Hong Kong Internet Service Providers Association
HKISPA

By Email to: *hklrc@hkreform.gov.hk*

18 October 2022

Dear Sir/Madam,

HKISPA's response to
Consultation Paper on CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

I am writing on behalf of HKISPA in response to your consultation paper of the captioned subject, published by the Law Reform Commission of Hong Kong in June 2022.

Essence of our response is summarised below.

(i) Re: Recommendations 9 and 10 on "possession of ransomware or viruses", the HKISPA strongly requests further clarity on "reasonable excuse", and recommends amendments to require actual criminal acts as conditions for conviction rather than simply by mere possession.

(ii) Re: Recommendation 6 on "intentional interference", HKISPA requests that ISPs be explicitly exempted, unless dishonest or criminal acts were found.

(iii) Re: Recommendations 4 and 5 on "interception", HKISPA requests that ISPs should be explicitly exempted, unless dishonest or criminal acts were found.

(iv) Re: Recommendations 1, 2, 8, we suggest a framework to qualify what is legitimate "cyber security operations/purposes".

Details of our response and relevant rationales are set out below.

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.

HKISPA's Response to Recommendation 1

1. We welcome the provision of a statutory defence of reasonable excuse, which we see as an improvement over the CMA-EW model, although the scope of "reasonable excuse" is not clearly defined.

2. ISPs often initiate network maintenance operations, where such operations may be interpreted as unauthorised access attempts to the network or devices of both their connected customers and to networks outside of the ISP's own perimeter due to the connectedness of the Internet. We strongly recommend that "network scanning from

Internet Service Providers for operational reasons" be explicitly defined and included in the scope of "reasonable excuse".

3. It is also the commonly accepted mode of operation of the cyber security industry that automatic and uninvited probes, either from within HK or outside of HK, be done continually to discover common and simple vulnerabilities, like outdated web server software on a connected computer. Network operators or public Internet users in general can subscribe to such services, often free of charge, and see the common vulnerabilities of both their own network and other's networks. While this seems not a normally accepted practice when contrasted with the real-world counterpart of finding faulty door-knobs of all houses and let the world access such information for free, it is however an accepted practice in the Internet space and it actually has helped improve the overall network security of the global Internet.

4. On the other hand, we also acknowledge that real cyber criminals may also do similar operations, of launching massive uninvited scans to find vulnerable botnet computers.

5. To address the practical dilemma of such situations, we recommend that "cyber security operations" be explicitly accepted into the scope of "reasonable excuse", but prescribe additional requirements to qualify what are "cyber security operations", as iterated in the following paragraph.

6. We recommend that any uninvited network probes, scans or access attempts have to comply with all these requirements in order to be classified as "cyber security operations" or "for cyber security purposes".

   I. The operation should cause no disruption to the normal operation of the targets; and
   II. Network vulnerabilities found shall be timely and proactively disclosed to the concerned parties before making available to any other parties; and
   III. Software vulnerabilities found shall follow the typical responsible disclosure protocol with software developers; and
   IV. Records of such operations and disclosures shall be kept and available to be validated.

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:

(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, 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 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))[112]?

HKISPA's Response to Recommendation 2

7. We can all agree that the cybersecurity profession and the global Internet are quickly changing. Each year, service providers, software companies or cyber security bodies design and offer new accreditation programs; and each year, new technologies and applications get introduced (lets name NFT, blockchain, metaverse) which may create new modes of cyber security problems that we cannot accurately predict. Designing an accreditation regime in the form of legislation or to be operated by a local statutory body may not be able to adapt to changes timely, and globally.

8. Therefore, Re: Recommendation 2(a)(ii), we do not prefer an additional accreditation regime to be introduced through the legislation.

9. But we also believe constraints and requirements are necessary to be spelled out explicitly to qualify what are "cyber security purposes".

10. Re: Recommendation 2(a)(iii), likewise to our response to Recommendation 1, we recommend that defence or exemptions for unauthorised access should be explicitly provided for "cyber security purposes", but conform to additional requirements as prescribed in paragraph 6 to qualify what operations are for "cyber security purposes".

11. Re: Recommendation 2(b), we recommend that such defence and exemptions for "cyber security purposes" should also be made available to non-security professionals, provided the same additional requirements in paragraph 6 are satisfied. For reference, defendant Mr Chan of WKS6208/2019 who discovered the vulnerability of the airline's website would have been acquitted with our above recommendation.

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, including the *mens rea* (ie to intercept "intentionally").

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)?

HKISPA's Response to Recommendations 4 and 5

12. Service providers intercept data on a daily basis. They intercept email data to remove viruses for their customer, intercept network metadata for resources planning purposes.

13. We believe that Recommendation 4(a), where the prosecution has to proof "dishonest or criminal purpose" to convict the interception as a crime, is sufficient to protect the normal operation of service providers.

14. Regarding Recommendation 4(c), we have to stress that ISPs interception are all intentional. To avoid any confusion, we recommend that the wording be clearly defined, of "dishonest or criminal purpose" as a prerequisite mens rea, rather than just "to intercept intentionally".

15. Regarding Recommendation 5(a), we believe Internet service providers should be explicitly exempted for interception as it is their ordinary and legitimate operation.

16. Regarding Recommendation 5(b), we believe there need not be any restrictions on coffee shops or shopping malls which offer free Wifi, because the data the coffee shop or shopping mall could gather are not personal data as encryption between the end-user and the server is now norm. The data the coffee shop and shopping malls could intercept through the free Wifi are only metadata. We believe they should be allowed to intercept and use the metadata being transmitted without incurring any criminal liability, provided that "dishonest or criminal" use of the data are not found.

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.

(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).

HKISPA's Response to Recommendation 6

17. ISPs remove email viruses for customers, by definition it is intentional alteration of computer data.

18. Therefore, we strongly recommend that "Normal course of operation of Internet Service Providers" be enlisted explicitly as reasonable excuse, or otherwise amend this offence with "dishonest or criminal purpose" as a requirement for conviction.

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);81 and/or

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

(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?

HKISPA's Response to Recommendation 8

19. Regarding Recommendation 8(a), following the same line of recommendations, we recommend that "cybersecurity purposes" should be lawful excuse for scanning or similar form of testing of a computer system on the Internet without the knowledge or authorisation of the owner of the target computer, provided that the requirements as iterated in paragraph 6 be conformed to.

20. Regarding Recommendation 8(b)(i), we believe simple probes by search engines, or by any person, to well-known and designated protocol ports should be legal and allowed, because such protocol ports are designed to be used for such purposes, of being probed for services.

21. Regarding Recommendation 8(b)(ii), we recommend that uninvited scanning should be open, legal and available to professionals or non-professionals alike, provided that the four requirements as iterated in paragraph 6 be verifiably met.

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.

(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 CMA-SG.

HKISPA's Response to Recommendation 9

22. There are two mentions of "subject to a statutory defence of reasonable excuse", but there is no concrete definition of what constitutes reasonable excuse.

23. While we see a piece of software or code residing on the network of an ISP should not constitute possession by the ISP concerned, we have grave concern if the law may be interpreted otherwise and cause unnecessary legal struggles to any service provider.

24. There may be scenarios where the ISP provides network hosting space for its clients, and the client connects a device to the network.

25. And there may be scenarios the ISP provides cloud hosting space for clients, where malicious code is uploaded for distribution.

26. Additionally, our email servers obviously holds many malware, viruses and ransomware which are detached from our customers' emails. Such malicious codes may be used to train our spam filters. We have grave concern if such would be interpreted as "knowingly" "possession" of such codes, as it conforms to the legal definition of possession as cited in the consultation paper, which stated that:

"*A person may be held to be in possession of a thing if sufficient evidence is forthcoming to demonstrate both physical control over it, in the sense of ability to use as may be desired, within the parameters of practicality and the law, and to exclude others, and of an intention to exercise such control.".*

27. Therefore we strongly recommend that the law should explicitly provide that "A piece of software, device, data, or program residing on or connected to the network of an internet service provider (ISP) as a result of providing service to any of its customers shall not constitute possession of the same by the internet service provider concerned". This should be spelled out explicitly in the definition of "statutory defence of reasonable excuse".

28. ISPs, cyber security professionals all have in their control some virus codes in this category. Therefore, as an alternative to paragraph 26 above, we recommend LRC to consider that mere possession of a device or data should not constitute crime. That is, remove Recommendations 9(a), (b) and (c), and leave only Recommendations 9(d) which requires proof of intent.

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?

HKISPA's Response to Recommendation 10

29. There are scenarios where a service provider or a cyber security professional knowingly possess ransomware or viruses.

30. ISPs email servers obviously holds many malware, viruses and ransomware, and ISPs know about it. Such codes may be used to train our spam filters. We have grave concern if such would be interpreted as "knowingly" "possession" of such codes, as it conforms to the legal definition of possession as cited in the consultation paper, which stated that:

"*A person may be held to be in possession of a thing if sufficient evidence is forthcoming to demonstrate both physical control over it, in the sense of ability to use as may be desired, within the parameters of practicality and the law, and to exclude others, and of an intention to exercise such control.".*

31. Therefore, regarding Recommendation 10(a), we strongly recommend that "Exemptions shall be provided to service providers and cybersecurity professionals for operational reasons to be in possession of ransomware or viruses".

32. Regarding Recommendation 10(b)(i), we believe exemptions should be made available to all service providers, if attacks have not been launched with the ransomware or viruses.

33. Regarding Recommendation 10(b)(ii), we believe such exemption for possession should be open to all service providers and not be regulated, as what constitutes ransomware or virus cannot be clearly defined with quickly evolving technologies.

34. Therefore, in conclusion regarding Recommendation 9 and 10, we believe a service provider or a cyber security entity should be exempted to have in their possession or control ransomware or viruses. An entity should only be proven guilty if the actual intent or the actual act to launch attacks can be proven.

Thank you for your kind attention.

Lento Yip
Chairman
Hong Kong Internet Service Providers Association