THE LAW REFORM COMMISSION OF HONG KONG

SUB-COMMITTEE ON CYBERCRIME

CONSULTATION PAPER ON CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

EXECUTIVE SUMMARY

(This executive summary is an outline of the Consultation Paper issued to elicit public response and comment on the recommendations and consultation questions of the Law Reform Commission ("LRC") Sub-committee on Cybercrime ("Sub-committee"). It adopts the same abbreviations and defined terms in the Consultation Paper. Those wishing to comment should refer to the full text of the Consultation Paper, which can be downloaded from the LRC's website at https://www.hkreform.gov.hk or obtained from the LRC Secretariat at 4th Floor, East Wing, Justice Place, 18 Lower Albert Road, Central, Hong Kong.

Comments should reach the Secretary to the Sub-committee by 19 October 2022.)

Preface

Terms of reference

1. The Sub-committee commenced its study on cybercrime in January 2019 with the Terms of Reference set out below:

> "*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.*"

Three planned parts of the project

2. The Consultation Paper relates to the first of the following three parts of the project:

(a) Part One addresses cyber-dependent crimes[1] and jurisdictional issues;

(b) Part Two, subject to further discussion in due course on its scope, will cover cyber-enabled crimes [2] and attempt to address the macro challenges in the digital age, including data sovereignty;[3] and

(c) Part Three will deal with evidentiary and enforcement (procedural) issues.

Five cyber-dependent offences to study in Part One

3. The Consultation Paper examines five cyber-dependent offences which are the core species of cybercrime recognised globally that should be addressed, namely:

(a) illegal access to program or data;

(b) illegal interception of computer data;

(c) illegal interference of computer data;

(d) illegal interference of computer system; and

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

4. After the Sub-committee had commenced its study, the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**National Security Law**") was enacted and applied, as a national law, to Hong Kong by promulgation on 30 June 2020. The duty of Hong Kong to safeguard national security reaffirmed the need for reform of cybercrime laws in Hong Kong[4] and the Sub-committee has taken this into consideration in its pursuit of the cybercrime project.

Guiding principles behind the recommendations

5. We appreciate the need and importance to take into account various stakeholders' different interests and perspectives when we devise our recommendations. Our guiding principles are to balance:

---

1 Crimes that can be committed only through the use of Information and Communications Technology ("**ICT**") devices, where the devices are both the tool for committing the crime, and the target of the crime. Examples include hacking, distribution of computer virus, and a distributed denial of service ("**DDOS**") attack.

2 Traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT. Examples include online dissemination of child pornography, setting up of a phishing website, and online doxxing.

3 Data sovereignty is also known as cyber, digital or technological sovereignty. It refers to the idea that a place should be able to take autonomous actions and decisions regarding its digital infrastructures and technology deployment. It also relates to efforts in ensuring the security of digital infrastructures and their authority regarding digital communication matters pertaining to their territories and citizens. See Julia Pohle & Thorsten Thiel, "Digital Sovereignty", Internet Policy Review: Journal on internet regulation (2020), Vol 9, Issue 4, at 8.

4 In addition to the general principles set out in Article 3, Article 9 of the National Security Law provides, in particular, that the Hong Kong Special Administrative Region Government shall take necessary measures to strengthen regulation over matters concerning national security, including the internet.

(a) the right of netizens and interests of persons in the information technology industry; and

(b) protection of the public's interest and right not to be disturbed or attacked when using and operating their computer system.

Chapter 1: Categorisation of cybercrime

6. At the United Nations level, there is no definitive or exhaustive list of cybercrime. Multiple ways to categorise cybercrime and multiple sets of terminologies for such categorisation exist in the literature. The United Nations Office on Drugs and Crime Global Programme on Cybercrime differentiates between "cyber-dependent offences" and "cyber-enabled offences".[5]

7. The Council of Europe's Convention on Cybercrime ("**Budapest Convention**") tackles four categorises of offences.[6] Among them, the category "offences against the confidentiality, integrity and availability of computer data and systems" broadly corresponds to the focus of the Consultation Paper.

8. Among the seven jurisdictions covered in our comparative study, Australia, Canada, England and Wales, and the United States of America are parties to the Budapest Convention, and the remaining three jurisdictions, namely Mainland China, New Zealand and Singapore (same as Hong Kong) are not.

Chapter 2: Illegal access to program or data

9. Broadly speaking, an offence in respect of illegal access to program or data would seek to address dangerous threats to, and attacks against, the security of computer systems, and thereby protect people's right to manage, operate and control their computer system in an undisturbed and uninhibited manner. Hacking is the quintessential example of this offence.

Current Hong Kong law

10. Under section 161 of the Crimes Ordinance (Cap 200) ("**CO**") ("**section 161**"), it is an offence to obtain access to a computer:

(a) with intent to commit an offence;

(b) with a dishonest intent to deceive;

(c) with a view to dishonest gain for himself or another; or

---

[5] United Nations Office on Drugs and Crime, "Global Programme on Cybercrime", available at https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (accessed on 3 May 2022).

[6] These are offences against the confidentiality, integrity and availability of computer data and systems, 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.

(d) with a dishonest intent to cause loss to another.

11. Based on *Secretary for Justice v Cheng Ka Yee*,[7] section 161 does not apply to the use by a person of his or her own computer, not involving access to another's computer. It therefore does not apply to, for example, the use of one's own computer to set up a phishing website.

12. Section 161 does not, on its face, require that an access in question must be unauthorised. Yet, the courts appear to have read in such a requirement.[8]

13. The "gain" in section 161 is not confined to financial or proprietary benefits, but is wide enough to cover intangible benefits such as information to which a person previously had no access.[9]

14. Under section 27A of the Telecommunications Ordinance ("**TO**") (Cap 106) ("**section 27A**"), any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorised access to any program or data held in a computer commits an offence.

15. A perpetrator must have obtained access "by telecommunications" for section 27A to apply. This suggests the use of a telecommunications device (eg another computer) to obtain access, in addition to the target computer.

16. Case law shows that incidents of hacking tend to be prosecuted under section 161. One reason may be the apparent difficulty for the prosecution to prove the *mens rea* under section 27A, which has two aspects, namely the defendant:

(a) "*does not believe that he has been … authorized*" to obtain access of the kind in question; and

(b) "*does not believe that he would have been so authorized if he had applied for the appropriate authority*".

17. In circumstances where both sections 161 and 27A can be invoked, the choice is potentially material because of the disparity in their maximum sentences (ie a fine at level 4 under section 27A ($25,000) and imprisonment for five years on conviction upon indictment under section 161).

The Sub-committee's views

Bespoke cybercrime legislation preferable

18. At present, Hong Kong does not have an Ordinance applicable to cybercrime specifically. Different offences are covered in various Ordinances, some of which are outdated.

---

7 (2019) 22 HKCFAR 97, [2019] HKCFA 9.

8 Same as above, at para 38.

9 *HKSAR v Tsun Shui Lun* [1999] 3 HKLRD 215, HCMA 723/1998 (date of judgment: 15 Jan 1999), cited with approval in *HKSAR v Au Yeung Ka Man Yuniko* [2018] HKCFA 23.

19. In comparison, most of the other jurisdictions surveyed in our comparative study either have bespoke cybercrime legislation, or have a part of their codified law dedicated to cybercrime. Those jurisdictions' approach helps ensure uniformity, comprehensiveness and consistency (eg the definitions of key concepts). We propose a wholesale reform of the current law by enacting a piece of bespoke legislation on cybercrime that will include our proposed offences.

Definition of key terms

20. We observe that the current dictionary meaning of "computer" reflects the modern state of technology.[10] We have also considered the definition of "computer" in the Evidence Ordinance (Cap 8) (which was drafted in the context of admitting documentary evidence in criminal proceedings)[11] as well as the definition of "information and communications technology (ICT) device"[12] in the "*Draft United Nations Convention on Cooperation in Combating Cybercrime*" submitted by the Russian Federation to the United Nations in 2017 ("**Russian Convention**"). In our view, despite the advances in digital technology, the term "computer", as compared with "ICT device", remains a clear concept that is well understood by the public and widely used in the legislation of other jurisdictions.

21. Nevertheless, we are mindful of the possibility that any statutory definition, including a general one of "ICT device", may fall behind the inexorable advancement of information technology. Although we trust that the courts can construe any definition flexibly in light of advances in technology to best reflect the true legislative intent, difficulties of applying a statutory definition may still arise in practice as defendants may attempt to make every technical argument to assert that a "device" does not legally constitute a "computer" as originally intended by the legislature. All things considered, we are, on balance, in favour of leaving terms such as "computer" and "computer system" undefined, but this issue can be further considered by the law draftsman during the legislative stage should the Government implement our recommendations.

Outlawing mere unauthorised access

22. Mere unauthorised access is an offence in Hong Kong (section 27A) and some other jurisdictions. Unauthorised access to computer / program or data happens every moment on the internet for a myriad of reasons, both legitimate and potentially illegitimate. A layperson would likely have little clue as to whether his or her computer was accessed by someone with or without malice.

23. We discussed at length the extent to which unauthorised access to computer / program or data is analogous to the scenario in the physical world where a stranger enters an area without permission. In this regard, we must point out that

---

[10] See Oxford English Dictionary (Mar 2022), which refers to a "computer" as "*an electronic device (or system of devices) which is used to store, manipulate, and communicate information, perform complex calculations, or control or regulate other devices or machines, and is capable of receiving information (data) and of processing it in accordance with variable procedural instructions (programs or software); esp. a small, self-contained one for individual use in the home or workplace, used esp. for handling text, images, music, and video, accessing and using the internet, communicating with other people (e.g. by means of email), and playing games*".

[11] S 22A(12) of the Evidence Ordinance (Cap 8) defines a "computer" as "*any device for storing, processing or retrieving information*".

[12] Article 4(o) of the Russian Convention defines an "ICT device" as "*an assemblage (grouping) of hardware components used / designed for automatic processing and storage of electronic information*".

the characteristics inherent in the design and functioning of the virtual space mean that in certain widely accepted circumstances, authorisation to access program or data is implicitly granted by an online user. For example, an online user is generally not expected to seek prior express authorisation for displaying an advertisement on a webpage browsed by another user, just as a search engine normally does not obtain consent from a website before scanning the internet protocol address concerned. We consider that these customary practices, in respect of which authorisation is regarded as implicitly granted, should continue to be tolerated. On this basis, our majority view is that mere unauthorised access should be criminalised as a summary offence, which does not require malice to be an element of the offence, subject to the statutory defence of reasonable excuse. In our view, this approach is in line with the treatment of equivalent conduct in the physical world and provides legal certainty since it can be difficult to determine the actual point at which unauthorised access should be outlawed (eg whether it should be outlawed at the point of access, or the point at which the intruder commits further wrongful acts upon access).

Unauthorised nature of an access

24. The new legislation should explicitly stipulate that only an unauthorised access is proscribed so as to provide guidance to obviate unnecessary dispute. As regards how the unauthorised nature of an access should be articulated, we favour the formulation adopted, for offences of unauthorised access to computer materials in England and Wales, in section 17(5) and (8) of their Computer Misuse Act 1990 ("**CMA-EW**") as construed by the House of Lords in *R v Bow Street Metropolitan Stipendiary Magistrate*, *Ex parte United States (No 2)*.[13] Whether there is implied authorisation for access in a particular case would depend on the facts and circumstances as disclosed in the evidence.

25. We further believe that it is fair for our proposed offence to be premised on a person's knowledge that his or her access is unauthorised. The court will likely draw inferences regarding such knowledge based on circumstantial evidence. As with the physical world, a common sense approach should apply in determining whether an access is authorised in cyberspace.

Access to program or data

26. While the meaning of "computer" is rapidly evolving, the terms "program" and "data" are relatively well-defined and static.[14] We lean towards referring to access to program or data because that is clearer and can prevent unnecessary association of the offence with any physical device.

Defence of reasonable excuse

27. We recommend a generic defence based on reasonable excuse because it can better incorporate public interest considerations, cater for unforeseen circumstances and give the court flexibility.

---

[13] [2000] 2 AC 216.

[14] A "program" is "*a series of coded instructions and definitions which when fed into a computer automatically directs its operation in performing a particular task*", while "data" means "*the quantities, characters, or symbols on which operations are performed by a computer, considered collectively*". In non-technical contexts, "data" also means "*information in digital form*". See the Oxford English Dictionary (Mar 2022).

Aggravated offence

28. The proposed summary offence alone will be an insufficient response to the potentially serious harm that an offender may further cause after accessing program or data (eg installation of spyware, or blackmail of the victim).

29. We propose that unauthorised access with intent to carry out further criminal activity should constitute an aggravated offence. As to what further criminal activity should warrant sanction by way of such aggravated offence, the formulation in section 2(2) of the CMA-EW can be a starting point for consideration.

Recommendation 1

The Sub-committee recommends that:

(a) Subject to a statutory defence of reasonable excuse, unauthorised access to program or data should be a summary offence under the new legislation.

(b) 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.

(c) The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the CMA-EW.

Unauthorised access for cybersecurity purposes

30. The concept of "cybersecurity" is grounded on the practices of protecting computer systems from digital attacks.[15] Our extensive debate on unauthorised access for cybersecurity purposes reflects the difficulties in balancing the conflicting arguments for and against the proscription of unauthorised access for cybersecurity purposes. Some relevant considerations and background are cited below:

(a) There are always some people in cyberspace who are testing others' computers (say, by "port scanning") without authorisation. Testing tools are readily available and widely used. The tests may be for benevolent, commercial or malicious purposes.

(b) Some cybersecurity companies scan the internet continuously for common vulnerabilities in webcams, web servers, etc. Those companies may seek to profit from any vulnerabilities identified.

(c) Cybersecurity is a dynamic area. The accreditation landscape keeps changing. No industry organisation is regarded as the sole authority. In

[15] For example, "cybersecurity" has been understood as "*the procedures that are taken to protect computers, networks and programs from a cyberattack or acts of cybercrime (e.g., viruses, malware or ransomware)*". It is also known as "information technology security". See Marion and Twede, Cybercrime: An Encyclopedia of Digital Crime (ABC-CLIO, 2020), at 92.

Hong Kong, many cybersecurity practitioners have hands-on experience but are not formally accredited.

(d) Prohibiting all kinds of unauthorised testing will not preclude scanning from other jurisdictions of computer systems in Hong Kong, and will affect cybersecurity companies without stopping criminals from identifying the vulnerabilities.

31. There appears to be scope for different opinions on where to draw the line between permissible access and impermissible access. Some may think that our proposed offence will be too broad if all kinds of unauthorised testing of a computer can lead to criminal liability irrespective of the reasons and whether damage is caused. Instead of proposing to settle on a position at this stage, we welcome public feedback on the consultation questions set out in Recommendation 2(a) below.

32. We wish to highlight that if any defence or exemption is accorded to professionals in the cybersecurity industry, a fundamental issue that arises is how the identity of these professionals may be ascertained or verified. It appears that a possible solution is to develop some form of accreditation regime, with a statutory or administrative accreditation body maintaining an accessible list of cybersecurity professionals. Accordingly, we invite the public to comment on the questions set out under Recommendation 2(a)(i) and (ii) regarding the manner, method and operational details of an accreditation regime.

33. On the other hand, if it is considered that the dynamic accreditation landscape poses hindrance to a formal accreditation framework, then a possible alternative is to prescribe in the new bespoke cybercrime legislation the requirements for putative cybersecurity professionals to invoke the proposed defence or exemption for cybersecurity purposes, provided that reliable means are available for ascertaining whether a cybersecurity practitioner satisfies the statutory requirements. We welcome public views in this regard in our question in Recommendation 2(a)(iii) below.

34. Lastly, as non-security professionals may also engage in illegal access to program or data, we seek public feedback as to whether there should be any lawful excuse to the offence of illegal access for non-security professionals as we also consult the public similarly over the offence of illegal interference with computer system in Chapter 5.[16]

Recommendation 2

The Sub-committee invites submissions on whether there should be any specific defence or exemption for unauthorised access:

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

[16] See paras 80 to 81 below.

(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 sub-paragraph (i) is yes, how should the accreditation regime work, eg what are the criteria for such accreditation? Should the accredited persons be subject to any continuing education requirements? Should Hong Kong establish an accreditation body (say, under the new cybercrime legislation or otherwise created administratively) that maintains a list of cybersecurity professionals so that, for instance, accredited persons who fail to satisfy the continuing education requirements may be removed from the list or not be allowed to renew their accreditation? Who outside the accreditation body (if any) should also have access to the list?

(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 professionals? 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))[17]?

Limitation period in summary cases

35. The Magistrates Ordinance (Cap 227) stipulates a general limitation period of six months from the time when the matter arose unless the relevant legislation governing a particular summary offence prescribes otherwise. 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. Analysis of the log records may require a few more months. Further time to reach a prosecutorial decision must be factored in.

36. As the default limitation period may be insufficient, we recommend extending the limitation period as stated below.

[17] The examples in Recommendation 8(b) are web scraping by robots or web crawlers initiated by internet information collection tools (eg search engines) to collect data from servers without authorisation, as well as scanning a service provider's system for identifying vulnerability or ensuring the security and integrity of an Application Programming Interface.

Recommendation 3

The Sub-committee recommends 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

37. Broadly speaking, an offence in respect of the interception of computer data would seek to outlaw interception carried out without legal authority and thereby protect people's right to privacy of data communication.

Current Hong Kong law

38. The Basic Law provides that Hong Kong residents shall have freedom of speech (Article 27), and their freedom and privacy of communication shall be protected by law (Article 30).

39. The Hong Kong Bill of Rights provides that no one shall be subjected to arbitrary or unlawful interference with his privacy or correspondence (Article 14), and everyone shall have the right to freedom of expression (Article 16(2)).

40. The Interception of Communications and Surveillance Ordinance (Cap 589) prescribes a statutory regime for the authorisation and regulation of interception of communications and covert surveillance conducted by law enforcement agencies to prevent or detect serious crime and protect public security. However, this Ordinance only applies to public officers, and only regulates the interception of a communication "*in the course of its transmission*".

41. Under section 27(b) of the TO ("**section 27(b)**"), any person who damages, removes or interferes with a telecommunications installation with intent to intercept or discover the contents of a message shall be guilty of an offence.

42. While a computer arguably amounts to a "telecommunications installation" so that section 27(b) applies to the damage, removal or interference with a computer with the stipulated intent, the statutory language and definitions presuppose a telecommunications context and do not apply well to cyberspace.

43. In addition, the subject of an intended interception under section 27(b) is limited to "the contents of a message". This phrase apparently does not cover metadata (ie information about a communication as opposed to the content or substance of the communication) which can be as worthy of protection as "the contents of a message" in terms of its importance to the parties and potential value to a non-party to a communication.

The Sub-committee's views

Outlawing unauthorised interception of computer data

44. To our understanding, an external party can intercept any unencrypted computer data being transmitted in an open network, and it is possible for transmission of computer data to continue notwithstanding any interception.

45. To safeguard the integrity of communications, we take the view that unauthorised interception of computer data should be an offence. Unauthorised disclosure or use of the intercepted data should be prohibited as well.

Interception for a dishonest or criminal purpose

46. The operation of modern networking devices has an element of interception. Given the prevailing technology, the scope of our proposed offence will be unjustifiably broad if mere unauthorised interception of computer data will result in criminal liability.

47. We have concluded against insisting on proof of an intent to commit *a specific offence* as this may cause excessive difficulty in law enforcement. We recommend that under our proposed offence, an interception in question must have been carried out "for a dishonest or criminal purpose".

Offence not to be restricted to private communication

48. Article 3 of the Budapest Convention, which deals with illegal interception of computer data, does not require the computer data in question to be private. We further understand that the Law Commission and the Ministry of Justice in New Zealand have suggested that references to "private communication" in its Search and Surveillance Act 2012 be replaced with "communication". We similarly favour an interception offence that will protect communication in general, rather than just private communication.

Offence to cover all data including metadata

49. The internet adopts a layered approach. Metadata in one layer may be data in another layer. Metadata is not a well-defined concept. We recommend that our proposed offence should apply to data generally, whether it be metadata or not.

Offence to apply to data throughout its transmission

50. Some types of internet-based communications utilise a mechanism known as "store and forward" delivery, ie a communication may be temporarily stored multiple times on a network while *en route* to its destination. A question that arises is whether the interception offence should apply to data at the sliver of time when it is momentarily at rest during transmission.

51. For simplicity, we propose that so long as the data in question is *en route* from the sender to the intended recipient, intercepting it without legal authority should be an offence. One way to achieve this is to introduce a provision along the lines of section 5F of the Telecommunications (Interception and Access) Act 1979 (Cth) of

Australia deeming when a communication is taken to start passing over a system of communication and to continue passing over that system.

Recommendation 4

The Sub-committee recommends that:

(a) Unauthorised interception, disclosure or use 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,[18] including the *mens rea* (ie to intercept "intentionally").

Conduct which society may regard as proper investigations

52. Just as we invite submission on whether there should be a specific defence or exemption for unauthorised access for cybersecurity purposes in the context of the proposed offence of illegal access to program or data (Chapter 2), we also welcome comments on whether the proposed offence of illegal interception of computer data may have the unintended consequence of affecting the conduct of what society may regard as proper investigations.

Interception by genuine businesses

53. Another issue is whether 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 should be allowed to intercept data being transmitted. Such data have many possible uses, eg analysing the data in an employee's computer to ascertain whether he has breached a restrictive covenant, and discovering the preferences of patrons by tracking their smartphones or tablet computers connected to a network system inside a shopping mall.

[18] This was developed by the Commonwealth of Nations after taking into account the Budapest Convention.

54. We observe that it is typically the larger businesses that can afford to draw up meticulous terms and conditions (of providing a Wi-Fi hotspot or a computer for use) that reserve the contractual right to intercept and utilise data of customers or employees. In some cases, it is doubtful how many of the customers or employees would peruse or understand those terms and conditions.

55. One possible way to better protect the customers and the employees is to require the businesses to have statutory authority in order to intercept data lawfully, ie an interception must satisfy certain requirements imposed by legislation. As we are keen to ensure that our recommendations are fair to all stakeholders and their interests are fairly balanced, we invite views on whether the types of data interception and usage described in paragraphs 52 to 53 above should be allowed, in which case we would welcome further suggestions on the types of professions and businesses that should be permitted to intercept and use the data intercepted or transmitted, and whether such permission should carry any conditions or restrictions. We look forward to public feedback on the following consultation questions, which will better inform our approach to the proposed defence or exemption.

Recommendation 5

The Sub-committee invites submissions on:

(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)?

Chapter 4: Illegal interference of computer data

56. Broadly speaking, an offence in respect of illegal interference (as opposed to interception) of computer data would seek to combat intentional damage, deletion, alteration, etc of computer data, and thereby protect the integrity and proper functioning or use of such data.

57. The offences of illegal access and data interference are closely related to each other because one argument in favour of criminalising mere unauthorised access to a system is that such access can result in non-intentional damage.

Current Hong Kong law

58. At present, Hong Kong law addresses illegal interference of computer data mainly by treating it as a form of criminal damage under section 60(1) of the CO. An aggravated form of that offence, applicable to a defendant who intends to endanger the life of another or is reckless as to whether the life of another would be endangered, is prescribed by section 60(2). The CO was amended in 1993 so that:

(a) the meaning of "property" as used in the Ordinance was extended to include "*any program, or data, held in a computer or in a computer storage medium …*";[19] and

(b) to destroy or damage any property in relation to a computer includes "misuse of a computer".[20]

59. There are authorities illustrating successful enforcement of section 60 of the CO ("**section 60**") against cybercrime. In our understanding, people charged under section 161 are occasionally also charged under section 60 as an alternative. One difference between the two provisions is that the *mens rea* under section 60 (either intent or recklessness) is probably more straightforward to prove than the intent as particularised in section 161(1)(a) to (d).[21]

60. Under section 25(a) of the TO ("**section 25(a)**"), any person (not being a telecommunications officer, or a person who, though not a telecommunications officer, has official duties in connection with a telecommunications service) who wilfully secretes, detains or delays a message intended for delivery to some other person shall be guilty of an offence.

61. The language of section 25(a) appears sufficiently broad to prohibit people from suppressing transmission (by telecommunications) of computer data that constitutes a "message". However, section 25(a) has limitations when applied to computer data:

(a) The formulation of section 25(a) does not apply well to cyberspace because it presupposes a telecommunications context.

(b) The *actus reus* under section 25(a) only covers secretion, detention or delay of a message. It does not cover other ways to interfere with computer data, such as deletion or encryption.

---

[19] Crimes Ordinance ("**CO**"), s 59(1)(b).

[20] S 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 of computer data (as opposed to 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."

[21] See para 10 above.

The Sub-committee's views

Prohibiting intentional and unauthorised data interference

62. Data is inevitably altered whenever there is any operation of a computer or interaction with the internet. For example, an email server would remove a dangerous email attachment. A website may add data to a visitor's computer by saving "cookies" in it. Many computer users probably accept such alteration of computer data even if the alteration is intentional (consciously caused by the administrator of the email server or the website).

63. At the same time, in principle, the law should prohibit interference that may cause or has caused harm. Logically, such interference would be unauthorised and may be intentional.

64. Our view is that the issue ultimately boils down to whether the interference is justified by any reasonable excuse. We propose that intentional interference (damaging, deletion,[22] deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence.

Actus reus, mens rea, lawful excuses, and aggravated offence

65. We took the current law – specifically, sections 59 to 64 of the CO regarding criminal damage – as the blueprint in discussing the various aspects of the proposed offence.

66. Our consensus is that the existing regime (including the stipulations on the *actus reus*, the *mens rea*, the two lawful excuses, and the aggravated offence) is generally satisfactory.

Transposing the offence to the new legislation

67. We suggest that the provisions regarding "misuse of a computer" be separated from the offence of criminal damage and adopted in the new legislation to combat cybercrime, while deleting section 59(1)(b) and (1A) of the CO (which was added to expand the scope of the general offence of criminal damage to property in relation to a computer).

Recommendation 6

The Sub-committee recommends that:

(a) Intentional interference (damaging, deletion, deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence under the new legislation.

[22] Even if it may be recoverable by using certain data recovery tools.

(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, but not malice);

(iii) the two lawful excuses under section 64(2), while preserving any other lawful excuse or defence recognised by law; and

(iv) the aggravated offence under section 60(2).

(c) 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).

Chapter 5: Illegal interference of computer system

68. Broadly speaking, an offence in respect of illegal interference of computer system (as opposed to computer data) would seek to prohibit hindrance of lawful use of computer systems by using or interfering with computer data, and thereby protect the proper functioning of computer systems.

69. The functioning of a computer system may be hindered without any modification of data. This may result from, for instance, a distributed denial of service ("**DDOS**") attack[23] or a slow attack, whereby access to a computer network is prevented or its functioning is restricted.

70. Where a computer system has been subject to what appears to be a DDOS attack, whether the parties who caused the result intended to attack the system may be a crucial factual issue.

Current Hong Kong law

71. As discussed, one form of criminal damage under section 60 is "misuse of a computer" as defined in section 59(1A) of the CO. Section 59(1A)(a)[24] is the most relevant to illegal interference of computer system. Case law has established that a DDOS attack can constitute "misuse of a computer".[25]

---

[23] A DDOS attack may be perpetrated by means of a "botnet", ie a group of compromised computers. A criminal can, for example, remotely instruct all computers in a botnet to request the same webpage simultaneously and repeatedly. If the server hosting the webpage has insufficient capacity to respond to the same request from a large number of computers at the same time, the server may freeze, crash or otherwise fail. Those computers' owners may be innocent and kept in the dark.

[24] See fn 20.

[25] *香港特別行政區 訴 朱婷婷* [2017] 4 HKLRD 651 (The English translation of the judgment was reported as *HKSAR v Chu Ting Ting* [2017] 4 HKLRD 666), HCMA 33/2016 (date of judgment: 11 Oct 2016).

72. While a DDOS attack can hinder normal access to a computer or restrict its intended functioning, section 59(1A)(a) is couched in broader terms. In *HKSAR v Chu Tsun Wai*,[26] the Court of Final Appeal ("**CFA**") held that the "functions" for which a computer is established to do are not so much concerned with the way it works, or fails to work, but what it was intended to do. In that case, the defendant's conviction for participating in a DDOS attack on a bank's website was upheld, notwithstanding that the attack failed because the server had enough surplus capacity to prevent the attack from impacting its other operations.

73. Separately, a DDOS attack may, in principle, also engage section 59(1A)(c)[27] on account of the log record that the target computer system generates in response to the attack.

The Sub-committee's views

Tackling data and system interference consistently

74. Hong Kong law currently addresses illegal interference of computer data and that of computer system mainly by treating both as "misuse of a computer", which is a form of criminal damage. The partial overlap of the two types of misconduct justifies such legal position. Overall, the existing statute has functioned satisfactorily.

75. In our view, the consistency of the present regime against data interference and system interference is a virtue and should be preserved. Accordingly, we recommend that the proposed provisions regarding illegal interference of computer data and that of computer system should be phrased in the same way.

New legislation should adopt the existing provisions

76. We have considered whether one can still rely on judicial authorities based on the current law regarding "misuse of a computer" if this concept is no longer covered by the offence of criminal damage, but rather – as suggested in Recommendation 6(c) – a new and discrete offence not to be found in the CO.

77. Provided sufficient care is given to the drafting of the new legislation with proper reference to the current statutory language, we may take comfort from a faithful reflection of the purpose of the new legislation that after the recommended change, the policy and legislative intent underpinning "misuse of a computer" will remain clear, especially if the opportunity will be taken to codify the underlying legal principles from relevant case law.

Possible clarification of "misuse of a computer"

78. If the relevant provisions will be moved from the CO to the new legislation, this can be an opportunity to refine the statutory concept of "misuse of a computer". For instance, it seems beneficial to:

---

[26] (2019) 22 HKCFAR 30, [2019] HKCFA 3.

[27] See fn 20 and *HKSAR v Chu Tsun Wai* (2019) 22 HKCFAR 30, at 37, [2019] HKCFA 3 (para 18).

(a) clarify whether the new legislation's equivalent of section 59(1A)(a)[28] is engaged if an attack is so destructive that it causes the target computer not to function at all; and

(b) incorporate notions such as "impair the operation of any computer" into the definition of "misuse of a computer".

Scope of application of the proposed offence

79. The new legislation should retain the breadth of the existing law and should not be too restrictive. By way of illustration, apart from the scenarios already covered by the existing law, we consider that the proposed offence should apply to the parties described in Recommendation 7(d) below.

Recommendation 7

The Sub-committee recommends that:

(a) The proposed provisions regarding the illegal interference of 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 of 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 of 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.

[28] See fn 20 above.

Lawful excuse

80. As mentioned earlier,[29] there are always people in cyberspace who are testing others' computers often without the knowledge, let alone authorisation, of the target computer's owner. The tools for conducting those tests are readily available. Many types of testing tools exist and they can cause different degrees of intrusion. The critical issue is how the tool is used.

81. We invite submissions on whether scanning (or any similar form of testing) of others' computers should qualify as a lawful excuse with regard to the proposed offence of illegal interference of computer system. As to how the law should balance the interests of cybersecurity practitioners and those of the general public, our tentative thinking is that any loss which a more regulated regime may cause to cybersecurity practitioners appears less extensive than the damage or loss which unauthorised use of testing tools may cause to the administrator and owner of the target computer system.

Recommendation 8

The Sub-committee invites submissions on:

(a) Should scanning (or any similar form of testing) of a computer system on the internet by cybersecurity professionals, for example, to evaluate potential security vulnerabilities without the knowledge or authorisation of the owner of the target computer, be a lawful excuse for the proposed offence of illegal interference of computer system?

(b) Should there be lawful excuse to the proposed offence of illegal interference of computer system for non-security professionals, such as:

(i) web scraping by robots or web crawlers initiated by internet information collection tools, such as search engines, to collect data from servers without authorisation by connecting to designated protocol ports (eg ports as defined in RFC6335);[30] and/or

(ii) scanning a service provider's system (which has the possibility of abuse or bringing down the system) for the purpose of:

[29] See para 30(a) above.

[30] Information about RFC6335 is available on the website of the Internet Engineering Task Force, at https://datatracker.ietf.org/doc/rfc6335/ (accessed on 3 May 2022).

(1) identifying any vulnerability for their own security protection, for example, whether the encryption for a credit card transaction is secure before they, as private individuals, provide their credit card details for the transaction; or

(2) ensuring the security and integrity of an Application Programming Interface offered by the service provider's system?

Chapter 6: Making available or possessing a device or data for committing a crime

82. The actual use of devices or data (such as a degausser, a password cracker or software for carrying out a penetration test) to commit cybercrime would already be punishable for the particular cyber-dependent offence(s) as proposed. Broadly speaking, a distinct offence in respect of making available or possessing such devices or data would seek to curb the production, supply and possession of devices or data that can be used in cyberspace for illegitimate purposes, and thereby prevent their use for the commission of cybercrime.

Current Hong Kong law

83. Under section 62 of the CO ("**section 62**"), a person who has custody or control of "anything", and intends without lawful excuse to use it (or cause or permit another to use it) to destroy or damage property, shall be guilty of an offence.

84. Section 62 does not differentiate between things which can be used for both legitimate and illegitimate purposes on the one hand, and things with only illegitimate uses on the other. Whether a person with custody or control of a thing in question is liable depends largely on the person's intent. The subjective nature of a person's mental state may give rise to evidentiary issues in enforcement.

85. In addition, the English text of section 62 describes the proscribed object as "anything". This term, in common parlance, is not restricted to tangibles and appears to be broader than the corresponding term in the Chinese text ("任何物品"). However, whether the natural meaning of the Chinese term clearly extends to certain intangibles (such as malware and know-how regarding an exploit) is another question.

86. Moreover, section 62 is linked to the offence of criminal damage under section 60. It does not apply with regard to an offence under another provision, eg section 161 ("*Access to computer with criminal or dishonest intent*").

87. While the TO has no provision corresponding to section 62, it has created a regime for licensing of radiocommunications apparatus. In circumstances where the regime applies, non-compliance is an offence.

88. The regime potentially applies to a computer or a smartphone that can be used to commit cybercrime. However, we consider the regime insufficient. For example, its coverage is narrow, in that it only applies to telecommunication technologies such as radio waves.

The Sub-committee's views

New offence with a basic form and an aggravated form should be enacted

89. In our view, the new legislation should include a provision corresponding to section 62 and the provision should apply to all four cyber-dependent offences discussed in Chapters 2 to 5 in the Consultation Paper.

90. Devices and data with both legitimate and illegitimate uses give rise to challenges similar to those presented by offensive weapons in the physical world. In applying the definition of "offensive weapon" under the Public Order Ordinance (Cap 245):

(a) criminal intent need not be proved and mere possession in a public place suffices for criminal liability in cases involving an article "made" or "adapted" for causing injury to a person; whereas

(b) an article that is neutral by nature would become an offensive weapon only if it is intended by the person having it in his / her possession or under his / her control for such use.

91. Borrowing from the taxonomy above, we recommend splitting the proposed offence into a basic form and an aggravated form. Apart from categorisation of the device or data based on whether it was made or adapted for illegitimate use in a given case, another differentiating factor should be whether criminal intent exists.

Devices and data to which the proposed offence should apply

92. We consider that the proposed offence (the basic and aggravated forms), to be effective in cyberspace, should apply to both tangibles and intangibles. In light of the precedent legislation in New Zealand, the illegitimate use of the devices and data to be prohibited should not be limited to committing cybercrime, but should relate to any offence generally. Based on section 62 and *Chu Tsun Wai*, the proposed offence should apply to a device or data which is believed or claimed to be capable of being used to commit an offence, irrespective of whether that is true or not.

93. In our view, the proposed offence will be too restrictive if it only applies to a device or data without any possible legitimate use. Accordingly, the primary use of a device or data should be determined objectively, regardless of a defendant's subjective intent.

94. We recommend that the basic offence should cover a device or data made or adapted to commit an offence. We further recommend that the aggravated offence should apply to a device or data that is, or is believed or claimed by the perpetrator to be, capable of being used to commit an offence.

Actus reus

95. A market exists for "hacker tools" and similar tools. A comprehensive statutory response to the thriving of such market must target all categories of its participants. We therefore recommend that the *actus reus* of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device or data in question) and the demand side (such as obtaining, possession, purchase and import of a device or data in question).

Mens rea

96. We consider that a person should be guilty of either the basic or aggravated form of the proposed offence only if the person acted with knowledge. A lower threshold – requiring, say, recklessness or no particular mental state at all – seems inappropriate given that it is common for someone to possess software or computer data, or even make it available to others, without knowledge. The coverage of the offence would appear to be unnecessarily broad.

97. If a person is charged with the basic offence on account of the person's belief that the relevant device or data can be used to commit an offence, such belief will form part of the *mens rea* to be established by the prosecution.

98. If a person is charged with the aggravated offence, by definition, the person's intent to use the relevant device or data to commit an offence must be proved in addition to all other aspects of the *mens rea* mentioned in paragraphs 96 and 97 above.

Proposed statutory defence of reasonable excuse

99. Possessing an offensive weapon in a public place constitutes no offence if there is "*lawful authority or reasonable excuse*".[31] To avoid over-criminalisation, we recommend that the proposed offence should likewise incorporate a statutory defence of reasonable excuse, because there can be various legitimate reasons for a person or entity to require devices or data that can be used to commit a crime.

Recommendation 9

The Sub-committee recommends that:

(a) Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code) made or adapted to commit an offence – ie not necessarily cybercrime – should be a basic offence under the new legislation, subject to a statutory defence of reasonable excuse.

[31] Public Order Ordinance (Cap 245), s 33(1), eg where the possessor uses a pole weapon in performing art.

(b) The *actus reus* of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device or data in question) and the demand side (such as obtaining, possession, purchase and import of a device or data in question).

(c) The proposed offence should apply to:

(i) a device or data so long as its primary use (to be determined objectively, regardless of a defendant's subjective intent) is to commit an offence, regardless of whether or not it can be used for any legitimate purposes; and

(ii) a person who believes or claims that the device or data in question could be used to commit an offence, irrespective of whether that is true or not.

(d) Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code):

(i) which is, or is believed or claimed by the perpetrator to be, capable of being used to commit an offence; and

(ii) which the perpetrator intends to be used by any person to commit an offence

should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse.

(e) The proposed provisions should be modelled on section 3A of the CMA-EW as well as sections 8 and 10 of the Computer Misuse Act (Cap 50A) of Singapore.

Possession of data with only harmful use

100. While computer data such as ransomware, virus, software for creating and managing botnets, and harvesting software can only be used to perform a cyber-attack and are harmful, we can see an argument that the law need not (or should not) criminalise their possession for the purposes of, say, education, research, or development of antivirus software. We therefore ask the consultation questions below.

Recommendation 10

The Sub-committee invites submissions on:

(a) Whether there should be a defence or exemption for the offence of knowingly making available or possessing computer data (the software or the source code), such as ransomware or a virus, the use of which can only be to perform a cyber-attack?

(b) If the answer to paragraph (a) is "yes",

(i) in what circumstances should the defence or exemption be available, and in what terms?

(ii) should such exempted possession be regulated, and if so, what are the regulatory requirements?

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

101. In examining the jurisdictional issues associated with cybercrime, the focus is on the criteria for the Hong Kong court to assume jurisdiction.

General principles on jurisdiction

Common law approach

102. In general, for both common law and statutory offences, the courts' criminal jurisdiction is territorial and does not extend to cover acts committed on land abroad.[32]

103. In cases of "result crimes" where a defendant does a prohibited act producing a prohibited result, and the act and the result occur in two different jurisdictions, the traditional view was that the offences were deemed to have been committed only in the place where the offence was completed, ie where the final essential element occurred.

104. However, various common law jurisdictions have now embraced some form of approach that is more flexible. The Hong Kong courts have endorsed the approach in England and Wales, whereby the courts can assume jurisdiction if:

(a) the last act took place in the jurisdiction, or a substantial part of the crime was committed in the jurisdiction; and

(b) there is no reason of comity why it should not be tried in the jurisdiction.

[32] Nevertheless, many states have claimed jurisdiction over offences committed upon ships flying their flags and aircraft registered under their laws. See the Explanatory Report to the Convention on Cybercrime, at para 235.

Hong Kong legislation prescribing jurisdictional rules

105. Section 2(2) of the Criminal Jurisdiction Ordinance (Cap 461) ("**CJO**") defines certain substantive offences of fraud and dishonesty as Group A offences. Section 3 of the CJO provides that a person may be guilty of a Group A offence so long as any "relevant event" – ie 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 essential elements of the offence occurred elsewhere.

106. The Government's proposal in 2002 to add three computer offences[33] to the list of Group A offences was not implemented due to a lack of support from the relevant Subcommittee of the Legislative Council.

107. There are also some other Ordinances which contain provisions on jurisdictional issues with regard to specific offences.[34]

Generally accepted bases of extra-territorial jurisdiction

108. There are four generally accepted bases of extra-territorial jurisdiction:

(a) The active personality principle (based on a perpetrator's nationality);

(b) The passive personality principle (based on a victim's nationality);

(c) The universality principle (ie any state should have jurisdiction over the most serious offences, such as crimes against humanity); and

(d) The protective principle (ie a state should have jurisdiction over an act which threatens its national security or interest, even if the act occurred outside the state).

Jurisdictional issues associated with cybercrime

Challenges presented by cybercrime and recognised by courts

109. The financial and technological thresholds to launch a cross-jurisdictional attack in cyberspace are low. Partly due to this, cybercrime often involves multiple jurisdictions. Determining where a fact occurred is potentially difficult. The courts have long recognised the jurisdictional issues often found in cybercrime.[35]

110. Resolution of jurisdictional conflicts is a key area in the international effort against cross-border crimes. In practice, consultation among the affected places has been the solution, and some regional instruments provide guidance on the factors that

---

[33] These offences were "unauthorized access to computer by telecommunications" under s 27A of the Telecommunications Ordinance, "destroying or damaging property" relating to misuse of a computer under ss 59 and 60 of the CO and "access to computer with criminal or dishonest intent" under s 161 of the CO.

[34] See, for instance, ss 153P and 153Q of, read together with Schedule 2 to, the CO and s 4 of the Prevention of Bribery Ordinance (Cap. 201).

[35] For instance, in *DPP v Sutcliffe* [2001] VSC 43, at paras 62-63, the Supreme Court of Victoria (Australia) acknowledged that the "*Internet provides a speedy, relatively inexpensive means of communications between persons*" and that access "*is not confined to ownership of a computer … The law must move with these changes.*"

may be taken account of during legal cooperation among states.[36] Pending the conclusion of any such bilateral agreements for Hong Kong (which requires the authorisation of the Central People's Government),[37] we envisage that if our recommendations are implemented, the relevant law enforcement agency and the prosecutorial authority will invoke the jurisdictional rules that the new cybercrime legislation prescribes for each of the five cyber-dependent offences,[38] bearing in mind that the rule against double jeopardy applies to a previous conviction or acquittal in another jurisdiction as it does to one in Hong Kong.[39]

The Sub-committee's views

Preliminary considerations

111. We consider that the nature of cybercrime justified extra-territorial application of Hong Kong law. The new legislation should expressly prescribe a broad range of jurisdictional rules which apply to the offences created by it. The prosecution retains a discretion as to whether a charge should be brought. This would also offer protection to the public which aligns with our guiding principle.

112. It is also 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. We discussed the offences proposed in the Consultation Paper with reference to the following fact patterns:

(a) Any "essential element" of the offence occurred in Hong Kong, even if other "essential element(s)" occurred elsewhere (cf section 3, CJO);

(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

---

[36] For example, Article 10(4) of the Council Framework Decision 2005/222/JHA on attacks against information systems in the European Union and Article 30(3) of the Arab Convention on Combating Information Technology Offences (21 Dec 2010) set out the following factors:
(i) the state whose security or interests were disrupted by the offence;
(ii) the state in whose territory the offences have been committed;
(iii) the state of which the perpetrator is a national;
(iv) the state in which the perpetrator has been found; and
(v) (in case of similar circumstances) the first state that requests the extradition.

[37] Under the Basic Law, the Central People's Government is responsible for the foreign affairs relating to Hong Kong and Hong Kong is authorised to conduct relevant external affairs (ie in the economic, trade, financial and monetary, shipping, communications, tourism, cultural and sports fields as stipulated in Article 151) on its own.

[38] The jurisdictional rules proposed for the five cyber-dependent offences are summarised in Recommendations 11, 12, 13, 14 and 15 respectively. See paras 113 to 127.

[39] The rule against double jeopardy applies to barring the prosecution of a person if he has been previously acquitted or convicted of an offence and is later charged with the same offence. The rule also applies to previous conviction or acquittal in another jurisdiction. As the CFA confirmed in *Yeung Chun Pong & Others v Secretary for Justice* (2009) 12 HKCFAR 867, there is a discretionary power to stay a prosecution as an abuse of process where "*a person faces a second trial arising from the same or substantially the same set of facts as gave rise to an earlier trial (whether in the same jurisdiction or in a competent court in another jurisdiction)*" (para 21).

threatened or may threaten the security of Hong Kong.

Illegal access to program or data

113. It appears uncontroversial to us that fact patterns (a), (d) and (e) should apply. We discuss fact patterns (b) and (c) below.

114. We recommend against applying fact pattern (b) because it covers cases where the harm is not suffered by any "Hong Kong person".[40] Law enforcement agencies in the affected jurisdiction will probably take action if a case is serious.

115. In our view, applying fact pattern (c) would be useful for the protection offered by the proposed offence. As cybercrime may involve parties in multiple jurisdictions, the concept of victim should be broadly defined in that, for example, if a cloud server holds data belonging to a person from another jurisdiction, both the server owner and data owner should be taken as potential victims. Consistent with the focus of the proposed offence, we have concluded in favour of maximising the protection offered in this manner because the emphasis should be on the data to be protected.

116. We consider that requiring double criminality may defeat the purpose of strengthening protection of the general public. One may seek to evade liability by deliberately launching a cyber-attack at a place where it constitutes no crime. We suggest applying the double criminality requirement to the *summary* offence of illegal access of program or data, but not the *aggravated* offence. In sum, we take the view that where a perpetrator is charged with the proposed 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 proposed offence, must constitute a crime in the jurisdiction where it was done.

Recommendation 11

The Sub-committee recommends 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 a company carrying on business in Hong Kong;

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

[40] Eg where the perpetrator ("albeit a Hong Kong person"), his or her act, the device used, the data in question and the victim are all outside Hong Kong.

(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.

Illegal interception of computer data

117. For similar reasons, we recommend that fact patterns (a), (c), (d) and (e) should apply to the proposed offence of illegal interception of computer data.

118. We recommend against applying fact pattern (b) because the points which we raised above in connection with the first proposed offence – ie the harm is likely done not to any "Hong Kong person", and prosecution in Hong Kong may be impractical – are equally valid here.

119. For consistency, we opine that double criminality should not be required of this proposed offence, which is more analogous with the aggravated offence of illegal access to program or data than the summary offence.

Recommendation 12

The Sub-committee recommends 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 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.

Illegal interference of computer data

120. Again, we believe that applying fact patterns (a), (c), (d) and (e) to the proposed offence of illegal interference of computer data should be uncontroversial.

121. Since we have recommended against applying fact pattern (b) to the first two proposed offences, we likewise recommend against applying fact pattern (b) to this proposed offence.

122. We further observe that not applying the double criminality requirement to this proposed offence will be consistent with our recommendations regarding the first two proposed offences.

Recommendation 13

The Sub-committee recommends that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference 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 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.

Illegal interference of computer system

123. Our recommendation is to treat this proposed offence and the preceding one in the same way. The close relationship between the two proposed offences suggests that they should have the same jurisdictional reach. We also recommend that double criminality should not be required of this proposed offence.

Recommendation 14

The Sub-committee recommends that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference of 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 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.

Making available or possessing a device or data for committing a crime

124. We have recommended that this proposed offence should include a basic form and an aggravated form, based on whether a defendant intends the device or data in question to be used by any person to commit an offence. While the severity of the two forms varies, the gap is not so wide as to justify the two forms having different jurisdictional rules. We suggest that the same jurisdictional rules should apply to both forms.

125. A case of this proposed offence may not involve any victim or any target computer, program or data, which fact patterns (c) and (d) presuppose respectively. We thus take these fact patterns as inapposite for this proposed offence.

126. As regards the limb of *possessing* a device or data, to state that the device or data is possessed at the location of the individual with possession may not reflect reality if the device or data is stored in, say, a cloud server. As regards the limb of *making available* a device or data, a piece of malware uploaded onto the internet can theoretically be available to anyone anywhere in the world with internet access. Thus, we recommend that fact patterns (a), (b) and (e) should apply to this proposed offence.

127. Save for the summary offence of illegal access to program or data, we have recommended that double criminality should not be required of the first four proposed offences. We consider that the same reasoning and hence recommendation apply to the proposed offence of making available or possessing a device or data for

committing a crime.

Recommendation 15

The Sub-committee recommends that, in respect of the proposed offence of making available or possessing a device or data for committing a 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 or data for committing an offence;

(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

128. The appropriate maximum sentences for the proposed offences are recommended after examining the views of Hong Kong courts towards cybercrime. The maximum sentences for the corresponding cybercrime offences in Hong Kong and other jurisdictions are summarised in the Appendix to the Consultation Paper.

129. To summarise, the courts have consistently regarded cases of intrusion, damage or misuse of computer as serious. For example, the Appeal Committee of the CFA has noted that deliberate damage to computer software and data should ordinarily attract a custodial sentence.[41]

The Sub-committee's views

The relatively serious proposed offences

130. In view of the significant harm that can be caused by the non-summary offences proposed in the Consultation Paper, we favour setting uniform maximum sentences for:

[41] *Liu Wai Shun v HKSAR*, FAMC 30/2004 (date of judgment: 27 Sept 2004), at para 7.

(a) The proposed aggravated offence of illegal access to program or data (Chapter 2);

(b) The proposed offence of illegal interception of computer data (Chapter 3);

(c) The proposed basic offences of illegal interference of computer data and illegal interference of computer system (Chapters 4 and 5); and

(d) The proposed aggravated offence of making available or possessing a device or data for committing a crime (Chapter 6).

131. Recognising that the severity of the harm caused by cybercrime has a wide range, we recommend that each of the proposed offences in (a), (b), (c) and (d) of the preceding paragraph should have two maximum sentences, one applicable to summary convictions and the other to convictions on indictment.

132. We deliberated having regard to the respective sentencing jurisdiction of various levels of court, as well as the maximum sentences for existing cybercrime offences, certain representative types of crimes in the Theft Ordinance (Cap 210), and comparable offences in other jurisdictions. We consider that our recommended maximum sentence (14 years' imprisonment) for the proposed offences identified in paragraph 130 above will have the necessary deterrent effect and is not too out of tune with the references noted by us.

133. We further opine that a maximum sentence of imprisonment for two years on summary conviction would be proportionate to our recommendation with regard to cases of conviction on indictment.

The proposed summary offence of illegal access to program or data

134. The nature of this proposed offence is, to an extent, comparable to the offence under section 27A. However, section 27A has rarely been invoked and its maximum sentence (a fine at level 4, currently $25,000) appears rather light. In our view, there should be the possibility of imprisonment even in summary cases. We recommend a maximum sentence of imprisonment for two years for this proposed offence.

The proposed aggravated offences of illegal interference of computer data and computer system

135. For consistency with the offence of criminal damage, we suggest adopting the maximum sentence now prescribed by section 63(1) of the CO, ie imprisonment for life, for the proposed aggravated offences of illegal interference of computer data and that of computer system.

The proposed basic offence of making available or possessing a device or data for committing a crime

136. As the basic offence applies to a device or data made or adapted to commit an offence, we consider that it should be regarded as serious and be punishable by imprisonment for seven years, which would lay halfway when compared with the recommended maximum sentence for the related aggravated offence.

Recommendation 16

The Sub-committee recommends 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 of computer data and illegal interference of 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 or possessing a device or data for committing a crime, 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.