THE LAW REFORM COMMISSION OF HONG KONG

REPORT ON CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

EXECUTIVE SUMMARY

*(This executive summary is an outline of the Report. Copies of the full Report can be downloaded from the website of the Law Reform Commission ("**LRC**") at https://www.hkreform.gov.hk or obtained from the LRC Secretariat at 9th Floor, Champion Tower, 3 Garden Road, Central, Hong Kong.)*

Consultation process

1. In July 2022, the LRC's Cybercrime Sub-committee ("**Sub-committee**") published the Consultation Paper on Cyber-dependent Crimes and Jurisdictional Issues ("**CP**"), pursuant to the following Terms of Reference:

> "*Having regard to the rapid developments associated with information technology, the computer and internet, and the potential for them to be exploited for carrying out criminal activities, to —*
>
> *(a) identify, from a criminal law point of view, the challenges to protection of individuals' rights and law enforcement arising from such developments;*
>
> *(b) review existing legislation and other relevant measures dealing with the challenges identified in (a) above;*
>
> *(c) examine relevant developments in other jurisdictions; and*
>
> *(d) make recommendations on possible law reforms to address the above matters.*"

2. The Sub-committee received 65 submissions during the public consultation. We are most grateful to all those who have responded ("**Respondents**"). A list of Respondents is at the Annex of the Report.

Structure of the Report

3. The Report relates to Part One of the Sub-committee's study.[1]

[1] Given the breadth of the Sub-committee's Terms of Reference, our study is divided into three phases. Part Two of the study will, subject to further discussion on its scope, cover cyber-enabled crimes. Part Three will deal with evidentiary issues and enforcement (procedural) issues.

There are nine chapters dealing with 16 Final Recommendations:

(a) Chapter 1 describes the ways in which international organisations and initiatives have categorised cybercrime. The "*offences against the confidentiality, integrity and availability of computer data and systems*" tackled by the Council of Europe's Convention on Cybercrime ("**Budapest Convention**")[2] broadly corresponds to the focus of the Report.

(b) Chapters 2 to 6 address the five cyber-dependent offences respectively, namely:

  (i) illegal access to program or data;

  (ii) illegal interception of computer data;

  (iii) illegal interference with computer data;

  (iv) illegal interference with computer system; and

  (v) making available or possessing a device, program or data for committing a cyber-related crime.

(c) Chapter 7 addresses the criteria for the Hong Kong court to assume jurisdiction.

(d) Chapter 8 tackles the issue of sentencing for the offences.

(e) Chapter 9 summarises our Final Recommendations.

Chapter 2: Illegal access to program or data ("Access Offence")

4. Recommendation 1 in the CP proposed that unauthorised access to program or data should be a summary offence, and that such access with intent to carry out further criminal activity should constitute an aggravated offence. The provisions should be modelled on sections 1, 2 and 17 of the Computer Misuse Act of England and Wales ("**CMA-EW**"). The Respondents generally agreed with Recommendation 1, but some doubted whether mere unauthorised access (ie "without criminal intent") should be criminalised. Others suggested clarifying the coverage of the "reasonable excuse" defence.

The mental element of the Access Offence[3]

5. It is useful to note that, as far as the *mens rea* of both the summary and aggravated offences are concerned, the prosecution must prove that at the time that the unauthorised access was made, the defendant knew that such access was unauthorised as is the case under section 1(1) of the CMA-EW.

---

2 Other categories of offences tackled by the Convention are computer-related offences (including computer-related forgery and fraud), content-related offences (including offences related to child pornography, and dissemination of racist and xenophobic material through computer systems) and offences relating to infringement of copyright and related rights.

3 Paras 2.18 to 2.24 of the Report.

6. We agree that the characteristics of the design and functioning of the cyberspace means that in certain widely accepted circumstances, authorisation to access program or data is implicitly granted by an online user, and the customary practices of not seeking prior express authorisation for access in situations that are generally accepted when using the cyberspace should continue to be tolerated. Further examples of circumstances involving implied authorisation include, but are not limited to, situations where access to program or data occurs by virtue of automatic connections by design and practical necessity.[4]

7. We therefore continue to be of the view that it is fair for the Access Offence to be premised on a person's knowledge that the access being performed is unauthorised. Ultimately, it will be a matter for the court to determine in all the circumstances of the case whether or not the evidence permits drawing the necessary inference of the defendant's knowledge.[5]

Mere unauthorised access should be an offence[6]

8. The Respondents' comments on the mental element of the Access Offence relate to the question of whether mere unauthorised access to program or data should be criminalised, which was discussed in the CP.[7]

9. The offence of mere unauthorised access under the CMA-EW was a response, because of the uncertainty and cost caused by hacking attempts, to the need to protect the integrity and security of computer systems from attacks from unauthorised persons, whatever their intention may be. Whether there is implied authorisation for access in a particular case would depend on the facts and circumstances as disclosed in the evidence.

10. As the internet permeates most aspects of public and private life nowadays, there is all the more a need to ensure the integrity of computer systems and networks against unauthorised access. The summary and aggravated offences are intended to operate together to provide an effective deterrent against all forms of unauthorised access. Thus, we maintain the view that mere unauthorised access to program or data should constitute an offence.

General reasonable excuse defence and specific defences[8]

11. We take the view that any attempt to provide an interpretation of "reasonable excuse" or, for that matter, a list of examples in the cybercrime legislation to illuminate the legislative intent may run the risk of narrowing the scope of the reasonable excuse defence inadvertently.

12. While we conclude that "reasonable excuse" should be left undefined, we recommend that specific defence(s) should be added alongside to exclude those types of behaviour that plainly should not, in our view, be

---

4 Paras 2.25 and 2.26 of the Report.
5 Please see the illustrations in paras 2.23 and 2.24 of the Report.
6 Paras 2.25 to 2.31 of the Report.
7 At paras 2.4, 2.5, 2.96 to 2.101.
8 Paras 2.32 to 2.34 of the Report.

regarded as illegal.[9] This will dispel the public's doubt as to whether certain activities fall within the ambit of the reasonable excuse defence, hence enhancing clarity of the new law.

Lawful activities conducted by law enforcement agencies ("LEAs")[10]

13. Some Respondents sought clarifications as to whether LEAs which access computer programs or data with or without warrant for criminal investigation purposes would be exempted from criminal liability. Since the Access Offence does not intend to affect any lawful activities conducted by LEAs, we recommend adding "without lawful authority" as an element of the offence. Whether "lawful authority" exists in a particular case is a question of fact. If a police officer has obtained a search warrant issued by a magistrate for conducting a search on a mobile phone or other electronic devices, or has a reasonable basis for conducting a warrantless search on these devices such that the requirements laid down in *Sham Wing Kan v Commissioner of Police*[11] are satisfied, there is "lawful authority" for the access to program or data. Moreover, access to program or data made, with or without lawful authority, in exigent situations may, in its own right, fall within the reasonable excuse defence. Therefore, even for law enforcement purposes, we consider it appropriate that access to program or data without warrant, when it cannot be justified, should constitute the Access Offence.

14. Our **Final Recommendation 1** is thus as follows:

> *"We recommend that:*
>
> *(a) Subject to a statutory defence of reasonable excuse, unauthorised access to program or data without lawful authority should be a summary offence under the new legislation.*
>
> *(b) The mens rea of the proposed offence are that:*
>
> *(i) the defendant intends to secure access to the program or data, or intends to enable such access to be secured; and*
>
> *(ii) the defendant knows that the intended access to the program or data was unauthorised when he makes the access.*
>
> *(c) Unauthorised access to program or data with intent to carry out further criminal activity should constitute an aggravated form of the offence attracting a higher sentence under the new legislation.*

---

9 See paras 18 to 33 of this Summary.
10 Paras 2.35 to 2.37 of the Report.
11 [2020] 2 HKLRD 529, CACV 270/2017 (date of judgment: 2 April 2020).

(d) The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the Computer Misuse Act of England and Wales."

Consultation question in Recommendation 2

15. Recommendation 2 in the CP invited submissions on whether there should be any specific defence or exemption for unauthorised access. The question consisted of several parts, namely:

"*(a) If the answer is yes for cybersecurity purposes, in what terms? For example:*

(i) should the defence or exemption apply only to a person who is accredited by a recognised professional or accreditation body?

(ii) if the answer to subparagraph (i) is yes, how should the accreditation regime work …?

(iii) alternatively, if an accreditation regime is not preferred, should the new bespoke cybercrime legislation prescribe the requirements for putative cybersecurity professionals to invoke the proposed defence or exemption for cybersecurity purposes? If so, what should these requirements be?

(b) Should the defence or exemption apply to non-security professionals (please see the examples in Recommendation 8(b))?"

16. An overwhelming majority of the Respondents supported a specific cybersecurity defence as they saw value in the work of white hat hackers and other cybersecurity professionals in detecting cybersecurity threats and vulnerabilities. On the other hand, the few Respondents who opposed such a specific defence did not favour what would effectively be the creation of a "privileged class". They opined that the specific defence should be available to everyone, but not only to persons accredited by a recognised professional or accreditation body regardless of intention.

17. In line with the general consensus that a specific defence for unauthorised access is desirable, a clear majority of the Respondents agreed that an accreditation regime should be put in place. Some agreed that the establishment of an accreditation body and a properly recognised cybersecurity profession would bring long-term benefits to Hong Kong.

Specific defence for accredited cybersecurity practitioners[12]

18. We consider it reasonable and pragmatic to create a specific defence for a defined category of persons within the information technology

[12] Paras 2.63 to 2.74 of the Report.

industry. We propose that there should be a specific defence or exemption for accredited cybersecurity practitioners who act for a genuine cybersecurity purpose. The defendant's purpose and conduct must, however, be reasonable having regard to all the circumstances.

Accredited or licensed cybersecurity practitioners

19. Given the level of intrusion of access to program or data made for cybersecurity purposes and their broad notion, we consider that access for cybersecurity purposes should only be made by licensed or accredited practitioners, ie those who are expected to possess a certain level of professional expertise and standard of integrity.

20. There should be an independent system for accrediting cybersecurity practitioners and overseeing their disciplinary matters. We agree with the Respondents that an accreditation regime may be implemented in different ways. The designation of a statutory authority is one way whereas recognition of members of reputable information technology professional bodies or international information technology associations is another.

21. Depending on the approach taken, the impact of the accreditation regime on the cybersecurity industry and cyberspace users is not limited to the supply and the cost of cybersecurity professionals. The detailed implementation issues of an accreditation regime are essentially ones of Government policy. Such details (including the requirements for accreditation as a cybersecurity professional, record-keeping obligations on the part of the practitioners, questions as to whether the accreditation body is to be managed by the information technology industry or other authorities, and how the accreditation regime should be financed) would be appropriate to be left to the Government.[13]

Genuine cybersecurity purpose

22. An additional requirement for "genuine cybersecurity purpose" would mean that the accreditation or identity of the defendant should not be conclusive. We so recommend with the intended outcome that an accredited cybersecurity practitioner who, for example, accessed the data on the phone of his child other than for genuine cybersecurity purposes would have to fall back on the defence of access for protecting the interests of a child discussed in paragraphs 24 to 27 below.

The defendant's conduct must be reasonable having regard to all the circumstances

23. We also propose to incorporate the requirement of "reasonableness" into the specific defence so as to provide for safe and consistent parameters delineating conduct that would be acceptable to a reasonable person. If any code of ethics is promulgated by the accreditation

[13] To facilitate the Government's consideration of the accreditation regime, we have set out our observations on the proposal of accreditation and its potential implications in paras 2.67 to 2.70 of the Report.

body, the court may certainly make reference to the code when assessing the reasonableness of a defendant's conduct.

Other specific defences to the Access Offence

Access for protecting the interests of a child[14]

24. During the consultation exercise, there were comments as to whether parents should be allowed to access their children's computers. We find it sensible to explicitly carve out access for the purpose of protecting children under 16 from the Access Offence. While the specific defence may diminish the privacy right of children under 16, given the high internet penetration rate among them, we consider that the existence of the defence would be consistent with the principle of protecting their interests.

25. To maximise the protection, the proposed defence is predicated on the subjective purpose of the person who sought such access and not on the relationship between that person and the child.

26. To avoid abuse of this defence, the act of access should be restricted to what is reasonably necessary for protecting the interests of a child, having regard to all circumstances of the case. We have identified the following two options of formulating this defence:

(a) A broader defence: Access to program or data for protecting the interests of a child; and

(b) A narrower defence: Access to program or data for preventing physical, emotional or psychological harm to a child.

27. We have analysed the pros and cons of both options in the Report.[15] The first (broader) option is preferred by a narrow majority in the Sub-committee. As the Government may further consult the public should it decide to implement our recommendation, the issue is best left for the decision of the Government having regard to the sentiments in society.

28. Since an adult with mental disability may be prone to exploitation, we further recommend that the specific defence for unauthorised access to program or data should be extended to the protection of a vulnerable person, ie a mentally disordered person [16] and a mentally handicapped person[17] as defined in the Mental Health Ordinance (Cap 136).

---

14 Paras 2.75 to 2.91 of the Report.

15 At paras 2.85 to 2.87.

16 Under s 2 of the Mental Health Ordinance ("**MHO**"), a "*mentally disordered person*" means "*a person suffering from mental disorder*".

17 Under s 2 of the MHO, a "*mentally handicapped person*" means "*a person who is or appears to be mentally handicapped*".

Access for genuine research purposes[18]

29. A number of information technology related bodies suggested exempting access to program or data made for the purposes of research, analysis or testing tester-owned devices or targets performed in a controlled environment.

30. We agree that it would be reasonable to provide a specific defence for access to program or data made for research purposes since such research could yield useful analysis or information.[19] We opine that the proposed defence, modelled on that for the various child pornography offences,[20] may be formulated as access to program or data made for a genuine educational, scientific or research purpose. To avoid abuse, one of the requirements of the defence is that the access must be reasonable and no more than is necessary for achieving the relevant purpose. This "reasonableness" requirement serves as an objective yardstick for determining whether the access made by a defendant is proportionate or reasonable.

Defences under section 64(2) of the Crimes Ordinance ("CO") for the offences of illegal interference with computer data and computer system ("Interference Offences")[21]

31. As interference with computer data and/or computer system normally only occur upon access to program or data, we take the view that the consent defence and the property protection defence under section 64(2) of the CO ("**S64(2)**")[22] (which apply to the Interference Offences)[23] should likewise apply to the Access Offence.

32. Given that the consent defence and the property protection defence both apply to the Interference Offences, we take the view that uniform treatment should apply to the defences to the Access Offence. When transposing the defences under S64(2) to the cybercrime legislation, we propose to set a higher bar for invoking the defence by incorporating an objective test into them, ie:

---

18 Paras 2.92 to 2.94 of the Report.

19 Eg a researcher or cybersecurity practitioner ascertaining the number of unprotected computers in Hong Kong.

20 Prevention of Child Pornography Ordinance (Cap 579), ss 4(2)(a) and (3)(a).

21 Paras 2.95 to 2.102 of the Report.

22 Under s 64(2) of the Crimes Ordinance (Cap 200) ("**CO**"), a defendant charged with criminal damage is treated as a having a lawful excuse:

(a) if, at the time of the act(s) alleged to constitute the offence, the defendant believed that the person(s) whom the defendant believed to be entitled to consent to the destruction of or damage to the property had so consented, or would have so consented to it if the person(s) had known of the destruction or damage and its circumstances ("**consent defence**"); or

(b) if the defendant destroyed or damaged, or threatened to destroy or damage the property, or in the case of a charge under s 62, intended to use or cause or permit the use of something to destroy or damage the property, in order to protect property (whether belonging to himself or another), and at the time of the act(s) alleged to constitute the offence, the defendant believed—

(i) that the property was in immediate need of protection; and

(ii) that the means of protection adopted or proposed to be adopted were or would be reasonable having regard to all the circumstances ("**property protection defence**").

23 See paras 62 to 64 of this Summary.

(a) in the case of the consent defence, the defendant must reasonably believe that there was, or would be, consent to his access to the program or data; and

(b) in the case of the property protection defence, the defendant must reasonably believe that the property was in immediate need of protection.

33. The above adjustment would align the consent defence and the property protection defence with other specific defences that we recommend for the Access Offence, ie all defences will consistently adopt the requirement of "reasonableness".

34. We therefore make our **Final Recommendation 2** as follows:

> *"Apart from the statutory defence of reasonable excuse, we recommend that for the proposed offence of illegal access to program or data:*
>
> *(a) There should be a specific defence for unauthorised access for cybersecurity purposes with the following conditions:*
>
> *(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);*
>
> *(ii) The defendant must act for a genuine cybersecurity purpose; and*
>
> *(iii) The defendant's conduct must be reasonable having regard to all the circumstances.*
>
> *(b) There should be a specific defence for unauthorised access for the protection of the interests of a child under the age of 16 and a vulnerable person (ie a mentally disordered person or a mentally handicapped person as defined in the Mental Health Ordinance (Cap 136)):*
>
> *(i) The defence is based on the subjective purpose of the person making the access to the program or data of a child or vulnerable person (ie for the protection of the interests of the child or vulnerable person), but not the relationship between the person and the child or vulnerable person.*
>
> *(ii) The access to program or data made by a defendant must be reasonable having regard to all the circumstances.*

(c) *There should be a specific defence for unauthorised access for educational, scientific or research purposes. The access to program or data made by a defendant must be reasonable having regard to all the circumstances.*

(d) *The defences to the offences of illegal interference with computer data and illegal interference with computer system under section 64(2) of the Crimes Ordinance (Cap 200) ("**S64(2)**") should also be available to the offence of illegal access to program or data.*

(i) *The two defences under S64(2) cover situations where a defendant:*

(1) *accessed program or data in the belief that his act was, or would be, consented to; or*

(2) *accessed program or data in the belief that the property was in immediate need of protection, and the means of protection adopted was reasonable having regard to all the circumstances.*

(ii) *The defendant's belief under both the consent defence and the property protection defence must be reasonably held."*

Extending the limitation period in summary proceedings for the five cyber-dependent offences[24]

35. Section 26 of the Magistrates Ordinance (Cap 227) stipulates a general limitation period of six months to commence prosecution. As six months may be insufficient for investigating cybercrime cases, [25] Recommendation 3 in the CP proposed that the new cybercrime legislation extend the limitation period to two years.

36. The majority of the Respondents supported Recommendation 3, while a few preferred to keep the six-month period in order to encourage vigilance on the part of LEAs. We wish to clarify that Recommendation 3 only seeks to extend the limitation period to ensure that the ensuing prosecution of an investigation of alleged offences which cannot reasonably be completed within the default six months given the inherent complications is not time-barred, and not because of the lack of confidence that LEAs are capable of dealing with a cybercrime case as swiftly as is fair and possible.

37. Thus, we recommend retaining Recommendation 3 in the CP as our **Final Recommendation 3**:

---

24 Paras 2.106 to 2.110 of the Report.

25 As explained in the CP, a victim may only report a cybercrime case to the Police two or three months after it occurs or, worse still, by the time when an incident is discovered, six months have already lapsed. The Police may need a few months to obtain log records from an internet service provider ("**ISP**"). Analysis of the log records may require a few more months. Further time to reach a prosecutorial decision must be factored in.

"*We recommend that the limitation period applicable to a charge for any of the proposed offences by way of summary proceedings should be two years after discovery of any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence, notwithstanding section 26 of the Magistrates Ordinance (Cap 227).*"

Chapter 3: Illegal interception of computer data

38. A clear majority of the Respondents supported Recommendation 4 in the CP which proposed that unauthorised interception, disclosure or use of computer data carried out for a dishonest or criminal purpose should be an offence. Some information technology bodies were, however, concerned that the proposed interception offence would bring potential uncertainties to the legitimate acts involving interception carried out by cybersecurity practitioners, such as network intrusion detection, penetration test and network monitoring for discovering attacks or analysing network traffic.

The requirement "for a dishonest or criminal purpose" is appropriate[26]

39. As with the CP,[27] we emphasise that we fully acknowledge that the operation of modern networking devices has an element of interception and data interception may occur in various ways under the normal practice of cybersecurity companies. This was why the CP recommended interception "*for a dishonest or criminal purpose*" as a requirement. This mental element intends to impose a high threshold to avoid creating an offence whose scope is unjustifiably broad in order that data interception which normally takes place under the ordinary use of computer network technology will not be criminalised.

40. We also acknowledge that some uncertainty may arise in respect of certain borderline behaviours. In those cases, whether a person is guilty of the interception offence would depend on the specific circumstances of the case, including the defendant's purpose of interception and the data involved.[28]

41. The merit of the criterion "*for a dishonest purpose*" is that the court may consider a multitude of factors in deciding whether the conduct of interception fell within the acceptable realm. On balance, we conclude that the *mens rea* threshold "*for a dishonest or criminal purpose*" is appropriate as it can avoid catching the innocent interceptors inadvertently.

Unauthorised disclosure or use of data[29]

42. Recommendation 4 in the CP intended to prohibit unauthorised disclosure or use of "intercepted data", given that the subsequent disclosure or use of intercepted data may give rise to privacy concerns and other potential

---

26 Paras 3.30 to 3.36 of the Report.
27 At para 3.97.
28 For examples given, see paras 3.34 and 3.35 of the Report.
29 Paras 3.25 to 3.29 of the Report.

issues.[30] On further reflection, an offence based on unauthorised disclosure or use of "any data" (which is not limited to intercepted data) for a dishonest or criminal purpose may be too broad since the offence will essentially apply to all kinds of data encountered in our digital everyday life.

43. Given the wide implications of a general offence of unauthorised disclosure or use of computer data,[31] it would be prudent to study this topic in depth in Part Two[32] of our study before we express any settled view as to whether a new offence in this regard should be recommended, and if so, how. For example, further considerations may be given to whether such offence should be confined to intercepted data as some may hold the view that if a person discloses or uses computer data "*for a dishonest or criminal purpose*", the conduct should by itself be culpable, no matter whether the data was obtained by authorised or unauthorised interception, or any other means.

44. For these reasons, our **Final Recommendation 4** is as follows:

> *"We recommend that:*
>
> *(a) Unauthorised interception of computer data carried out for a dishonest or criminal purpose should be an offence under the new legislation.*
>
> *(b) The proposed offence should:*
>
> *(i) protect communication in general, rather than just private communication;*
>
> *(ii) apply to data generally, whether it be metadata or not; and*
>
> *(iii) apply to interception of data en route from the sender to the intended recipient, ie both data in transit and data momentarily at rest during transmission.*
>
> *(c) The proposed provision should, subject to the above, be modelled on section 8 of the Model Law on Computer and Computer Related Crime, including the mens rea (ie to intercept "intentionally").*
>
> *(d) The implications of unauthorised disclosure or use of computer data, intercepted or otherwise, should be studied*

---

30 Eg financial loss may occur to the holder of a credit card if its details intercepted during their transmission to the vendor in an e-commerce transaction are wrongfully used. See paras 3.92 and 3.94 of the Consultation Paper.

31 An offence on unauthorised disclosure or use of computer data, insofar as it involves personal data, is more a matter within the purview of the Office of the Privacy Commissioner for Personal Data ("**PCPD**"). In the most recent legislative amendment exercise in 2021 (ie the enactment of the Personal Data (Privacy) (Amendment) Ordinance 2021), the PCPD specifically focused on the doxxing offences in a bid to combat disclosure of personal data without consent (see the long title of that Amendment Ordinance). The *mens rea* for the doxxing offences is highly specific and confined in scope.

32 Part Two, subject to further discussion in due course on its scope, will cover cyber-enabled crimes, which are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of information and communications technology. See para 8 of the Preface of the Report.

in greater detail in Part Two of our study before we express any settled view as to whether any new offence in this regard should be recommended, and if so, how."

Defences to the offence[33]

45. Recommendation 5 in the CP invited submissions on the following questions, which overlap to a certain extent:

> *"(a) Should there be a defence or exemption for professions who have to intercept and use the data intercepted in the course of their ordinary and legitimate business? If the answer is yes, what types of professions should be covered by the defence or exemption, and in what terms (eg should there be any restrictions on the use of the intercepted data)?*
>
> *(b) Should a genuine business (a coffee shop, a hotel, a shopping mall, an employer, etc) which provides its customers or employees with a Wi-Fi hotspot or a computer for use be allowed to intercept and use the data being transmitted without incurring any criminal liability? If the answer is yes, what types of businesses should be covered, and in what terms (eg should there be any restrictions on the use of the intercepted data)?"*

46. The majority of the Respondents considered that there should be a defence for professions which have to intercept and use the data intercepted in the course of their ordinary and legitimate business. They suggested specific categories of professions or activities that should be covered by the defence.[34] There were mixed responses as to whether a genuine business should be allowed to intercept and use the data being transmitted without incurring criminal liability.

47. After carefully reflecting on the Respondents' submissions and the elements of the proposed offence of illegal interception of computer data, we consider that it is not necessary to put in place any specific defences or exemptions for those who have to, in the course of their ordinary and legitimate business, intercept and use computer data. The main reasons are:

(a) in theory, it does not seem logical to provide any defence to an offence which already expressly requires proof of a "*dishonest or criminal purpose*";

---

33 Paras 3.54 to 3.64 of the Report.

34 Para 3.54 of the Report. Six categories were proposed, namely (a) ISPs, (b) Institutions whose daily work frequently requires use and handling of intercepted data; (c) Companies which intercept their own network purely for security threat detection; (d) LEAs' investigation of criminal activities and matters of national security; (e) Whistleblower activities carried out in good faith, for public interest, or for collecting evidence for future legal proceedings; and (f) Business or organisations which hold a legitimate belief that activities are being carried out against their interest.

(b) in context, if a profession or genuine business intercepts computer data for a dishonest or criminal purpose, it should not be exempted from criminal liability merely because it runs a particular profession or business;

(c) giving a defence to institutions whose daily work frequently requires use and handling of intercepted data would in effect give some professions or businesses (such as a private investigation agency or a media agency) a carte blanche licence to intercept data; and

(d) providing defences to specific categories of professions or persons in the bespoke cybercrime legislation may imply that data interception by other professions or persons not specified in the legislation will always be unlawful, thereby bringing more confusion than clarity to the law.

48. We conclude that any business that wishes to intercept the data of patrons or consumers may obtain the latter's authorisation for intercepting data. If the intercepted data is used for a purpose other than the authorised purpose, it would be up to the court to decide on the evidence of a particular case whether the interception is carried out for a dishonest or criminal purpose.

49. We therefore make our **Final Recommendation 5** as follows:

> *"We do not recommend any defence or exemption for professions or genuine businesses (eg coffee shops, hotels, shopping malls, employers) which intercept or use computer data in the ordinary course of their operation. The mens rea requirement of interception of computer data for a dishonest or criminal purpose has mitigated the need to provide for any specific defence or exemption."*

Chapter 4: Illegal interference with computer data

50. The vast majority of the Respondents supported Recommendation 6 in the CP which proposed making intentional interference with computer data without lawful authority or reasonable excuse an offence by transposing the current regime on "*misuse of a computer*" under sections 59(1A), 60 and 64(2) of the CO to the new legislation.

The mental elements of the proposed offence[35]

51. Some information technology-related bodies opined that "malice" should be a requisite element of the proposed offence. A legal professional body sought clarifications as to why the mental requirement of "recklessness" is appropriate or relevant.

---

[35] Paras 4.14 to 4.22 of the Report.

52. "Malice" is an archaic term that caused difficulties for interpretation.[36] Besides, the existing offence of criminal damage under section 60 of the CO, which extends to "*misuse of a computer*" by virtue of section 59(1)(b) and (1A),[37] adopts the mental elements of "intention" and "recklessness". As a general principle, the concept of "recklessness" under criminal law requires proof that a defendant was aware of the risk and that, in the circumstances known to him, it was unreasonable to take the risk.[38] It has been adopted as a fault element alongside "intention" or "knowledge" in many criminal offences.

53. In the context of cybercrime, the concept of "recklessness" underscores the importance of exercising care and responsibility in the use of computer technology, ie a person must be vigilant to the possible consequences of his online actions, including the impact that they may have on others.

54. Accordingly, we recommend retaining the *mens rea* elements in Recommendation 6(b)(ii), ie "*intent or recklessness, but not malice*" for the offence of illegal interference with computer data.

The aggravated offence and acts endangering national security

55. A Respondent suggested that on top of the elements stated in section 60(2) of the CO, "*any act or activity intending to endanger national security or being reckless as to whether national security would be thereby endangered"* should also be regarded as an aggravated offence.

56. Our analysis is detailed at paragraphs 4.23 to 4.31 of the Report. In gist, we observe that a number of provisions of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**NSL**") seem wide enough to embrace acts of illegal interference with computer data (and computer system) already. Among them, Article 24(4) of the NSL distinctly covers acts of interference with, and damage to, the electronic control systems of the internet. Since the NSL forms an essential part of the fabric of our legal system, it is important that the bespoke cybercrime legislation does not create any inconsistencies or conflict, even if unintended, with the NSL.

---

[36] The Law Commission of England and Wales saw difficulty with the term "malice" when it reviewed the offences of damage to property, which led to the enactment of the Criminal Damage Act 1971 (on which the criminal damage offence in Hong Kong was modelled). See Law Commission, *Criminal Law Report on Offences of Damage to Property* (1970), Law Com No 29, at para 44.

[37] Section 59(1A) of the CO defines "*misuse of a computer*" to mean the following acts, among which paras (b) and (c) are the most relevant to illegal interference with computer data (as opposed to illegal interference with computer system):

"(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;

(b) to alter or erase any program or data held in a computer or in a computer storage medium;

(c) to add any program or data to the contents of a computer or of a computer storage medium,

and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it."

[38] *Archbold Hong Kong 2025*, at para 16-40, discussing *R v G* [2004] AC 341 decided in the context of the offence of criminal damage and subsequent jurisprudential developments.

57. In March 2024, the Safeguarding National Security Ordinance ("**BL 23 legislation**") was enacted. Offences under the BL 23 legislation include, *inter alia*, the offence of sabotage activities carried out with intent to endanger national security (or being reckless as to whether national security would be endangered), damaging or weakening public infrastructure (which includes any software constituting the infrastructure),[39] and more specifically, the offence of doing an act in relation to a computer or electronic system with intent to endanger national security without lawful authority.[40]

58. Given the manner in which Article 23 of the Basic Law is now implemented by way of local legislation (which includes the introduction of a specific offence covering national security risks in cyberspace), we consider that the Government would be better placed to evaluate the adequacy or otherwise of all extant national security-related offences holistically and consider our recommendations to see if any refinements should be proposed.

Specific defences

Interference with computer data for cybersecurity purposes[41]

59. As interference with computer data (or computer system) normally occurs upon access to program or data, we have considered whether the defences applicable to the Access Offence discussed in Chapter 2 should likewise apply to the Interference Offences. The logical conclusion is that the defence of interference with computer data for cybersecurity purposes[42] should apply to both types of offences and we so recommend.

Interference with computer data for protecting the interests of a child or vulnerable person [43]

60. While a parent, guardian or other persons may require access to the program or data of a child or vulnerable person to safeguard him from online harm, we understand that such access does not entail any alteration or interference with computer data (or computer system). Also, granting a person access to any program or data in no way implies that the person is authorised to alter or otherwise tamper with the data. Thus, we consider that it is not necessary to provide a specific defence to the Interference Offences for the purpose of protecting the interests of a child or vulnerable person.

Interference with computer data for genuine research purposes[44]

61. We find it inconceivable that the conduct of genuine research would necessitate interference with computer data (or computer system). Thus, it is not necessary to provide a specific defence to exempt illegal interference with computer data (or computer system) carried out for genuine research

---

39 Safeguarding National Security Ordinance, s 49 (sabotage endangering national security).
40 Same as above, s 50 (doing acts endangering national security in relation to computers or electronic systems).
41 Paras 4.34 to 4.35 and 5.23 to 5.24 of the Report.
42 See paras 18 to 23 of this Summary.
43 Paras 4.36 to 4.37 and 5.25 to 5.26 of the Report.
44 Paras 4.38 and 5.27 of the Report.

purposes.

Transposing the defences under S64(2) of the Crimes Ordinance[45]

62. Recommendation 6 of the CP proposed to adopt the two "lawful excuses" currently provided for under S64(2) of the CO. As the Respondents generally welcomed the adoption of the existing regime under the CO for the purposes of the Interference Offences, we recommend maintaining Recommendation 6, subject to the inclusion of an objective test into the consent defence and the property protection defence (as in the case of the Access Offence discussed in paragraph 32 above).

63. We noted that the "lawful excuse" under the existing S64(2)(b) of the CO is confined to property protection only and does not cover the protection of human lives. We have considered whether the specific defence to the Interference Offences should provide for the protection of life and/or prevention of physical harm to a person. We believe that the general "reasonable excuse" defence under Recommendation 6 could cater to situations where a person interfered with computer data (or computer system) for the protection of life and/or prevention of physical harm, so it might not be necessary to propose another defence for this specific purpose. We are content to maintain the status quo of S64(2)(b) in this respect.

64. Our **Final Recommendation 6** is as follows:

> *"We recommend that:*
>
> *(a) Subject to a statutory defence of reasonable excuse, intentional interference (damaging, deletion, deterioration, alteration or suppression) with computer data without lawful authority should be an offence under the new legislation.*
>
> *(b) The new legislation should adopt the following features under the Crimes Ordinance (Cap 200):*
>
> *(i) the actus reus under section 59(1A)(a), (b) and (c);*
>
> *(ii) the mens rea under section 60(1) (which requires intent or recklessness, instead of malice);*
>
> *(iii) the two defences identified under section 64(2) subject to such refinement as may be required for their proper articulation in the light of the reformulation of the offence under paragraph (a) above, while preserving any other lawful excuse or defence recognised by law; and*
>
> *(iv) the aggravated offence under section 60(2).*

[45] Paras 4.39 to 4.44 and 5.28 of the Report.

(c) The two defences covered under section 64(2) apply to situations where a defendant:

(i) interfered with computer data in the belief that his act was, or would be, consented to; or

(ii) interfered with computer data in the belief that the property was in immediate need of protection, and the means of protection adopted was reasonable having regard to all the circumstances.

The defendant's belief under both the consent defence and the property protection defence must be reasonably held.

(d) The above provisions regarding 'misuse of a computer' should be separated from the offence of criminal damage and adopted in the new legislation, while deleting section 59(1)(b) and (1A) of the Crimes Ordinance (Cap 200).

(e) There should be a specific defence for illegal interference with computer data for cybersecurity purposes with the following conditions:

(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);

(ii) The defendant must act for a genuine cybersecurity purpose; and

(iii) The defendant's conduct must be reasonable having regard to all the circumstances."

Chapter 5: Illegal interference with computer system

65. As Hong Kong law currently addresses illegal interference with computer data and that of computer system by treating both as "*misuse of a computer*" (which is a form of criminal damage), Recommendation 7 of the CP proposed to phrase the provisions regarding illegal interference with computer data and that of computer system in the same way.

66. As the offences of illegal interference with computer system is closely related to that of illegal interference with computer data, Recommendation 7 was likewise supported by an overwhelming majority of the Respondents, whose responses on Recommendation 7 were largely similar to those on Recommendation 6. We repeat our analysis in paragraphs 51 to 63 above and make our **Final Recommendation 7** as follows:

"We recommend that:

(a) The proposed provisions regarding the illegal interference with computer data and computer system should be phrased in the same way.

(b) Sections 59(1A) and 60 of the Crimes Ordinance (Cap 200) suffice to prohibit the illegal interference with computer system and should also be adopted in the new legislation.

(c) The new legislation should retain the breadth of the existing law and should not be too restrictive, while clarifying the phrase 'misuse of a computer' as appropriate (eg incorporating the notion 'impair the operation of any computer').

(d) The proposed offence of illegal interference with computer system should, for example, apply to a person who intentionally or recklessly:

(i) attacked a computer system, whether successful or not (criminal liability should not depend on the success of an interference);

(ii) coded a software with a bug during its manufacture; and

(iii) changed a computer system without authorisation, knowing that the change may have the effect of preventing access to, or proper use, of the system by legitimate users."

67. Recommendation 8 of the CP mainly sought the public's views on whether the following activities should qualify as a lawful excuse with regard to the proposed offence of illegal interference with computer system:

(a) scanning (or any similar form of testing) of others' computers;

(b) actions by non-security professionals, such as web scraping (ie the process of using bots to extract content and data from a website) by robots or web crawlers (ie an internet bot that systematically browses webpages for the purpose of indexing) initiated by internet information collection tools, such as search engines, to collect data from servers without authorisation.

Recommendation 8(a): Specific defences[46]

68. Given the close relationship between the Interference Offences, we similarly recommend that interference with computer system for cybersecurity purposes should be a defence to the offence of illegal interference with computer system. Our reasoning for the specific defences to

[46] Paras 5.23 to 5.28 of the Report.

the offence of illegal interference with computer data in paragraphs 59 to 63 above equally applies to the offence of illegal interference with computer system.

Recommendation 8(b): Not necessary to propose defence for non-security professionals[47]

69. Some activities which do not necessarily serve any cybersecurity purposes are inherent in the operation of cyberspace or interaction between computer devices or systems. It would be impossible to exhaustively set out all the legitimate activities in cyberspace which we consider to be part and parcel of our digital life and hence acceptable. This is particularly so given the quick pace of technological development. We agree with the CP that when a person opts to connect himself to the internet, he or she is taken to have impliedly consented to any interaction that can reasonably be expected to occur in the use of cyberspace. We should avoid inadvertently outlawing some widely accepted internet practices that should be permitted by virtue of the normal functioning of the internet or computer systems. Furthermore, the cybercrime legislation in other countries has not provided any specific defences for non-security professionals (such as the operation of search engines) although they have enacted the offence of illegal interference with computer system and the Access Offence.

70. Thus, we consider it unnecessary to provide a specific defence for non-security agents encountered in the day-to-day operation of cyberspace, which should be distinguishable from a cyber-attack.[48]

71. Our **Final Recommendation 8** is as follows:

> *"(a) There should be a specific defence for illegal interference with computer system for cybersecurity purposes with the following conditions:*
>
> *(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);*
>
> *(ii) The defendant must act for a genuine cybersecurity purpose; and*
>
> *(iii) The defendant's conduct must be reasonable having regard to all the circumstances.*
>
> *(b) It is not necessary to provide any specific defence to the proposed offence of illegal interference with computer system for non-security professionals (such as web scraping by robots or web crawlers initiated by internet*

---

47 Paras 5.29 to 5.33 of the Report.

48 Eg when 10,000 emails are sent to a specific mailbox within a minute to overwhelm it and its corresponding server.

information collection tools to collect data from servers without authorisation by connecting to designated protocol ports) since activities which form part of the normal functioning of the internet or computer systems should continue to be allowed under the principle of implied authorisation."

Chapter 6: Making available or possessing a device, program or data for committing a cyber-related crime

72. Recommendation 9 of the CP, which proposed a distinct offence of making available or possessing a device or data for committing a crime, has sparked much debate among the public. A number of Respondents raised concerns about the breadth of the basic offence. To address these concerns, we have reviewed Recommendation 9 holistically and propose the following amendments:

Including "program" in the offence, ie "device, program and data"[49]

73. We consider it appropriate to include "program" as one of the subject matters of the proposed offence, which aims to combat cybercrime. This position also accords with the standard of criminalisation under the Budapest Convention.[50]

Limiting the application of the offence to cases where a device, program or data is used to commit a cyber-related offence (but not any offence at large)[51]

74. If the illegitimate use of a device, program or data is not restricted to the commission of cybercrime, Recommendation 9 will have an all pervasive application in the physical world.[52] Besides, the cybercrime legislation in other jurisdictions discussed in the CP has consistently confined the scope of the proposed offence to the commission of cyber-dependent crimes. If a person uses a device, program or data for committing other general offences that are not cybercrime, the culpable conduct can be tackled under the myriad of statutory and common law offences in Hong Kong.

75. Thus, we recommend that the proposed offence should only apply if the offence committed by making available a device, program or data (or possessing such device, program or data for the purpose of making it available) is a cyber-related offence, ie one of the four other cyber-dependent crimes

---

49 Paras 6.24 to 6.25 of the Report.

50 Article 6 of the Budapest Convention requires each party to adopt measures to criminalise "*the production, sale, procurement for use, import, distribution or otherwise making available of … a device, including a computer program, designed or adapted primarily for the purposes of committing any of the [cyber-dependent] offences established in accordance with Articles 2 through 5.*" (emphasis added)

51 Paras 6.26 to 6.36 of the Report.

52 Eg if a person who composes an email that seeks to blackmail a victim eventually decides not to send the email but to keep the draft, he will be in possession of data that can be used to commit "an offence", and hence be guilty of the proposed offence under Recommendation 9 of the CP.

discussed in Chapters 2 to 5.[53]

Recasting the possession limb of the offence[54]

76. We acknowledge that there is a wide range of circumstances in which a person may possess a malicious program or data without any intention to use the same to commit a cyber-related crime.[55] To avoid over-criminalisation, we recommend limiting the scope of the possession limb in Recommendation 9(a) as "*possessing a device, program or data made or adapted to commit a cyber-related crime for the purpose of making it available to another*". Under this narrower form of the possession offence, persons who possess a device, program or data made or adapted to commit a cyber-related crime in non-culpable circumstances will not incur criminal liability by reason of merely in possession of such device, program or data, but persons who possess the device, program or data for their own use to commit a cyber-related crime will be caught by the offence.

Incorporating additional mens rea requirements into the offence[56]

Knowledge, belief, etc in respect of the nature of a device, program or data

77. A person may not accurately know or understand the primary use of a device, program or data.[57] This is particularly so if the harmful nature of a program is not readily identifiable, or if the harmful program is not well-known. In our view, if a person misunderstands the nature of the device, program or data, or does not know that its primary use is criminal, the person should not be liable for the proposed offence. Thus, we recommend that the prosecution must prove that the defendant knows, believes, or claims that the primary use of a device, program or data (determined objectively) is to commit a cyber-related crime.

Maintaining a basic offence of "making available"

78. In the context of possession for the purpose of "making available", we have to first consider whether or not the proposed offence should require a defendant to "know" or "intend" that the device, program or data is to be used by another to commit an offence (ie the defendant must have knowledge as to the actual intended use of the device, program or data). Putting this requirement in place would in effect abandon the basic offence recommended in the CP and result in some suppliers of harmful devices, programs or data slipping through the net because a supplier may simply make available such devices, programs or data on the dark web without caring or knowing how

---

53 Namely, the offences of illegal access to program or data, illegal interception of computer data, illegal interference with computer data and illegal interference with computer system. In Part Two of our study, which will cover cyber-enabled crimes, we would consider what else, if any, should also come under the list of "cyber-related offences" to be scheduled to the bespoke cybercrime legislation.

54 Paras 6.37 to 6.40 of the Report.

55 Eg a person may learn from an anti-virus scan run on his computer that he is in possession of a malicious program or data, but the anti-virus scan may not provide an average computer user with a lot of information about the nature or impact of the program or data.

56 Paras 6.41 to 6.51 of the Report.

57 Eg a person may download a program on the understanding that the program is harmless.

buyers intend to use them. In order not to undermine the objective of the offence to curb the supply and possession of devices or data that can be used in cyberspace for illegitimate purposes, we take the view that the basic offence should be maintained, subject to the refinements recommended in paragraphs 76 and 77 above.

Alternative mental element: having reasonable grounds to believe in the culpable primary use of a device, program or data[58]

79. Although a defendant who comes into possession of, for example, a computer program may not have actual knowledge that the program comprises a ransomware or virus (which can be used to commit a cyber-related crime), the circumstances may be so dubious as to warrant the defendant to have reasonable grounds to hold such belief.[59] There is a substantial degree of criminality in knowingly making available devices, programs or data for committing cybercrime and knowingly possessing any of these items for the purpose of making them available. Curbing this sort of behaviour is in line with the broader objective of the proposed offence to prevent the use of harmful devices, programs or data for the commission of cybercrime.

80. To enhance the deterrent effect of the law, we recommend that the proposed offence should also catch a person who "*has reasonable grounds to believe*" that the primary use of a device, program or data is to commit a cyber-related crime.

Making available or possessing part of a malicious device, program or data[60]

81. With the advancement in technology, programs or data can be stored, accessed and shared in a decentralised way (eg in a distributed file system such as the InterPlanetary File System, or the Blockchain technology[61]). A perpetrator may only hold a portion of the overall data, which is by itself innocent, but technology makes it possible to aggregate data stored at multiple locations and make the composite malicious data available to any person.

82. To allow more flexibility in the law, we recommend refining Recommendation 9 by specifying that the reference to a "*device, program or data*" includes a part thereof. This revision does not fundamentally alter the nature of the proposed offence because for criminal liability to arise, the prosecution must prove the same *mens rea* elements beyond reasonable doubt, ie the person (i) knows that he is in possession of a device, program or data (or any part thereof); and (ii) knows, believes, has reasonable grounds to believe, or claims that the primary use of a device, program or data (or any part thereof)

---

58 Our reasoning is detailed at paras 6.48 to 6.51 of the Report.

59 Eg a stranger passes a program to a defendant who is requested to upload the program to a certain computer system at a particular time on a specified date in return for a large monetary reward without any explanation.

60 Paras 6.52 to 6.54 of the Report.

61 A blockchain is a distributed database or ledger shared among a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralised record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable. See https://www.investopedia.com/terms/b/blockchain.asp (accessed on 1 Nov 2025).

is to commit a cyber-related crime.

The "reasonable excuse" statutory defence[62]

83. As with the Access Offence discussed in Chapter 2, we consider it unnecessary to provide a list of examples of legitimate activities that would fall within the general "reasonable excuse" defence to the proposed offence. We have recommended a number of specific defences, which will be discussed in paragraphs 85 to 93 below.

84. Based on Recommendation 9 in the CP (with some modifications), we make our **Final Recommendation 9** as follows:

> *"(a) Knowingly making available a device, program or data (or a part thereof) made or adapted to commit a cyber-related crime,*[63] *or knowingly possessing the device, program or data for the purpose of making it available, irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code, should be a basic offence under the new legislation, subject to a statutory defence of reasonable excuse.*
>
> *(b) The actus reus of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device, program or data in question) and the demand side (such as obtaining, possession, purchase and import of a device, program or data in question).*
>
> *(c) The proposed offence should apply to a device, program or data (or a part thereof) so long as its primary use (to be determined objectively) is to commit a cyber-related crime, regardless of whether or not it can also possibly be used for any legitimate purposes.*
>
> *(d) The mens rea requirements of the proposed offence are that:*
>
> > *(i) a person knows that he is making available or that he is in possession of a device, program or data (or a part thereof) for the purpose of making it available; and*
> >
> > *(ii) a person knows, believes, has reasonable grounds to believe, or claims that the primary use of a device, program or data (or a part thereof) is to commit a cyber-related crime.*
>
> *(e) A person who claims (whether or not the claim is true) or mistakenly believes that the primary use of a device,*

---

62 Paras 6.57 to 6.59 of the Report.

63 Namely, illegal access to program or data, illegal interception of computer data, illegal interference with computer data and illegal interference with computer system.

program or data is to commit a cyber-related crime should also be guilty of an offence in the same way as a person is guilty of attempting to traffic in a dangerous drug even if the person's culpable belief in the nature of the substance being trafficked turns out to be incorrect.

(f) *Knowingly making available a device, program or data (or a part thereof) made or adapted to commit a cyber-related crime, or knowingly possessing the device, program or data for the purpose of making it available, irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code, should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse, if the device, program or data:*

(i) *is, or is known, believed*[64] *or claimed by the perpetrator to be, capable of being used to commit a cyber-related crime; and*

(ii) *the perpetrator intends it to be used by any person to commit a cyber-related crime.*

(g) *Knowingly possessing a device, program or data (or a part thereof) should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse, if the device, program or data:*

(i) *is, or is known, believed*[65] *or claimed by the perpetrator to be, capable of being used to commit a cyber-related crime; and*

(ii) *the perpetrator intends to use it to commit a cyber-related crime.*

(h) *Subject to the above, the proposed provisions should be modelled on section 3A of the Computer Misuse Act in England and Wales as well as sections 8 and 10 of the Computer Misuse Act in Singapore."*

Specific defences

Making available a harmful device, program or data for cybersecurity purposes (or possessing such a device, program or data for making it available for cybersecurity purposes)[66]

85. As with the Access Offence and the Interference Offences, we recommend that there should be a specific defence for making available a

---

64 Including cases where a person has reasonable grounds to believe that the device, program or data is capable of being used to commit a cyber-related crime.

65 Same as above.

66 Paras 6.71 to 6.75 of the Report.

harmful device, program or data for cybersecurity purposes (or possessing the same for making it available for cybersecurity purposes). As devices, programs or data may be possessed or made available by persons other than accredited cybersecurity practitioners,[67] we propose that the cybersecurity defence should extend beyond cybersecurity practitioners to cover persons who possess or make available a device, program or data for cybersecurity purposes with the prior permission or authorisation of cybersecurity practitioners.

Making available a harmful device, program or data for educational, scientific or research purposes (or possessing such a device, program or data for making it available for the aforementioned purposes)[68]

86. We agree with the Respondents that there should be a defence to the proposed offence for educational or research purposes, which would apply to teachers and students in the field of computer science, as well as amateurs who acquire or create a harmful computer program (eg a trojan horse) for their own study. We appreciate that computer science research may be carried out for benevolent or malicious purposes, but the law should allow room for advancement of research on harmful devices, programs or data. To safeguard against abuse, we recommend that the conduct of the person who relies on this defence must be reasonable and no more than is necessary for achieving the relevant purpose.

*Defence for internet service providers ("**ISPs**")*[69]

87. ISPs provide internet connections and related services (such as web hosting) to individuals and organisations. As an internet protocol address assigned by an ISP may host multiple websites and URLs, it may not always be feasible for ISPs to disable access to harmful websites, programs or data made or adapted to commit a cyber-related crime (eg a fake bank website) as this may disrupt their provision of services to other internet users.

88. Taking into account the position ISPs are in, we recommend providing a defence for ISPs by modelling on the mere conduit defence under Article 4 of the Digital Services Act ("**DSA**") approved by the Council of the European Union and by adopting the a definition of "service provider" as broad as that in section 65A(2) of the Copyright Ordinance (Cap 528).[70] It is a defence for an ISP to show that it, as a service provider:

(a) does not initiate the transmission of the device, program or data concerned (collectively "**illegal content**");

---

67 Eg in a company that develops anti-virus software, its technicians, salespersons and other non-professional employees may come into possession of computer viruses in the course of performing their duties.

68 Paras 6.76 to 6.79 of the Report.

69 Paras 6.82 to 6.87 of the Report.

70 Section 65A(2) of the Copyright Ordinance (Cap 528) provides that a "service provider" is "*a person who, by means of electronic equipment or a network, or both, provides, or operates facilities for, any online services*". Under s 65A(2)(a) to (c), an "online service" includes:

"(a) the transmission, routing, or provision of connections for digital online communications, between or among points specified by a user, of information or material of the user's choosing;

(b) the hosting of information or material that can be accessed by a user; and

(c) the storing of information or material on a system or network that can be accessed by a user."

(b) does not select the receiver of the transmission; and

(c) does not select or modify the illegal content contained in the transmission.

Defence for storage and/or dissemination of devices, programs or data[71]

89. In the digital age, a vast array of internet services are offered by hosting service providers, cloud service providers and data storage facilities. To make the bespoke cybercrime legislation comprehensive, we recommend modelling on Article 6 of the DSA[72] to develop a defence in favour of different "service providers" whose services include the "storage" and/or "dissemination" of devices, programs or data provided by a recipient of the service. This approach will cover these service providers without the need to differentiate between them.

90. As it may not always be technically feasible for such a service provider to remove or disable access to an illegal content due to the knock-on effect on other users, we propose that it is a defence to prove that:

(a) access to the illegal content is removed or disabled as soon as reasonably practicable upon the provider's knowing or having reasonable grounds to believe that illegal content has been provided by a recipient of the service; or

(b) (if the removal, or disabling access to, the illegal content is not technically feasible or reasonably practicable) the service provider has reported the existence of the illegal content to an LEA as soon as reasonably practicable.

Defence for making available a device, program or data by automated technology[73]

91. As technological advancement now makes it possible for a harmful device, program or data to be made available or disseminated by means of an automated process (eg a blockchain or an internet bot), we envisage situations where an automated process, tool or technology used for distributing data may, in itself, be innocuous, but a perpetrator taints the innocent process, tool or technology with a malicious device, program or data (eg a virus or malicious app), and the blockchain or bot then automatically distributes the malicious material further.

---

71 Paras 6.88 to 6.92 of the Report.

72 Article 6(1) of the DSA reads:
"*Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider:*
(a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or
(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content."

73 Paras 6.93 to 6.96 of the Report.

92. We consider it fair that if certain illegal content is made available solely by means of an automated process, tool or technology, it is a defence for a person to show that he:

(a) was not knowingly involved in designing, producing, or generating such illegal content; and

(b) was not knowingly involved in the process by which such illegal content became part of that automated process.

93. Instead of referring to any specific technology, the defence is framed generically by reference to "automated process". This is because as technology continues to evolve, alternatives to blockchain and bots may emerge.

94. Our **Final Recommendation 10** is as follows:

"Apart from the statutory defence of reasonable excuse, we recommend the following specific defences to the offence of making available a device, program or data for committing a cyber-related crime (or possessing such device, program or data for the purpose of making it available for committing a cyber-related crime):

(a) Making available the device, program or data for cybersecurity purposes (or possessing such device, program or data for the purpose of making it available for cybersecurity purposes):

(i) This defence should only apply to an accredited cybersecurity practitioner (whose qualifications would be recognised under a regime to be established by the Government) who has acted for a genuine cybersecurity purpose;

(ii) The cybersecurity practitioner's purpose and conduct must be reasonable having regard to all the circumstances; and

(iii) This defence should extend to:

(1) persons who possess or make available the device, program or data for cybersecurity purposes with the prior permission or authorisation of a cybersecurity practitioner; and

(2) persons who assist the cybersecurity practitioner in carrying out his professional duties.

(b) Making available the device, program or data for genuine educational, scientific or research purposes (or possessing

such device, program or data for the purpose of making it available for genuine educational, scientific or research purposes). The conduct of a person who relies on this defence must be reasonable having regard to all the circumstances.

(c) *Modelling on Article 4 of the Digital Services Act ("**DSA**") of the European Union, it is a defence for an internet service provider*[74] *that serves as a mere conduit in making available the device, program or data (or possessing the device, program or data for the purpose of making it available) to show that the provider:*

  (i) *does not initiate the transmission of the device, program or data ("**illegal content**");*

  (ii) *does not select the receiver of the transmission; and*

  (iii) *does not select or modify the illegal content contained in the transmission.*

(d) *Modelling on Article 6 of the DSA, where the services of a service provider*[75] *include storage and/or dissemination of a device, program or data provided by a recipient of the service, and the service provider becomes aware of or has reasonable grounds to believe that illegal content, or access to that illegal content (whether directly or indirectly), has been provided by a recipient of the service, it is a defence for the service provider to show that:*

  (i) *access to the illegal content is removed or disabled as soon as reasonably practicable upon the service provider's obtaining such knowledge or having such reasonable grounds to believe; or*

  (ii) *(if the removal, or disabling access to, the illegal content is not technically feasible or reasonably practicable) the service provider has reported the existence of the illegal content to a law enforcement agency as soon as reasonably practicable.*

(e) *If an illegal content is made available solely by means of an automated process, tool or technology, it is a defence for a person to show that he:*

---

74 We recommend adopting a definition of "service provider" as broad as that in s 65A(2) of the Copyright Ordinance (Cap 528) so as to cover service providers of all sizes, as well as individuals who create an online space (such as a forum or website) for hosting or storing program or data. See para 88 of this Summary.

75 Same as above.

(i) was not knowingly involved in designing, producing, or generating the illegal content; and

(ii) was not knowingly involved in the process by which the illegal content became part of that automated process."

Chapter 7: Criteria for the Hong Kong court to assume jurisdiction

Jurisdictional rules on cybercrime[76]

95. On the basis that it is apposite for Hong Kong to follow the international norm that a jurisdiction should provide for any extra-territorial application of its law within reasonable bounds, Recommendations 11 to 15 of the CP prescribed the jurisdictional rules for the five cyber-dependent crimes with reference to the following fact patterns:

(a) Any "essential element"[77] of the offence occurred in Hong Kong, even if other "essential element(s)" occurred elsewhere;

(b) The perpetrator is a "Hong Kong person";

(c) The victim is a "Hong Kong person";

(d) The target computer, program or data is in Hong Kong; and

(e) The perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Expanding fact pattern (c): The victim is a "Hong Kong person"[78]

96. We received overwhelming support for the extra-territorial application of the proposed cybercrime legislation from the Respondents. As regards fact pattern (c) in the preceding paragraph, the CP recommended that the concept of a "Hong Kong person" should include a Hong Kong permanent resident, a person ordinarily residing in Hong Kong and a company carrying on business in Hong Kong.

97. In the light of a Respondent's suggestion, we have reflected on the scope of protection that Hong Kong courts ought to accord to cybercrime victims. We recognise that persons who work or stay in Hong Kong temporarily for one reason or another (eg foreign domestic helpers, tourists and other visitors staying in Hong Kong on a transient basis falling victim to the proposed cyber-dependent offences while they are physically present in Hong Kong)

---

76 Paras 7.2 to 7.6 of the Report.

77 In technical terms, any "*act or omission or other event (including any result of one or more acts or omissions) proof of which is required for conviction of the offence*" as stated in s 3(1) of the Criminal Jurisdiction Ordinance (Cap 461).

78 Paras 7.25 to 7.28 of the Report.

should also be protected by Hong Kong laws.

98. Accordingly, we recommend refining fact pattern (c) as follows:

> *"the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or was physically present in Hong Kong at the time the relevant offence was committed, or a company carrying on business in Hong Kong."*

Jurisdiction over acts endangering national security[79]

99. As to whether it is necessary to provide for the extra-territorial effect of the cyber-dependent offences over acts endangering national security, but not merely acts threatening the "*security of Hong Kong*", our analysis is detailed at paragraphs 7.33 to 7.40 of the Report. In sum, this issue has been resolved by the BL 23 legislation, which clearly provides that a reference in any other ordinance to the "*security of the HKSAR*" (or a phrase which means the same)[80] is to be read as including "national security" as it is statutorily defined.[81] Besides, when a cybercrime case involves any offence under the NSL, it is abundantly clear that, as a general rule, Hong Kong courts may exercise jurisdiction over the case in accordance with Article 40 of the NSL.[82] Last but not least, given that jurisdiction over cybercrime cases that endanger national security is not exclusively vested in Hong Kong courts by reason of Articles 55[83] and 56[84] of the NSL, it would be inappropriate for the jurisdictional rules of the bespoke cybercrime legislation to prescribe that Hong Kong courts shall assume jurisdiction in such cases.

Evidentiary and procedural issues[85]

100. Some Respondents raised evidentiary and procedural issues, including the collection of evidence from other jurisdictions, the preservation and admissibility of evidence obtained from the cloud-based environment and whether any provisions under the Mutual Legal Assistance in Criminal Matters Ordinance (Cap 525) ("**MLACMO**") should be amended. As Part Three of our study will address enforcement and procedural issues, which is a substantial

---

79 Paras 7.33 to 7.40 of the Report.

80 Section 8(2).

81 Section 4.

82 Article 40 provides that "*The Hong Kong Special Administrative Region shall have jurisdiction over cases concerning offences under [the NSL], except under the circumstances specified in Article 55 of [the NSL].*"

83 Article 55 provides that *"The Office for Safeguarding National Security of the Central People's Government in the Hong Kong Special Administrative Region shall, upon approval by the Central People's Government of a request made by the Government of the Hong Kong Special Administrative Region or by the Office itself, exercise jurisdiction over a case concerning offence endangering national security under [the NSL], if:*

(1) the case is complex due to the involvement of a foreign country or external elements, thus making it difficult for the Region to exercise jurisdiction over the case;

(2) a serious situation occurs where the Government of the Region is unable to effectively enforce [the NSL]; or

(3) a major and imminent threat to national security has occurred."

84 Article 56 provides that "*In exercising jurisdiction over a case concerning offence endangering national security pursuant to Article 55 of [the NSL], the Office for Safeguarding National Security of the Central People's Government in the Hong Kong Special Administrative Region shall initiate investigation into the case, while the Supreme People's Procuratorate shall designate a prosecuting body to prosecute the case and the Supreme People's Court shall designate a court to adjudicate it.*"

85 Paras 7.20 to 7.22, 7.31 and 7.32 of the Report.

topic, we shall bear in mind the issues helpfully identified by the Respondents. Given that the related amendments to the MLACMO will ultimately depend on the form in which the proposed cybercrime legislation is enacted and negotiation with other jurisdictions may be required to foster cross-jurisdictional cooperation, it would be premature for us to make any recommendations with regard to the consequential amendments to the MLACMO, which would best be left to the Government's decision in due course.

101. For the above reasons, we retain Recommendations 11 to 15 in the CP and expand fact pattern (c), resulting in the following **Final Recommendations 11 to 15**:

> *"Final Recommendation 11*
>
> *We recommend that, in respect of the proposed offence of illegal access to program or data, Hong Kong courts should have jurisdiction where:*
>
> *(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;*
>
> *(b) the victim (the target computer's owner, the data's owner, or both) is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or was physically present in Hong Kong at the time when the offence was committed, or a company carrying on business in Hong Kong;*
>
> *(c) the target computer, program or data is in Hong Kong; or*
>
> *(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong,*
>
> *subject to a requirement that, in respect of a perpetrator charged with the summary offence on the basis of his or her act done outside Hong Kong, such act, either alone or together with other such act(s), omission(s) or event(s) the proof of which is required for conviction of the Hong Kong offence, must constitute a crime in the jurisdiction where it was done.*
>
> *Final Recommendation 12*
>
> *We recommend that, in respect of the proposed offence of illegal interception of computer data, Hong Kong courts should have jurisdiction where:*

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or was physically present in Hong Kong at the time when the offence was committed, or a company carrying on business in Hong Kong;

(c) the target computer, program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Final Recommendation 13

We recommend that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference with computer data, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or was physically present in Hong Kong at the time when the offence was committed, or a company carrying on business in Hong Kong;

(c) the target program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Final Recommendation 14

We recommend that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference with computer system, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or was physically present in Hong Kong at the time when the offence was committed, or a company carrying on business in Hong Kong;

(c) the target computer is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Final Recommendation 15

We recommend that, in respect of the proposed offence of making available a device, program or data for committing a cyber-related crime, or possessing a device, program or data for the purpose of making it available for committing a cyber-related crime, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere, eg a person physically in Hong Kong making available on the dark web, a device, program or data for committing a cyber-related crime;

(b) the perpetrator is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong; or

(c) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong."

Chapter 8: Sentencing

102. Recommendation 16 of the CP set out the maximum sentences for the five proposed cyber-dependent offences. In general, the Respondents supported introducing a set of penalties that is tougher than that in respect of

the current computer-related offences since it will help deter cyber-dependent crimes, and a sound and robust cybersecurity regime will contribute positively to Hong Kong's business standing.

Summary form of the Access Offence[86]

103. In view of a Respondent's suggestion, we have considered whether the two years' maximum imprisonment for the summary form of the Access Offence would provide sufficient deterrence. In sum, pitching the maximum penalty at two years' imprisonment serves to signify the gravity of the summary form of the Access Offence by the commission of which the sanctity of the targeted system or confidentiality of the information that the law seeks to protect has already been violated even though there is insufficient evidence of any intent to carry out further criminal activity upon unauthorised access to program or data. We are of the view that the proposed maximum sentence is appropriate since this will give the sentencing court sufficient power to impose a punishment which can properly reflect the gravamen of the offence.

The rationale behind the maximum sentence of life imprisonment for the aggravated Interference Offences[87]

104. The prescription of a maximum sentence of life imprisonment only sought to maintain consistency with the penalty for the aggravated offence of criminal damage under the existing section 63(1) of the CO which, when read together with section 60(2)(b) of the CO,[88] ensures that the penalty which may be imposed is sufficient to deal with property damage or destruction situations where an intention to endanger life is involved. As the Interference Offences may put the lives of thousands of people at risk,[89] a severe maximum sentence is justifiable. In fact, acts of illegal interference with computer data and/or computer system may, depending on the facts of the case, already constitute the aggravated criminal damage offence, which currently attracts a maximum penalty of life imprisonment. The new cybercrime legislation only intends to mirror these existing Interference Offences already envisaged under the CO.

105. Having reviewed Recommendation 16 in its entirety, we are satisfied that our recommendations will have the necessary deterrent effect to combat cybercrime, and are not too out of line with the maximum sentences for (a) the crimes in the Theft Ordinance (Cap 210)[90] as well as (b) relevant

---

86 Paras 8.9 to 8.13 of the Report.

87 Paras 8.14 to 8.18 of the Report.

88 Section 60(2) of the CO provides that:
"*A person who without lawful excuse destroys or damages any property, whether belonging to himself or another—*
(a) intending to destroy or damage any property or being reckless as to whether any property would be destroyed or damaged; and
(b) intending by the destruction or damage to endanger the life of another or being reckless as to whether the life of another would be thereby endangered,
shall be guilty of an offence." (emphasis added)

89 Eg interference with computer data processed by the system of an airport's control tower, a railway signal system, a power plant, etc.

90 The representative types of crimes used as references are the offences of theft, fraud, blackmail, burglary, aggravated burglary and robbery under the Theft Ordinance (Cap 210).

offences in other jurisdictions.[91] Thus, we retain Recommendation 16 in the CP as our **Final Recommendation 16**:

> *"We recommend that:*
>
> *(a) In respect of the proposed offence of illegal access to program or data, an offender should be liable to the following maximum sentences:*
>
> *(i) for the summary offence, imprisonment for two years; or*
>
> *(ii) for the aggravated offence, imprisonment for 14 years on conviction on indictment.*
>
> *(b) In respect of the proposed offence of illegal interception of computer data, an offender should be liable to imprisonment for two years on summary conviction and 14 years on conviction on indictment.*
>
> *(c) In respect of each of the proposed offences of illegal interference with computer data and illegal interference with computer system, an offender should be liable to the following maximum sentences:*
>
> *(i) for the basic offence, imprisonment for two years on summary conviction and 14 years on conviction on indictment; or*
>
> *(ii) for the aggravated offence, imprisonment for life.*
>
> *(d) In respect of the proposed offence of making available a device, program or data for committing a cyber-related crime (or possessing such a device, program or data for the purpose of making it available to another), an offender should be liable to the following maximum sentences:*
>
> *(i) for the basic offence, imprisonment for two years on summary conviction and seven years on conviction on indictment; or*
>
> *(ii) for the aggravated offence, imprisonment for 14 years on conviction on indictment."*

[91] See the Appendix to the CP, which summarises the maximum sentences for the five proposed cyber-dependent offences under the current laws in Hong Kong and other jurisdictions.