Comments from Information Security and Forensics Society (ISFS) in respect of the Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues

18 October 2022

(1) Illegal access to program or data

Recommendations

9.3 Subject to a statutory defence of reasonable excuse, unauthorised access to program or data should be a summary offence under a new piece of bespoke legislation on cybercrime. *[Recommendation 1(a)]*[1]

ISFS Comments:

Disagree.

- An unauthorised access to data without criminal intent should not be a criminal offence. It may be an inadvertent act, or just because of curiosity, eg,
(i) A person picked up a USB flash drive in the street, waited for a moment, but no one came to look for it. S/he then used his/her notebook computer to check the contents of the USB drive because of curiosity (wished to know what was contained inside). S/he did not take away the USB drive, but left it in the street hoping the owner would come back and take it.
Under this new legislation, s/he might have committed an offence – unauthorised access to data.
S/he would have committed no offence if s/he just picked up a book or a physical file in the street, looked at it, and then left it behind.

(ii) A student opened a schoolmate's homework file (in a computer), without his/her consent, but because of curiosity, to see if s/he had completed his/her work……could be unauthorised access to data

Curiosity may not be a reasonable excuse…. but it will be a nightmare to those mentioned above if they were arrested, charged (however unlikely) and/or convicted….

- Unauthorised access to program or data with intent to carry out further criminal activity, as recommended in 9.4 below, should be sufficient to cover possible crimes under unauthorised access.

1 Paras 2.89 to 2.106.

9.4 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. *[Recommendation 1(b)]*[2]

ISFS Comments:

Agree.

9.5 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

(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. *[Recommendation 11]*[3]

ISFS Comments:

Regarding the jurisdiction of court, it can be defined by Hong Kong, but we also need to consider the jurisdiction of other countries. Also it depends on how evidence could be collected.

2 Paras 2.107 to 2.108.
3 Paras 7.71 to 7.81.

9.6 An offender should be liable to the following maximum sentences:

(a) for the summary offence, imprisonment for two years; or

(b) for the aggravated offence, imprisonment for 14 years on conviction on indictment. *[Recommendation 16(a)]*[4]

ISFS Comments:

No comments.

9.7 The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the Computer Misuse Act 1990 in England and Wales. *[Recommendation 1(c)]*[5]

ISFS Comments:

No comments.

Consultation questions

9.8 Should there be any specific defence or exemption for unauthorised access?

ISFS Comments:

An unauthorised access to data without criminal intent should not be a criminal offence.

If there are grey areas, the following access should be exempted:

- Any authorized cases through contract or organization's internal policy
- If the access is for public interest/benefit
- If the access does not expose Personal Identifiable Information (PII)
- If the access is related to whistleblowing cases
- If the purpose of access is for research usage

4 Paras 8.12 to 8.18.
5 Para 2.109.

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

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

ISFS Comments:

Agree to establish an accreditation body for accrediting cybersecurity professionals.

However, establishing an accreditation body should not be linked or related to the exemption or defence of unauthorised access because (a) all business related cybersecurity service is considered to be authorized services; and (b) most access cases that should be exempted would be related to whistleblowing or research purposes. If it is related to research or whistleblowing, it should not be bound by any cybersecurity professional and accreditation requirements.

(b) If the answer to sub-paragraph (a) is yes, how should the accreditation regime work, eg what are the criteria for such accreditation? Should 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?

ISFS Comments:

1. Establishing an accreditation body would be helpful to Hong Kong as a whole, but it should not be tied up with any the cybercrime aspects. It should be tied up with the professionalism, ethics and qualification of practitioners.

2. In order to establish the cybercrime accreditation body, it is necessary to form an organization similar to CSA of Singapore with the rights to establish cybersecurity policies of HK.

(c) 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?

ISFS Comments:

Anything related to cybersecurity research and other researches involving cybersecurity and forensics research.

9.10 Should the defence or exemption apply to non-security professionals (please see the examples in Recommendation 8(b)) [6] ? *[Recommendation 2]*[7]

ISFS Comments:

Yes.

(2) Illegal interception of computer data

Recommendations

9.11 Unauthorised interception, disclosure or use of computer data carried out for a dishonest or criminal purpose should be an offence under the new legislation. *[Recommendation 4(a)]*[8]

ISFS Comments:

Yes. The new legislation should be enacted to prevent crime, so criminal intent should be required. If there is no criminal purpose, interception of computer data should not be an offence.

6 Para 9.30.
7 Paras 2.110 to 2.120.
8 Paras 3.92 to 3.99.

9.12 The proposed offence should:

(a) protect communication in general, rather than just private communication;

(b) apply to data generally, whether it be metadata or not; and

(c) 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. *[Recommendation 4(b)]*[9]

ISFS Comments:

Firstly, for this proposed offence, there must be a criminal intention. Also, it should only protect private communication as communication in general is too broad in the cyberworld and the so called protection may unnecessarily disturb proper communication.

Interception of computer data should not be considered as an offence if the network architecture is implemented to include interception of network such as Intrusion Detection, web application firewall protection or proxy server, etc. Those security design requirements should be exempted, ie they are not illegal interception.

9.13 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;

9 Paras 3.100 to 3.110.

(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. *[Recommendation 12]*[10]

ISFS Comments:

Regarding the jurisdiction of court, it can be defined by Hong Kong, but we also need to consider the jurisdiction of other countries. Also it depends on how evidence could be collected.

9.14 An offender should be liable to imprisonment for two years on summary conviction and 14 years on conviction on indictment. *[Recommendation 16(b)]*[11]

ISFS Comments:

2 years imprisonment for summary conviction of cases related to this offence is too heavy. A maximum penalty of six months for this summary offence is more appropriate.
14 years on conviction on indictment is fine.

9.15 The proposed provision should, subject to paragraphs 9.11 and 9.12 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 4(c)]*[12]

ISFS Comments:

Interception of computer data should only be considered as an offence if there is criminal intent.

Consultation questions

9.16 Should there be a defence or exemption for professions who have

10 Paras 7.82 to 7.88.
11 Paras 8.12 to 8.16.
12 Paras 3.111 to 3.112.

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)?

ISFS Comments:

Yes. Interception of computer data should not be considered as an offence if there is no criminal intent.

9.17 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)? [*Recommendation 5]*[13]

ISFS Comments:

Yes. Interception of computer data should only be considered as an offence if there is criminal intent.

(3) Illegal interference of computer data

Recommendations

9.18 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.

ISFS Comments:

Interference of computer data should only be considered as an offence if there is criminal intent.

9.19 The new legislation should adopt the following features under the

13 Paras 3.113 to 3.122.

Crimes Ordinance (Cap 200):

(a) the *actus reus* under section 59(1A)(a), (b) and (c);[14]

(b) the *mens rea* under section 60(1) (which requires intent or recklessness, but not malice);

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

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

ISFS Comments:

(a) Agree.

(b) Disagree.

'Malice' should be required because the maximum penalty, 14 years imprisonment, is severe.

(c) Agree.

(d) Agree.

9.20 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). *[Recommendation 6]*[15]

ISFS Comments:

No comments.

14 S 59(1A) defines "misuse of a computer" to mean the following acts:
"*(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."

15 Paras 4.81 to 4.99.

9.21 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. *[Recommendation 13]*[16]

ISFS Comments:

Regarding the jurisdiction of court, it can be defined by Hong Kong, but we also need to consider the jurisdiction of other countries. Also it depends on how evidence could be collected.

9.22 An offender should be liable to the following maximum sentences:

(a) for the basic offence, imprisonment for two years on summary conviction and 14 years on conviction on indictment; or

(b) for the aggravated offence, imprisonment for life. *[Recommendation 16(c)]*[17]

ISFS Comments:

(a) No comments.

(b) Disagree.

Life imprisonment, the penalty for murder and similar extremely serious criminal offences, is far too severe for illegal interference of computer data.

16 Paras 7.89 to 7.91.
17 Paras 8.12 to 8.16, 8.19 to 8.20.

(4) Illegal interference of computer system

Recommendations

9.23 The proposed provisions regarding the illegal interference of computer data and computer system should be phrased in the same way.

ISFS Comments:

Interference of computer system should only be considered as an offence if there is criminal intent.

9.24 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.

ISFS Comments:

No comments.

9.25 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”).

ISFS Comments:

Disagree.

Should adopt the features under the Crimes Ordinance (Cap 200) with reference to Sections 59(1A) and 60 of the Crimes Ordinance.

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

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

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

(c) 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. *[Recommendation 7]*[18]

ISFS Comments:

Interference of computer data should only be considered as an offence if there is criminal intent. Therefore, the act must be intentional. "Reckless" should be removed.

9.27 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. *[Recommendation 14]*[19]

ISFS Comments:

Regarding the jurisdiction of court, it can be defined by Hong Kong, but we also need to consider the jurisdiction of other countries. Also it depends on how evidence could be collected.

9.28 An offender should be liable to the following maximum sentences:

(a) for the basic offence, imprisonment for two years on summary

18 Paras 5.61 to 5.68.
19 Paras 7.92 to 7.93.

conviction and 14 years on conviction on indictment; or

(b) for the aggravated offence, imprisonment for life. *[Recommendation 16(c)]*[20]

ISFS Comments:

(a) No comments.

(b) Life imprisonment, the penalty for murder and similar extremely serious criminal offences, is far too severe for illegal interference of computer system.

Consultation questions

9.29 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?

ISFS Comments:

Yes, such scanning/testing should not be considered as an illegal act. There must be a criminal intention for it to be illegal.

9.30 Should there be lawful excuse to the proposed offence for non-security professionals, such as:

(a) 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); and/or

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

(i) identifying any vulnerability for their own security

20 Paras 8.12 to 8.16, 8.19 to 8.20.

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

(ii) ensuring the security and integrity of an Application Programming Interface offered by the service provider's system? *[Recommendation 8]*[21]

ISFS Comments:

Yes, there must be a criminal intention for any such act to become illegal. Non-criminal related action/interference should not be considered as an offence.

(5) Making available or possessing a device or data for committing a crime

Recommendations

9.31 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. *[Recommendation 9(a)]*[22]

ISFS Comments:

Disagree.

1) Merely possessing such devices or knowingly making them available should not be an offence. There must be a criminal intention.

2) This proposed offence should only be applied when it is proven that there has been:

(i) illegal access to program or data with intent to carry out further criminal activity;

(ii) illegal interception of computer data;

21 Paras 5.69 to 5.72.
22 Paras 6.73 to 6.79, 6.83 to 6.84, 6.86 to 6.87.

(iii) illegal interference of computer data; or

(iv) illegal interference of computer system.

9.32 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). *[Recommendation 9(b)]*[23]

ISFS Comments:

No comments.

9.33 The proposed offence should apply to:

(a) 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

(b) 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. *[Recommendation 9(c)]*[24]

ISFS Comments:

Disagree.

It must be proven that the only use of the tool(s) is for criminal purposes, and the criminal act has actually been performed.

Most tools, such as port scanning or network scanning devices, or password crackers, which are capable of being used for committing cybercrime, are not intentionally developed for criminal purposes. Port scanning or network scanning devices are used for determining the open network ports at the target machines. Many times, network development teams would need to rely on these tools to validate the network connectivity of the services for legitimate purposes. Also, password crackers are used to help data owners recover important data and could also be used by hackers for illegal purposes.

23 Paras 6.81 to 6.82.
24 Paras 6.76 to 6.77, 6.84.

Therefore, the presence of criminal intent is absolutely necessary and a mere possession or making it/them available should not be regarded as an offence.

9.34 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):

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

(b) 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. *[Recommendation 9(d)]*[25]

ISFS Comments:

It must be proven that the only use of the tools, either device or data, is for criminal purposes, and the criminal act has actually been performed.

9.35 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. *[Recommendation 15]*[26]

25 Paras 6.73 to 6.80, 6.83, 6.85 to 6.87.
26 Paras 7.94 to 7.100.

ISFS Comments:

Regarding the jurisdiction of court, it can be defined by Hong Kong, but we also need to consider the jurisdiction of other countries. Also it depends on how evidence could be collected.

9.36 An offender should be liable to the following maximum sentences:

(a) for the basic offence, imprisonment for two years on summary conviction and seven years on conviction on indictment; or

(b) for the aggravated offence, imprisonment for 14 years on conviction on indictment. *[Recommendation 16(d)]*[27]

ISFS Comments:

No comments.

9.37 The proposed provisions should be modelled on section 3A of the Computer Misuse Act 1990 in England and Wales as well as sections 8 and 10 of the Computer Misuse Act 1993 in Singapore. *[Recommendation 9(e)]*[28]

ISFS Comments:

No comments.

Consultation questions

9.38 Should there 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?

ISFS Comments:

1) Merely possessing such devices or knowingly making them available should not be an offence. There must be a criminal intention.

27 Paras 8.12 to 8.16, 8.21 to 8.23.
28 Para 6.88.

2) This proposed offence should only be applied when it is proven that there has been:

(i) illegal access to program or data with intent to carry out further criminal activity;

(ii) illegal interception of computer data;

(iii) illegal interference of computer data; or

(iv) illegal interference of computer system.

9.39		If the answer to the question above is "yes",
	(a)	in what circumstances should the defence or exemption be available, and in what terms?

ISFS Comments:

Same as 9.38 above.

	(b)	should such exempted possession be regulated, and if so, what are the regulatory requirements? *[Recommendation 10]*[29]

ISFS Comments:

Same as 9.38 above.

29 Paras 6.91 to 6.93.

(6) Limitation period for summary proceedings

Recommendation

9.40 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). *[Recommendation 3]*[30]

ISFS Comments:

Disagree.

Information Technology develops and changes very rapidly and so does a cybercrime. Such a crime should be stopped as soon as possible or else the harm done could become more and more serious in a short period of time. Also, the rapid development and changes of IT will make the proof difficult if the "crime" is not investigated and dealt with promptly. Therefore, there is no point "deferring" the limitation period from six months to two years for a summary offence. In fact, a six months limitation period may encourage law enforcement agencies to deal with cybercrimes earlier and quicker and protect the interest of the public better.

---

30 Paras 2.121 to 2.123.