Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues published (with photo/video)

The following is issued on behalf of the Law Reform Commission:

The Cybercrime Sub-committee of the Law Reform Commission published the Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues today (July 20), making preliminary proposals for law reform to address the challenges to protection of individuals' rights caused by the rapid developments associated with information technology, the computer and internet, and the potential for them to be exploited for carrying out criminal activities.

This consultation paper comprises the first part of the study on cybercrime. It addresses five cyber-dependent crimes, which are crimes that can be committed only through the use of information and communications technology devices, where such devices are both the tool for committing the crimes and the target of the crimes. The five cyber-dependent crimes are illegal access to program or data, illegal interception of computer data, illegal interference of computer data, illegal interference of computer system, and making available or possessing a device or data for committing a crime.

Currently, no single ordinance in Hong Kong deals with cybercrime specifically. Different offences are covered in the Crimes Ordinance (Cap 200) (CO) and the Telecommunications Ordinance (Cap 106) (TO), some of which are outdated. The Sub-committee has considered the laws of seven other jurisdictions, namely Australia, Canada, England and Wales, Mainland China, New Zealand, Singapore and the United States. A comparative study reveals that these jurisdictions have all provided for the five cyber-dependent crimes and their related jurisdictional issues either by enacting bespoke cybercrime legislation, or dedicating a part of their codified law to cybercrime.

The main recommendations in the paper are:

(i) A new piece of bespoke legislation on cybercrime should be enacted to cover the five types of offences proposed in the paper and to prescribe their applicable jurisdictional rules;

(ii) There should be a new offence of unauthorised access to program or data, subject to a statutory defence of reasonable excuse. This offence would apply no matter whether access to a computer is obtained by telecommunications or not, and would therefore enhance the existing section 27A of the TO (which only targets unauthorised access to a computer by "telecommunications" as defined in that ordinance). In view of the potentially serious harm that an offender may further cause after accessing program or data, the Sub-committee

proposes that unauthorised access with intent to carry out further criminal activity should constitute an aggravated offence;

(iii) There should be a new offence of unauthorised interception, disclosure or use of computer data carried out for a dishonest or criminal purpose. This offence would apply to data generally, including metadata (i.e. information about a communication), data in transit and data momentarily at rest during transmission, and would therefore offer better protection to communications by members of the public than the existing section 27(b) of the TO (which is predicated on a telecommunications context);

(iv) The existing provisions regarding "misuse of a computer" in sections 59(1A), 60 and 64(2) of the CO should be transposed into the new legislation to provide for the offences of illegal interference of computer data and computer system. The new legislation should retain the breadth of the existing law, and the opportunity can be taken to refine the statutory definition of "misuse of a computer", e.g. by incorporating notions such as "impair the operation of any computer" into it;

(v) After the provisions on "misuse of a computer" are reorganised in the above manner, a provision corresponding to the existing section 62 of the CO (possessing anything with intent to destroy or damage property) should be introduced in the new legislation to include an offence of knowingly making available or possessing a device or data for committing a crime. The relevant elements of this offence would be made out as long as the primary use of the device or data is for committing an offence, regardless of whether or not it can be used for any legitimate purposes. An aggravated offence would occur where the perpetrator intends to use the device or data to commit an offence. To avoid over-criminalisation, a statutory defence of reasonable excuse would apply to both the basic and aggravated forms of the offence;

(vi) The nature of cybercrime justifies extra-territorial application of Hong Kong law. Hong Kong courts should have jurisdiction in a case where connections with Hong Kong exist. As an illustration, Hong Kong courts may assume jurisdiction if the perpetrator's act has caused or may cause serious damage to Hong Kong; and

(vii) Recognising that the severity of the harm caused by cybercrime has a wide range, each of the five proposed cyber-dependent offences has two maximum sentences, one applicable to summary convictions (two years' imprisonment) and the other to convictions on indictment (14 years' imprisonment).

When devising the above recommendations, the Sub-committee observes the guiding principles of balancing the rights of netizens and the interests of persons in the information technology industry against the need to protect the public's interest and right not to be disturbed or attacked when using or operating their computer system.

The Sub-committee welcomes views, comments and suggestions on any issues discussed in the consultation paper, including:

(i) whether there should be any specific defence or exemption for unauthorised access for cybersecurity purposes;

(ii) whether there should be exemptions from criminal liability for interception and use of data (including metadata) in favour of any professions and businesses;

(iii) whether the proposed offence of illegal interference of computer system should provide for lawful excuses for both cybersecurity professionals and non-security professionals; and

(iv) whether there should be a defence or exemption for the offence of knowingly making available or possessing computer data that can only be used to perform a cyberattack.

All views should be submitted on or before October 19 to the Secretary of the Cybercrime Sub-committee, Law Reform Commission, by mail (4/F, East Wing, Justice Place, 18 Lower Albert Road, Central), by fax (3918 4096) or by email (hklrc@hkreform.gov.hk).

The consultation paper and the executive summary can also be accessed on the Commission's website at www.hkreform.gov.hk. Hard copies of the consultation paper are also available on request from the Secretariat of the Law Reform Commission at the above address.