For discussion
on 2 June 2015

Legislative Council Panel on Security
Scope of Application of Section 161 of the Crimes Ordinance
(i.e. Access to Computer with Criminal or Dishonest Intent)

Introduction

This paper provides Members with an update of technology crimes and information about section 161 of the Crimes Ordinance (Cap. 200) in relation to access to computer with criminal or dishonest intent.

Technology Crime Trend

2. As members of the public become increasingly reliant on information and communications technology infrastructure, coupled with the growing popularity of the Internet, the number of local technology crime cases has surged nearly 24 times since 2002, from 272 cases in 2002 to 6 778 cases in 2014. In the past five years from 2010 to 2014, related economic losses increased from $60 million to $1.2007 billion, an increase of nearly 19 times. As regards the technology crime cases reported to the Police in 2014, more than 60% of them involved the following three types of technology crime, i.e. cases relating to online games (e.g. theft of virtual weapons), online business fraud, and unauthorised access to a computer.

3. To enable the Police to better protect the security of the information systems of critical infrastructure, and to enhance the Police's capability in preventing and combating technology crimes, the Hong Kong Police Force (HKPF) upgraded the Technology Crime Division to the "Cyber Security and Technology Crime Bureau" (CSTCB) in January 2015. The HKPF's primary task is to expeditiously set the work of the newly established CSTCB on track, such as stepping up the detection of syndicated and highly sophisticated technology crimes, preventing and detecting cyber attacks against critical infrastructure, enhancing incident response capability to major cyber security incidents or massive cyber attacks, strengthening thematic researches on cyber crime trend and mode of operation, vulnerabilities of computer systems and development of malware, as well as strengthening partnership with local stakeholders and overseas law enforcement agencies.

Section 161 of the Crimes Ordinance (Cap. 200) : Access to Computer with Criminal or Dishonest Intent

4. Given that computers are extremely popular and have even become indispensable in people's daily life, section 161 of the Crimes Ordinance (Cap. 200), which targets against access to computer with criminal or dishonest intent is most effective in combatting illegal acts such as online frauds, illegal access to computers and the use of computers to commit other offences. The Police have invoked section 161 for handling cases such as online frauds, illegal access to a computer system, clandestine photo-taking using smart phones in non-public places such as toilets or changing-rooms, online publication of obscene or threatening information, as well as inciting others on the Internet to engage in illegal activities. Perpetrators of such cases may also be charged with other related crimes at the same time.

5. Section 161 concerning access to computer with criminal or dishonest intent reads as follows:

(1) Any person who obtains 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
  (d) with a dishonest intent to cause loss to another,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for five years.

As seen from the provision, any person who obtains access to a computer with one of the above intents or purposes commits an offence.

6. As understood from the court judgment of individual cases, the threshold for charging under section 161 is fairly high. In an appeal case (HCMA723/1998) heard at the High Court, the judge has made it clear that the offence under section 161 requires proof of a specific criminal or dishonest intent, which is more serious. It follows that not every kind of access to a computer constitutes an offence. The judgment of Mr. Justice Patrick CHAN is as follows:

> *"A s.161 offence requires proof of a specific criminal or dishonest intent or purpose and is more serious (as can be reflected from the maximum penalty specified in the provision). It follows that not every kind of access into a computer constitutes an offence under*

> *s.161. This section stipulates four situations in which the access becomes a crime."*

The above judgment was also quoted by Mr. Justice Barnabas FUNG in another appeal case (HCMA77/2013) heard at the High Court in 2013. As shown from the above, it is by no means easy to press charges under section 161. Between 2008 and 2014, amongst 293 prosecution cases pertaining to section 161, there were 252 cases in which the defendants were convicted, representing a conviction rate of over 85%.

7. When a case (HCMA 723/98) involving this section was heard at the High Court, the judge once clearly consented that section 161 aimed to combat offences related to the access to computer with criminal or dishonest intent. Mr. Justice Patrick CHAN stated the following in the judgment:

> *"S.161 offence requires proof of a specific criminal or dishonest intent or purpose and is more serious. It follows that not every kind of access into a computer constitutes an offence under s.161..... What s.161 is intended to do is to punish access into a computer with a particular intent or for a particular purpose. The intent with which or the purpose for which the access is made must be either criminal or dishonest. It would also follow that it is the intent or purpose of the offender at the time of the access which must be looked at, not his intent or purpose at some later stage..... It is clear from the section that it catches acts preparatory to the commission of a crime or fraud. But I do not agree that it is restricted to such acts. A person who makes an unauthorised access into another person's computer need not have any intention to commit a crime or fraud..... All these acts may result in a gain to the perpetrator or cause huge losses, great embarrassment and serious harm to others. But they are not necessarily criminal or fraudulent. The perpetrator's access to the computer cannot therefore be regarded as an act preparatory to the commission of a crime or fraud. However, if such access is obtained dishonestly, the perpetrator ought to be punished. That in my view is the objective of s.161(1)(c) and (d)."*

8. It is clearly stated in the judgment that as long as the perpetrator obtained access to a computer, and he had one of the four criminal intents or purposes specified in the section at the crucial moment, he committed an offence under section 161. As explicitly stated in the judgment, section 161 covers acts preparatory to the commission of a crime or a fraud, but the judge did not agree that the provision was restricted to such acts. The judge stated

that even if acts of the perpetrator were not preparatory to the commission of these crimes or frauds, or he did not have any intention to commit a crime or fraud, so long as he obtained access into the computer dishonestly, he ought to be punished. This is the objective of sections 161(1)(c) and (d).

Conclusion

9. Enhancing cyber security as well as combating technology crimes is one of the Commissioner's Operational Priorities. The Police shall continue to discharge their enforcement duties in a fair, just and impartial manner in accordance with the law.

Security Bureau
Hong Kong Police Force
May 2015