立法會
Legislative Council

LC Paper No. CB(2)1560/14-15(04)

Ref : CB2/PL/SE

Panel on Security

Information note prepared by the Legislative Council Secretariat for the meeting on 2 June 2015

Scope of application of section 161 of the Crimes Ordinance concerning access to computer with criminal or dishonest intent

The main statutory provisions concerning access to computer with criminal or dishonest intent are set out in section 161 of the Crimes Ordinance (Cap. 200), which provides, among others, that -

"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 5 years."

2. The subject of access to computer with criminal or dishonest intent per se has not been discussed by the Panel on Security ("the Panel"). However, Members have raised questions relating to the subject at the Council meetings of 24 April 2013 and 5 November 2014. The questions raised by Members and the Administration's replies are in **Appendices I and II** respectively. In addition, a motion on "Comprehensively reviewing the provision on 'access to computer with criminal or dishonest intent' under the Crimes Ordinance" was moved at the Council meeting of 4 February 2015.

3. The Panel will discuss the scope of application of section 161 of the Crimes Ordinance concerning access to computer with criminal or dishonest intent at the meeting on 2 June 2015.

Council Business Division 2
Legislative Council Secretariat
27 May 2015

Press Releases

LCQ14: Access to computer with criminal or dishonest intent
****

Following is a written reply by the Secretary for Security, Mr Lai Tung-kwok, to a question by the Hon Charles Peter Mok in the Legislative Council today (April 24):

Question:

In 1993, the authorities amended, through the Computer Crimes Bill 1992, the Crimes Ordinance (Cap. 200) by adding section 161, which provides for the offence of "access to computer with criminal or dishonest intent" (section 161). During the resumed debate on the Second Reading of the Bill, the then Secretary for Security pointed out that the making of "the new offence of access to a computer with criminal or dishonest intent" aimed at penalising "access to a computer for acts preparatory but falling short of the commission of a fraud". In this connection, will the Government inform this Council of the following since section 161 came into operation in 1993:

(a) the annual numbers of cases in which prosecutions were instituted (prosecution cases) under section 161 (and among them, the number of cases in which the charge was laid as an alternative charge); and among such cases, of the respective numbers of convicted cases and acquitted cases (set out in Table 1);

(b) the annual numbers of prosecution cases under section 161 which involved "access to a computer for acts preparatory of the commission of a fraud"; and among such cases, the respective numbers of convicted cases and acquitted cases (set out in Table 2); and

(c) the annual numbers of prosecution cases under section 161 other than those mentioned in (b), and among such cases, the respective numbers of convicted cases and acquitted cases (set out in Table 3 and type of crime involved)?

Reply:

President,

It is stipulated under section 161 of the Crimes Ordinance (Cap. 200) (i.e. access to computer with criminal or dishonest intent) that 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.

The above section aims at combating acts of "access to computer with dishonest or criminal intent", such as technology crimes like online fraud and illegal access to a computer system, as well as other crimes committed through the use of computer. Any persons who commit such an offence are subject to a maximum penalty of five-year-imprisonment upon conviction.

(a) to (c) The Administration has maintained the figures of prosecution cases, convicted cases and acquitted cases pertaining to "access to computer with criminal or dishonest intent",

section 161 of Crimes Ordinance (Cap. 200), from 1997 onwards. Details are at the Annex. The Administration, however, did not maintain information on whether the charges in prosecution cases were laid as alternative charges, or whether the cases involved "access to a computer for acts preparatory of the commission of a fraud".

In 2012, the Hong Kong Police Force set up a Cyber Security Centre in a bid to further enhance Hong Kong's resilience against various forms of cyber threats, by means of collaboration with relevant government departments and industry stakeholders (including Internet service and critical infrastructure operators). The Police will also continue to adopt multi-pronged strategies to combat technology crimes, such as maintaining professional competence and advanced capability in technology crime investigation, digital forensics and training; working closely with overseas law enforcement agencies, other government departments and key industry stakeholders; as well as raising public awareness of technology crime prevention through public education and community engagement.

Ends/Wednesday, April 24, 2013
Issued at HKT 15:55

NNNN

Table 1 to LCQ14

Year	Number of prosecution cases (among them, the number of cases in which the charge was laid as an alternative charge)	Number of convicted cases	Number of acquitted cases
1993	( )		

Table 2 to LCQ14

Year	Number of prosecution cases	Number of convicted cases	Number of acquitted cases
1993			

Table 3 to LCQ14

Year	Number of prosecution cases	Number of cases by type of crime		Number of convicted cases	Number of acquitted cases
		Type of crime	Number of cases		
1993					

Annex to LCQ14

Figures of prosecution cases, convicted cases and acquitted cases pertaining to "access to computer with criminal or dishonest intent", section 161 of the Crimes Ordinance (Cap. 200) (1997-2012)

	Number of prosecution cases	Number of convicted cases	Number of acquitted cases
1997	1	1	0
1998	18	13	5
1999	9	5	4
2000	10	8	2
2001	13	12	1
2002	9	8	1
2003	22	22	0
2004	30	23	7
2005	22	18	4
2006	25	19	6
2007	32	26	6
2008	26	19	7
2009	28	21	7
2010	25	18	7
2011	34	32	2
2012	39	32	7

Note: The respective year of the above figures represents the year in which the trial was concluded. The year in which a case was prosecuted may be different from the year in which the trial was concluded.

Press Releases

LCQ4: Access to computer with criminal or dishonest intent
****

Following is a question by the Hon Charles Peter Mok and a reply by the Secretary for Security, Mr Lai Tung-kwok, in the Legislative Council today (November 5):

Question:

When the authorities amended the Crimes Ordinance in 1993, section 161 was added to provide for the offence of "access to computer with criminal or dishonest intent" (section 161). The then Secretary for Security explained that the new section 161 was aimed at "penalising access to a computer for acts preparatory but falling short of the commission of a fraud. Examples would include someone obtaining access to computerised bank records to obtain details of credit balances for later fraudulent use". Last month, the Police noted that some persons had posted messages on the Internet to incite members of the public to take part in the unlawful assemblies in Mong Kok and Admiralty. After investigation, the Police arrested a man for allegedly committing the offence under section 161 and that of "unlawful assembly". Regarding the scope of application of section 161, will the Government inform this Council:

(1) of the details of the cases in which prosecutions were instituted by the authorities under section 161 in the past three years, including case numbers, other charges in the same case (if applicable), sentencing outcome, appeal outcome (if applicable), and case type (e.g. criminal intimidation, blackmail, indecent assault, theft, deception, criminal damage, public safety, soliciting for an immoral purpose, sale or use of non-compliant electronic products and network attacks), and set out such information in a table; among such cases, the number of those involving fraud or acts preparatory of the commission of a fraud and their case numbers; and

(2) as most of the laws for prevention of crimes in the physical world apply equally to the cyber world, whether the authorities have planned to review and amend section 161 to bring its scope of application more in line with its legislative intent, that is focusing on tackling crimes such as computer frauds and network attacks, instead of imposing criminal liabilities on people posting on the Internet messages which are not in violation of other legislative provisions?

Reply:

President,

According to section 161 of the Crimes Ordinance (Cap 200) (i.e. access to computer with criminal or dishonest intent), any person who obtains access to a computer with any of the following intention or purpose:

(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.

The above section aims at combating acts of "access to computer with criminal or dishonest intent", such as technology crimes like online fraud and illegal access to a computer system,

urging or inciting others to engage in illegal activities, as well as other crimes committed through the use of computer. Any persons who commit such an offence are subject to a maximum penalty of five-year-imprisonment on conviction upon indictment.

Between 2011 and 2013, there were a total of 128 prosecution cases pertaining to section 161 of the Crimes Ordinance (Cap 200). During the same period, there were 114 convicted cases. Detailed figures of prosecution cases, convicted cases and non-convicted cases between 2011 and 2013 are at Annex. The Administration, however, did not have any information on whether the charges in prosecution cases were laid as alternative charges, whether the cases involved "access to a computer for acts preparatory of the commission of a fraud", or other categories of crimes involved in such cases.

In early October this year, a hacker group threatened to launch cyber attacks on the network systems of Hong Kong government departments, and even incited others to join in the attacks by using hackers' websites or software. Meanwhile, the Police found that some people, via social networking platforms on the Internet, were inciting members of the public to take part in the attacks, as well as making available certain tools for such attacks. Despite that the Police had required the Internet Service Providers concerned to delete those messages inciting others to commit crime, some members of public, taking no heed of their criminal liabilities, responded to the appeals on the social networking platforms by participating in the illegal cyber attacks. The Police have, since early October, received a number of reports of "Denial of Service Attacks" on the network systems of Hong Kong government departments and private organisations. Some of their websites experienced an unusually high hit rate, leading to network congestion and intermittent service disruption. Upon in-depth investigation, the Technology Crime Division under the Commercial Crime Bureau of the Police launched a number of actions, in which 11 persons were arrested for suspected "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance, with two arrested persons being charged by the Police, while the remaining nine were released on police bail pending further investigation. These persons were arrested for having been incited to join the cyber attacks by using the hackers' websites or software.

The case mentioned in the Hon Mok's question was about a man urging members of the public to participate in the unlawful assemblies at Mong Kok and Admiralty. On an Internet discussion forum, the person in question incited others to join the unlawful assembly at Mong Kok and to storm the Police, suggesting protesters to paralyse the railway system by gathering on railway platforms in an attempt to create chaos, in case Mong Kok could not be successfully taken back. Upon investigation, the Police arrested the man on October 18 for having involved in the acts of "access to computer with criminal or dishonest intent" and "unlawful assembly".

As another issue, during "Occupy Central" or "Occupation Movement", a person uploaded the personal data of a police officer, and even those of his family members and children, onto the Internet. Apart from incessant personal attacks via social media, the person posted messages on an online discussion forum, claiming that somebody had been directed to assault the police officer's family members. The police officer and his family members were consequently subject to unnecessary nuisances and personal safety concerns. Upon in-depth investigation, the Police arrested the man on October 22 for suspected "criminal intimidation".

I have to stress that it is an act of extreme irresponsibility by inciting others to participate in illegal

activities and making threatening remarks on the Internet. The Police and I severely condemn such acts. As legal proceedings for the cases that I just mentioned have commenced or are going to commence, I am not in a position to make further comments. However, as seen from the above cases, any persons committing unlawful acts in the real world or cyber world, like launching cyber attacks on network systems, inciting others through online platforms to conduct illegal activities, and making remarks that put others' personal safety at risk, shall be criminally liable and be brought to justice.

The Police shall, in consideration of the nature of individual crimes, take enforcement actions in accordance with relevant laws. The Police have internal guidelines in which police officers are instructed to seek advice from the Department of Justice (DoJ) before pressing charges against any persons arrested for having involved in public order events. Police officers will also seek DoJ's advice as to which legal provisions shall be invoked when pressing charges. In handling other types of cases, including internet-related cases, the Police shall determine the charge(s) to be laid with regard to the evidence of individual cases, and, where necessary, DoJ's advice shall also be sought before prosecution. Whether a person is to be convicted is a matter of which the court shall pass a fair and impartial judgment upon considering all evidence available.

The Police always remind the public that the Internet is not an unreal world that is beyond the law. As far as the existing legislation in Hong Kong is concerned, most of the crime-prevention laws in the real world are applicable to the Internet world. As reminded by the Police, the public should not risk breaking the law. They are also advised to use the Internet properly and lawfully, while refraining from sending any irresponsible messages and inciting others to engage in illegal activities. The Police shall definitely collect evidence on any illegal online activities for follow-up investigations and take arrest actions where necessary.

The Administration considers that the law in place is effective in meeting the demand for combating technology crime and safeguarding cyber security and there is no plan for legislative amendments at this stage.

Ends/Wednesday, November 5, 2014
Issued at HKT 17:09

NNNN

Annex

Figures of prosecution cases, convicted cases and non-convicted cases pertaining to "access to computer with criminal or dishonest intent", section 161 of the Crimes Ordinance (Cap 200) (2011-2013)

	Number of prosecution cases	Number of convicted cases	Number of non-convicted cases
2011	34	32	2
2012	39	32	7
2013	55	50	5

Note: The respective year of the above figures represents the year in which the trial was concluded. The year in which a case was prosecuted may be different from the year in which the trial was concluded.