立法會
Legislative Council

LC Paper No. CB(3) 193/02-03

Ref : CB(3)/M/OR

Tel : 2869 9205

Date : 29 November 2002

From : Clerk to the Legislative Council

To : All Members of the Legislative Council

Council meeting of 18 December 2002

Proposed resolution to be moved by the Secretary for Security

I forward for Members' consideration a proposed resolution which the Secretary for Security will move at the Council meeting of 18 December 2002 relating to the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002. The President has directed that "it be printed in the terms in which it was handed in" on the Agenda of the Council.

2. The speech, in both English and Chinese versions, which the Secretary for Security will deliver when moving the proposed resolution, is also attached.

(Ray CHAN)
for Clerk to the Legislative Council

Encl.

Motion on the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 to be moved by the Secretary for Security at the Legislative Council meeting on Wednesday, 18 December 2002

Wording of the motion

"That the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002, to be made by the Chief Executive in Council, be approved."

DRAFT ORDER

CRIMINAL JURISDICTION ORDINANCE (AMENDMENT OF SECTION 2(2)) ORDER 2002

(Made by the Chief Executive in Council under section 2(4) and (5) of the Criminal Jurisdiction Ordinance (Cap. 461), a draft of the Order having been laid before and approved by resolution of the Legislative Council)

1. Commencement

This Order shall come into operation on a day to be appointed by the Secretary for Security by notice published in the Gazette.

2. Offences to which this Ordinance applies

Section 2(2) of the Criminal Jurisdiction Ordinance (Cap. 461) is amended –

(a) by adding before paragraph (a) –

"(aa) an offence under section 27A (unauthorized access to computer by telecommunications) of the Telecommunications Ordinance (Cap. 106)";

(b) in paragraph (b), by adding –

"section 60 (destroying or damaging property) but for the purpose of this section, the offence is limited to misuse of a computer as defined in section 59 of the Crimes Ordinance (Cap. 200)

section 161 (access to computer with criminal or dishonest intent)".

Clerk to the Executive Council

COUNCIL CHAMBER

2002

Explanatory Note

The purpose of this Order is to bring the offences of unauthorized access to computer by telecommunications, destroying or damaging property (but the offence is limited to misuse of a computer) and access to computer with criminal or dishonest intent within the scope of the Criminal Jurisdiction Ordinance (Cap. 461).

Draft speech of the Secretary for Security
for moving the motion on the draft
Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002

Madam President,

I move that the draft of the Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002, to be made by the Chief Executive in Council, be approved.

With the advancement of modern technology and the rapid growth in Internet and computer use, cross-boundary computer related offences are becoming more and more common. This development calls for a review of traditional jurisdictional rules for tackling such crimes.

In the physical world, the perpetrator of a crime is usually present at or near the scene of crime. Therefore, traditionally the concept of jurisdiction is closely associated with geographical boundaries. The jurisdiction of the court is limited to acts done within the geographical boundaries of a country or territory unless otherwise specified. At common law, an offence is regarded as being committed where the last act or event necessary for its completion took place, and jurisdiction is exercised where the offence is committed.

The information technology revolution which has removed geographical barriers to communication has unfortunately bred cross-border crime. Such crime cannot be sufficiently dealt with by traditional jurisdictional rules, as they may involve transactions and events which have

taken place in more than one jurisdiction. To overcome this problem, Hong Kong enacted the Criminal Jurisdiction Ordinance (Cap. 461) in 1994, taking reference from the Criminal Justice Act 1993 of the United Kingdom. The Ordinance aims at addressing the jurisdictional problems associated with international fraud, providing exception to the norm and enabling Hong Kong courts to exercise jurisdiction over offences of fraud and dishonesty –

(a) Hong Kong courts will have jurisdiction if any of the conduct (including an omission) or part of the results that are required to be proved for conviction of the offences takes place in Hong Kong;

(b) An attempt to commit the offences in Hong Kong is triable in Hong Kong whether or not the attempt was made in Hong Kong or elsewhere and irrespective of whether it had an effect in Hong Kong;

(c) An attempt or incitement in Hong Kong to commit the offences elsewhere is triable in Hong Kong;

(d) A conspiracy to commit in Hong Kong the offences is triable in Hong Kong wherever the conspiracy is formed and whether or not anything is done in Hong Kong to further or advance the conspiracy; or

(e) A conspiracy in Hong Kong to do elsewhere that which if done in Hong Kong would constitute the offences is triable in Hong Kong provided that the intended conduct was an offence in the jurisdiction where the object was intended to be carried out.

In simple words, if a person in Hong Kong perpetrates a crime outside Hong Kong, or if a person outside Hong Kong perpetrates a crime in Hong Kong, that person is triable in Hong Kong courts. The Ordinance sets out a list of offences to which the Ordinance applies. The list may be amended by an order of the Chief Executive in Council, subject to the draft order having been approved by the Legislative Council.

As I have mentioned earlier, many computer related offences are transborder in nature. However, they are currently not covered by the Criminal Jurisdiction Ordinance. It follows that if a person in an overseas country hacks into a computer in Hong Kong, or if he alters or erases computer programmes or data in a computer in Hong Kong, he has not committed any offence under the existing laws in Hong Kong, as his last act for completing the crime is done outside Hong Kong. Our courts cannot exercise jurisdiction over him even if he is present within the Hong Kong territory. These present loopholes should be plugged as early as possible to avoid exploitation by computer criminals.

In fact, many other jurisdictions have recognized the jurisdictional problem associated with computer crime. For example, the Computer Misuse Act 1990 of the United Kingdom provides that the courts have jurisdiction over offences covered by the Act if either the victim or perpetrator of the crime is in the United Kingdom. The offences include unauthorized access to computer programmes or data, unauthorized access with intent to commit or facilitate the commission of a further offence and unauthorized modification of any computer content. Similarly, the Computer Misuse Act of Singapore allows prosecution for computer related offences committed within or outside Singapore, when the offender was in Singapore at the material time, or the computer, programme or data was in Singapore at the material time. The offences include unauthorized

access to computer material, access with intent to commit or facilitate the commission of a further offence, unauthorized modification of computer material, unauthorized use or interception of computer service, unauthorized obstruction of use of computer and unauthorized disclosure of access code.

Indeed, in an effort to improve the regime of computer crime legislation, enforcement and prevention, we established the Inter-departmental Working Group on Computer Related Crime (Working Group) in 2000 to review, among other things, the adequacy of existing legislation to deal with the challenges posed by computer crimes, including the jurisdictional issues involved. The Working Group recommended that as a first step to address the inadequacy of present jurisdictional rules in tackling transborder computer crimes, the coverage of the Criminal Jurisdiction Ordinance should be expanded to some "pure" or "direct" computer crimes, namely –

(a) unauthorized access to computer by telecommunications under section 27A of the Telecommunications Ordinance (Cap. 106); and

(b) access to computer with criminal or dishonest intent under section 161 of the Crimes Ordinance (Cap. 200).

By putting these two offences within the scope of the Criminal Jurisdiction Ordinance, Hong Kong courts can exercise jurisdiction over the offences if either the person who obtained access to the computer or the computer to which access was obtained is in Hong Kong.

In following up the Working Group's recommendation, we have further considered it necessary to include in the Criminal Jurisdiction Ordinance the

offence of criminal damage to property in relation to the misuse of a computer under sections 59 and 60 of the Crimes Ordinance. The justification is that some computer related offences may not involve dishonesty, and would therefore fall outside the scope of the two offences as mentioned earlier. For example, a person in an overseas jurisdiction could "spam" a computer in Hong Kong causing it to cease functioning. Such an activity may just be done for "fun" and does not necessarily carry a dishonest intent. By including this offence within the scope of the Criminal Jurisdiction Ordinance, our legislative framework can be further improved to deter such undesirable activities and to enable the laying of charges against them.

As Members may recall, we consulted the public on the Working Group's recommendations in late 2000, including the suggested extension of jurisdictional rules to computer related crime. We also consulted the Panel on Security on these recommendations at a special meeting in February 2001. We further briefed Members on the way forward for implementing the recommendations in July 2001. The recommendation on the proposed amendments to the Criminal Jurisdiction Ordinance to cover computer related offences received across-the-board support from professional associations, Internet service providers and the telecommunications practitioners.

Madam President, I wish to emphasize that the purpose of the proposed amendments is to improve the existing legislative regime for tackling cross-border computer related crime. This will be important in providing a more secure environment conducive to the use of computers for business and personal pursuits in Hong Kong. Meanwhile, we remain vigilant in implementing the Working Group's other recommendations and in monitoring international developments to ensure that our response to computer crime keeps up with the times. We will also continue to work closely with other countries and

territories in bringing computer criminals to justice.

Madam President, with these remarks, I earnestly hope to have the support of Members to approve the proposed amendments to the Criminal Jurisdiction Ordinance.