By Fax and By Post

SBCR 11/14/3231/88

11 December 2002

Tel No. : 2810 2448
Fax No. : 2521 2848

Mr Lee Yu-sung
Senior Assistant Legal Adviser
Legal Services Division
Legislative Council Secretariat
Legislative Council Building
8 Jackson Road
Central
Hong Kong
(Fax : 2877 5029)

Dear Mr Lee,

**Draft Order under Section 2(4) and (5)
of the Criminal Jurisdiction Ordinance (Cap. 461)**

I refer to your letter of 7 December 2002 regarding the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002. Our response to the issues mentioned therein is set out below please.

Problems involved in dealing with cross-border computer related crime and how such problems have been dealt with

Cross-border computer crime involves crime committed or planned outside the geographical boundaries of Hong Kong. The offender who obtains access to the computer or the computer to which access is obtained may be outside Hong Kong. To effectively tackle the technological and jurisdictional challenges posed by such crime, the following actions at both the policy and law enforcement level are necessary.

Addressing the jurisdictional issues

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.

As cross-border computer crime may involve transactions and events which have taken place in more than one jurisdiction, it is obvious that such crime cannot be sufficiently dealt with by traditional jurisdictional rules. Amendments to the Criminal Jurisdiction Ordinance (Cap. 461), the enactment of which is aimed at addressing the jurisdictional problems associated with international crime, are necessary, so as to enable Hong Kong courts to exercise jurisdiction over computer crime committed or planned outside the geographical boundaries of Hong Kong but are connected to or intended to cause damage in Hong Kong. Detailed justification of the proposed amendments is set out in the paragraphs under "Basis for adding the three computer offences in the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002" on pages 4 and 5.

Resources and capabilities of law enforcement agencies

Effective enforcement against cross-border computer crime depends on the availability of sufficient resources and capabilities of our law enforcement agencies, namely, the Hong Kong Police Force, the Customs and Excise Department, the Independent Commission Against Corruption and the Immigration Department. They have all taken specific initiatives to respond to the challenges of computer crime over the past few years -

(a) The Hong Kong Police Force set up a Computer Crime Section in 1993, which was expanded in 2001 to a Technology Crime Division (TCD). TCD is capable of conducting investigation into complex and serious technology crime, operating the computer forensics laboratory and managing the computer crime intelligence system. In addition, to broaden the investigative capability, the Technology Crime Initial Response Cadre (TCIRC) comprising officers from various police formations has also been formed since December 1999. Members of TCIRC have been trained to provide immediate support to frontline officers in the handling of computer and digital evidence;

(b) The Customs and Excise Department has established an Anti-Internet Piracy Team since December 1999 to investigate copyright infringements on the Internet. To strengthen the technical support to investigations involving computer systems and digital evidence, a Computer Analysis and Response Team comprising members from various formations has also been formed since October 2000 to respond to requests for assistance by frontline officers either at the scene of crime or after seizure. A Computer Forensic Laboratory has been established since November 2000 to provide forensic computer support to retrieve and preserve the criminal evidence contained in computer-based systems seized by the Department;

(c) The Independent Commission Against Corruption has established a Computer Forensics and Research and Development Section since April 1999 to handle computer forensics and to assist computer related crime investigations; and

(d) The Immigration Department has set up a Computer Crime Unit since November 2001 for preliminary investigation on computer related crime in immigration cases.

Our law enforcement agencies have been vigilant in ensuring that their expertise and equipment for computer crime investigation and computer forensic examination are sufficient for tackling such crime with rapidly advancing technologies. For example, they have recently visited the forensics laboratories of the FBI of the United States, the National High-Tech Crime Unit of the United Kingdom and the National Police Agency of Japan, taking reference from the expertise and practices of advanced countries.

To deepen inter-agency cooperation, while continuing day-to-day coordination and sharing of intelligence and experience for the purposes of investigations, our law enforcement agencies have also established a joint forum where they will meet regularly to exchange other information relating to computer crime.

<u>Cooperation with law enforcement agencies in other jurisdictions</u>

Cooperation with law enforcement agencies in other jurisdictions is critically important in dealing with cross-border computer crime. While the regime of mutual legal assistance remains the formal basis for obtaining information and evidence relating to such crime, our law enforcement agencies

have also established effective channels of liaison with their overseas counterparts for speedy exchange of intelligence, experience and know-how.

Meanwhile, we are liaising with the United States the participation of Hong Kong in the 24-hour contact network for international high-tech cases, which will enable Hong Kong to have access to an international network of knowledgeable personnel on a 24-hour basis to obtain assistance for investigations into transborder computer crime.

Assistance from Internet Service Providers (ISPs)

Cross-border computer crime is commonly conducted via the Internet. Assistance from the ISPs for investigation and prevention of such crime is therefore essential. In this respect, our law enforcement agencies have set up a forum of exchange with the ISPs and other parties in the communication chain to discuss issues of mutual concern. A 24-hour central contact system has also been established under which the ISPs and our law enforcement agencies have designated contact officers for dealing with crime investigation requests.

Basis for adding the three computer offences in the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002

As explained above, traditional jurisdictional rules cannot sufficiently deal with cross-border computer crime. To address this problem, we have accepted the recommendation of the Inter-departmental Working Group on Computer Related Crime (the Working Group), which was established in 2000 to recommend measures to improve the existing regime on computer crime legislation, enforcement and prevention, that the coverage of the Criminal Jurisdiction Ordinance should be expanded to the following computer offences where the computer is the main subject of, and not merely incidental to, the offences -

(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 above. 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.

In fact, instead of listing each offence covered by the Criminal Jurisdiction Ordinance, the Working Group had considered the possibility of generally covering all offences triable on indictment under the Ordinance. However, as this approach would change the basic principle regarding jurisdictional rules and the Ordinance is meant to provide exception to the norm, the Working Group's view was that changing the ambit to cover in effect almost all criminal offences should not be attempted lightly. The Working Group had also considered the option of including all offences which may be committed via the computer or the Internet within the scope of the Ordinance. Upon further deliberation, this approach could result in different jurisdictional rules applying to offences essentially similar in substance and different only with regard to whether the computer or the Internet is used. The Working Group had therefore concluded that, as a first step, to address the inadequacy of present jurisdictional rules in tackling transborder computer crime, the existing approach as provided for in the Criminal Jurisdiction Ordinance should be adopted as far as possible. We agree with the Working Group's recommendation.

We have therefore not sought to deal with all transborder offences that may be committed via the computer or the Internet, such as transmitting copyright infringing articles, illegal gambling operations and pornographic materials through the Internet. They will be dealt with by respective policy bureaux in accordance with their overall policy considerations for the issues in question.

I hope the above information is useful in addressing the issues raised in your letter. If you need additional information, please contact me or Ms Manda Chan at telephone number 2810 2973.

Yours sincerely,

(Johann Wong)
for Secretary for Security