost revenue.

1.3. It is therefore important that Hong Kong has in place effective laws to combat cybercrime, and the CP is timely in this respect.[1]

1.4. The CP falls broadly into three parts:

- The proposed five new cyber-dependent offences;
- The proposed new jurisdictional rules associated therewith; and
- The proposed new sentencing rules.

1.5. We deal with each of these parts in turn. Finally, for ease of reference, we summarise our views on the CP's recommendations and consultation questions.

2. The proposed five new cyber-dependent offences

2.1. We agree that the basic questions in this consultation exercise should be, as stated in the CP, "*whether reform of the criminal law is needed, taking account various offence-creating and other relevant provisions applicable under existing legislation; and if so, what kind of reform is preferable*".[2]

[1] By "cybercrime", we mean what the CP refers to as "cyber-dependent crimes" and "cyber-enabled" crimes. Using the UK's terminology, the CP states that cyber-dependent crimes are crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime. Cyber-enabled crimes are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT. See CP Preface para 8.
[2] CP Preface para 14.

2.2. Assessing whether reform of Hong Kong *substantive* criminal law is needed - i.e., what conduct is or should be prohibited - implies a value judgment as to what sorts of conduct are unacceptable and should be criminalised. The CP states that "*there are five cyber-dependent offences which are the core species of cybercrime recognised globally that should be addressed*", namely:

(a) illegal access to program or data;

(b) illegal interception of computer data;

(c) illegal interference of computer data;

(d) illegal interference of computer system; and

(e) making available or possessing a device or data for committing a crime.[3]

2.3. Although the CP does not elaborate on how it has identified these five cyber-dependent offences, and other jurisdictions' criminal laws do not, and should not, determine what conduct Hong Kong should criminalise, we accept for the purpose of this submission that the activities described above should be classified as criminal under Hong Kong law, to the extent that this is not already the case. If this list of five cyber-dependent offences is not meant to be exhaustive, then, to protect the reputation of Hong Kong as an international financial centre and to squarely address growing online financial frauds, it may be worthwhile for the sub-committee to consider whether to add a category to address illegal schemes using computer, network or online platforms to perpetrate financial fraud on a grand scale.

2.4. The first of the basic questions raised in the CP is therefore whether, to criminalise these activities, "*reform of the criminal law is needed, taking account various offence-creating and other relevant provisions applicable under existing legislation*". This involves an assessment of whether, and if so to what extent, Hong Kong law already criminalises these activities. We summarise the position in this respect below, taking each of the proposed offences in turn.

2.4.1. Illegal Access to Computer Program or Data. As the CP notes, section 161 of the Crimes Ordinance already criminalises unauthorised access to computers where it is for certain illicit purposes as described in that section.[4] Although section 161 refers to a computer, and not to a computer program or data, this is immaterial, as illicit access to a computer program or data will inevitably involve illicit access to a computer. The CP recommends that, unlike under section 161, unauthorised access *in itself* should be a summary offence, irrespective of the intruder's intentions, unless the person gaining access without authorisation can rely on the proposed defence of "reasonable excuse" for this summary offence.[5] Whilst we agree with this recommendation in principle, a number of our

[3] CP Preface para 10.
[4] CP para 2.6.
[5] CP para 2.97.

members have pointed out that there are many real-life situations where IT specialists have to gain such access for legitimate purposes such as ensuring the security of computer systems, programs or data. While generally they would be given pre-approvals by the organisations concerned for such legitimate activities, and therefore should not be in a position of performing them without authorisation, there may be exceptional circumstances where the activity is not covered by the pre-authorisation, and where (due to urgency or other factors) it is not practicable to obtain authorisation in advance of such access. It is not clear whether such activities would be classified as a "reasonable excuse", which is a somewhat vague, subjective and uncertain concept. To give businesses greater comfort (and given that they would be subject to potential criminal liability if they wrongly assess that they have a reasonable excuse for unauthorised access), we would recommend that the Commission consult further with the industry with a view to formulating a non-exhaustive list of statutory examples of unauthorised legitimate activities which would fall within the definition of "reasonable excuse". We agree with the view in the CP that unauthorised access with the intention of carrying out further illicit activities should be an aggravated form of the offence.[6] Unauthorised access for illicit purposes is already criminalised by section 161 of the Crimes Ordinance, as noted above, but we appreciate that the scope of that section has been significantly narrowed by the Court of Final Appeal *Cheng Ka Yee* case, and that any vacuum (including other relevant existing offences or laws that do not carry the same maximum jail sentence and deterrence) could be filled and addressed by the new law.

2.4.2. Illegal Interception of Computer Data. We agree that illegal interception of computer data for a dishonest or criminal purpose should be a criminal offence.[7] We also agree that section 27 of the Telecommunications Ordinance does not sufficiently address this issue, as it only applies where there is damage, removal or interference with a telecommunications installation.[8] Moreover, we agree that many terms in the Telecommunications Ordinance have become outdated by technological development over the years. For example, this Ordinance refers to interception of a "message". The Ordinance was drafted at a time when computers were not prevalent, and therefore "message" could be interpreted as simply referring to SMS messages and phone calls, as opposed to interception of data packets, which individually is not a complete "message", e-mails and other electronic messages. We believe that this offence in particular requires to be carefully formulated and elaborated so that it is not interpreted too widely and does not catch legitimate activities. For example, what constitutes a "dishonest" purpose? Again, the use of statutory examples may be helpful.

[6] CP para 2.108.
[7] CP paras 3.92-3.99.
[8] CP paras 3.12-3.16.

2.4.3. Illegal Interference of Computer Data. The CP states that for this offence "*our consensus is that the existing regime is generally satisfactory*".[9] Our suggestion of a non-exhaustive list of statutory examples of "reasonable excuse" in paragraph 2.4.1 above (in relation to unauthorised access) also applies to this proposed offence.

2.4.4. Illegal Interference of Computer System. The CP states that overall, for this proposed offence, "*the existing statute has functioned satisfactorily*".[10] Our suggestion of a non-exhaustive list of statutory examples of "reasonable excuse" in paragraph 2.4.1 above (in relation to unauthorised access) also applies to this proposed offence.

2.4.5. Making available or possessing a device or data for committing a crime. The CP recognises that this proposed offence is to some extent covered by section 60, in combination with section 62, of the Crimes Ordinance. However, as noted in the CP, these provisions would only apply to things are intended to destroy or damage "property" (which may seem worded more narrowly than the Chinese text used in section 62(a), and hence might unintentionally be ruled as not covering intangible properties such as computer software), and therefore would not extend to all of the activities that are intended to be criminalised under the CP's proposals. Our suggestion of a non-exhaustive list of statutory examples of "reasonable excuse" in paragraph 2.4.1 above (in relation to unauthorised access) also applies to this proposed offence. Moreover, it should be made clear that an electronic service provider shall not be deemed to be "making available or possessing a device or data for committing a crime" merely because of the actions of a user of its service. There may also be situations where an organization's systems or devices are unknowingly used or hijacked by hackers to perform illegal activities: it should be made clear that the organization is not criminally-liable in these circumstances.

2.5. In conclusion, while existing Hong Kong legislation already criminalises to a large extent the activities that are subject to the CP's proposed new offences, there are certain gaps in the coverage of existing Hong Kong legislation in this respect. The question is whether these gaps should be filled by amending Hong Kong's existing legislation, in particular the Crimes Ordinance, or by enacting a new statute addressing cyber-dependent crimes as a whole, as the CP proposes. We deal with this issue in the next section.

2.6. Before doing so, it is necessary to deal with one procedural issue which is raised in this section of the CP. In the context of the discussion about unauthorised access to computer program or data, the CP proposes that the limit of six months under section 26 of the Magistrates Ordinance, which would apply to bringing a complaint against conduct that is subject to a summary offence under the new legislation proposed in the CP, be extended to two years.[11] The CP proposes that this extension should apply to all of the proposed new offences, not just

[9] CP para 4.99.
[10] CP para 5.62.
[11] CP para 2.123.

unauthorised access to computer program or data.[12] We support such extension, on the basis that cybercrime cases are often complex and require greater resources and time in deciding whether to bring a case to prosecution. However, it is also important that such cases are prosecuted as swiftly as possible, and therefore the maximum period of two years should be regarded as a safety net for the most complex cases, rather than the norm.

3. What kind of reform is preferable?

3.1. As noted above, the CP has identified the basic questions as "*whether reform of the criminal law is needed, taking account various offence-creating and other relevant provisions applicable under existing legislation; and if so, what kind of reform is preferable*".[13]

3.2. We have identified in the previous section certain gaps in existing Hong Kong criminal law, in respect of the five proposed cyber-dependent offences that the CP identifies. In other words, Hong Kong criminal law does not currently apply fully to all of the activities which the CP proposes be subject the new proposed criminal offences. This being the case, and in answer to the first of the two basic questions, reform is needed to fill the gaps.

3.3. The second basic question as identified in the CP is "what kind of reform is preferable"?

3.4. In this respect, the CP proposes a new piece of what it terms "bespoke" legislation to tackle cyber-dependent crimes, as opposed to amending the existing legislation that addresses these crimes. Its rationale for this proposal is as follows: "*At present, the legislation in Hong Kong does not have an ordinance applicable to cybercrime specifically. Different offences are covered in various Ordinances, some of which are outdated. In comparison, most of the other jurisdictions discussed above either have bespoke cybercrime legislation, or have a part of their codified law dedicated to cybercrime. We are attracted by those jurisdictions' approach because it helps ensure uniformity, comprehensiveness and consistency, e.g., as regards the definitions of the key concepts in this area*."[14]

3.5. Whilst we agree that there is scope for rationalising and consolidating existing legislative provisions, in particular to avoid unnecessary overlaps between the Crimes Ordinance and the Telecommunications Ordinance, the proposed new offences are to a large extent addressed by the existing legislation, as explained above. The gaps that exist (as compared to the proposed new offences) could arguably be addressed by amendments to the existing Ordinances (in particular the Crimes Ordinance), which may be a less onerous project than enacting a completely new statute.

3.6. However, on balance, we see greater benefit - particularly in terms of clarity for businesses, the enforcement authorities, and the courts - of a new statute

[12] See note 15 above.
[13] CP Preface para 14.
[14] CP para 2.89.

specifically devoted to cybercrimes. Such a statute would also send a powerful signal to potential cyber-criminals that Hong Kong treats this issue very seriously.

3.7. We therefore agree with the CP's proposal. However, as the CP emphasises, great care should be taken to ensure that the influence of the existing case law, where relevant, is not lost.[15]

4. The proposed new jurisdictional rules

4.1. Our members' views are divided on whether there should be specific jurisdictional rules for each of the proposed new cyber-offences. Those that support such rules argue that this should send a clear signal to potential offenders, thereby further increasing deterrence, as well as providing clarity to the courts and the legal profession. The contrary view is that it is inappropriate to single-out cyber-offences for special treatment in this respect, and that it is sufficient to leave it to the courts to adapt the rules of jurisdiction to suit evolving technological circumstances, as they have been doing, and to the existing rules in the Mutual Legal Assistance in Criminal Matters Ordinance.[16]

5. Sentencing

5.1. We agree with the CP's proposals to increase the existing maximum level of penalties, on the assumption that by doing so this will help deter and reduce cyber-dependent crimes. However, there is a growing body of academic literature suggesting that the likelihood of detection is an even greater deterrent to criminal activity than the severity of the penalty that may result.[17] We therefore suggest that continuing priority also be given to ensuring that sufficient resources are devoted to enforcement, and to investing in the necessary technology to keep one step ahead of the criminals.

6. Views on Recommendations and Consultation Questions

6.1. In this final section we respond briefly to each of the Sub-Committee's 16 Recommendations, noting that some of these recommendations are in fact consultation questions on which the Sub-Committee invites views. The rationale for our responses is explained in more detail above. We adopt the same numbering as the Recommendations:

1) We agree that unauthorised access to program or data should be a summary offence. Such unauthorised access for the purposes identified in the existing section 161 of the Crimes Ordinance should be an aggravated offence. The summary offence should be subject to a defence of "reasonable excuse". (Perhaps the phrase "unauthorised access" should be broadened to the phrase

[15] CP para 5.66.
[16] Cap 525.
[17] V. Wright "Deterrence in Criminal Justice: Evaluating Certainty vs. Severity of Punishment", The Sentencing Project Nov 2010; D.S. Nagin "Deterrence in the Twenty-First Century" Vol 42 No 1 Crime and Justice in America 1975-2025 (Aug 2013) 199; K Teodorescu, O, Plonsky, S Ayal and R Baran "Frequency of enforcement is more important than the severity of punishment in reducing violating behaviours" PNAS Vol 118 No 42 13 Oct 2021.

"use of" as in the case in New Zealand laws). We suggest that the Commission consult further with the industry in developing a non-exhaustive list of statutory examples of what would constitute a "reasonable excuse".

2) See 1) above.

3) We support the proposed extension of the limitation period from six months to two years.

4) We agree that there should be a new offence of illegal interception of computer data for a dishonest or criminal purpose.

5) There should be an exemption from the above offence for companies, either themselves or through their authorised security consultant, to intercept their own network purely for security threat detection.

6) Regarding illegal interference of computer data, the CP states that the existing regime under the Crimes Ordinance is working satisfactorily.[18] We therefore agree that the existing offence be transposed to the new statute. As with unauthorised access (see 1) above), we suggest that the Commission consult further with the industry in developing a non-exhaustive list of statutory examples of what would constitute a "reasonable excuse" for such interference.

7) Similarly, regarding illegal interference of computer system, the CP states "*case law suggests that, overall, the existing statute has functioned satisfactorily*". We therefore agree that the existing offence should be transposed to the new statute. As with unauthorised access (see 1) above) we suggest that the Commission consult further with the industry in developing a non-exhaustive list of statutory examples of what would constitute a "reasonable excuse" for such interference.

8) Scanning (or similar testing) of a computer system without the knowledge or authorisation of the owner of the target computer should be expressly criminalised.

9) We agree with the CP's proposals in respect of criminalising "making available or possessing a device or data for committing a crime". As with unauthorised access (see 1) above) we suggest that the Commission consult further with the industry in developing a non-exhaustive list of statutory examples of what would constitute a "reasonable excuse" for such activities.

10) There is a need to create an offence of "*knowingly making available or possessing computer data (the software or the source code), such as ransomware or a virus, the use of which can only be to perform a cyber-attack*". However, care should be taken to ensure that the law does not preclude the activities of companies conducting legitimate business such as software companies.

[18] CP para 4.99.

11) Our members' views are divided on the introduction of the proposed specific jurisdictional rules for cybercrimes, as suggested in recommendations 11-15.

12) See above.

13) See above.

14) See above.

15) See above.

16) We support the proposed increase in the maximum penalties for cyber-dependent crimes, for the reasons explained earlier in this submission.

HKGCC Secretariat
October 2022