

立法會
Legislative Council

LC Paper No. CB(2)2921/03-04

Ref : CB2/SS/3/02

Paper for the House Committee meeting on 25 June 2004

**Report of the Subcommittee on
the draft Criminal Jurisdiction Ordinance
(Amendment of Section 2(2)) Order 2002**

PURPOSE

This paper reports on the deliberation of the Subcommittee on the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 (the draft Order).

BACKGROUND

Recommendations of Inter-departmental Working Group on Computer Related Crime and Inter-departmental Task Force

2. In December 2000, the Inter-departmental Working Group on Computer Related Crime (the Working Group) consulted the public on a number of recommendations to improve the existing regime on computer crime legislation, enforcement and prevention. Having taken into account comments received during the consultation exercise, the Chief Executive in Council agreed at its meeting on 10 July 2001 to accept most of the recommendations put forward by the Working Group.

3. One of the recommendations accepted by the Chief Executive in Council is to add the following two offences to the list of offences in section 2(2) of the Criminal Jurisdiction Ordinance (CJO) (Cap. 461) -

- (a) unauthorized access to computers; and
- (b) access to computers with criminal or dishonest intent.

The jurisdiction of the courts of Hong Kong is limited to acts done within the geographical boundaries of Hong Kong unless otherwise specified. By putting these two offences within the scope of CJO, 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.

4. In addition, the Inter-departmental Task Force led by Security Bureau to follow-up the Working Group's recommendations has suggested that the jurisdictional rules should be extended to the misuse of a computer, as defined in section 59 of the Crimes Ordinance (Cap. 200) and covered under the offence of criminal damage in section 60 of the same Ordinance. This is considered necessary because some computer-related offences may not involve dishonesty, and would therefore fall outside the scope of the two offences outlined in paragraph 3 above.

The draft Order

5. The draft Order seeks to add the following three computer offences to the CJO as Group A offences -

- (a) "unauthorized access to computer by telecommunications" under section 27A of the Telecommunications Ordinance (Cap. 106);
- (b) "destroying or damaging property" under section 60 of the Crimes Ordinance (Cap.200) but limiting to criminal damage relating to the misuse of a computer as defined in section 59 of the Crimes Ordinance; and
- (c) "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance (Cap.200).

6. The offences to which CJO applies are listed in section 2(2) and 2(3) of CJO. Section 2(4) of CJO provides that the Chief Executive in Council may, by order in the Gazette, amend sections 2(2) or 2(3) by adding or removing any offence. Section 2(5) of CJO also provides that no order shall be made under section 2(4) unless a draft of it has been laid before and approved by resolution of the Legislative Council (LegCo), and section 34 of the Interpretation and General Clauses Ordinance (Cap. 1) shall not apply in relation to any such order.

THE SUBCOMMITTEE

7. At the House Committee meeting on 6 December 2002, members agreed to form a subcommittee to scrutinize the draft Order. Under the chairmanship of Hon James TO, the Subcommittee has held five meetings with the Administration. A membership list of the Subcommittee is in the **Appendix**.

8. The Administration had subsequently withdrawn the notice of moving a motion relating to the draft Order at the Council meeting on 18 December 2002, pending deliberation of the Subcommittee.

DELIBERATION OF THE SUBCOMMITTEE

Reference to offences set out in the National Security (Legislative Provisions) Bill as related to the three computer offences

9. At the first meeting of the Subcommittee on 8 January 2003, some members requested the Administration to identify the parts of the Consultation Document on "Proposals to implement Article 23 of the Basic Law" that were related to the draft Order. The National Security (Legislative Provisions) Bill (the Bill) to implement Article 23 of the Basic Law was subsequently introduced into LegCo on 26 February 2003.

10. According to the Administration, clause 11 of the Bill seeks to amend section 18 of the Official Secrets Ordinance (Cap. 521), adding a new subsection (5A). The new subsection (5A) provides that a person has "illegal access" to information if such information comes into his possession by virtue of any of the six offences specified therein. Section 27A of the Telecommunications Ordinance (unauthorized access to computer by telecommunications) and section 161 of the Crimes Ordinance (access to computer with criminal or dishonest intent) are among the six offences specified.

11. The legal adviser to the Subcommittee has pointed out that apart from clause 11 of the Bill, clause 4 which proposes amendments to the Crimes Ordinance (Cap. 200) may also be related to computer crimes -

- (a) in the proposed new offence of treason (proposed new section 2), one of the elements is "assist any public enemy at war with the People's Republic of China by doing any act with intent to prejudice the position of the People's Republic of China in the war". The "act" may include the use of a computer;
- (b) in the proposed offence of subversion (proposed new section 2A), one of the elements of the offence is using force or serious criminal means that seriously endangers the stability of the People's Republic of China. In the proposed section 2A(4)(b), "serious criminal means" include seriously interferes with or disrupts an electronic system; and
- (c) in the proposed offence of secession (proposed new section 2B), one of the elements of the offence is using force or serious criminal means that seriously endangers the territorial integrity of the People's Republic of China, and "serious criminal means" has the same meaning as in the proposed section 2A(4)(b).

The proposed offence of treason applies to any Chinese national who is a Hong Kong permanent resident in relation to an act done outside Hong Kong. The

proposed offences of subversion and succession apply to any Hong Kong permanent resident in relation to an act done outside Hong Kong.

12. As the draft Order and the Bill were under scrutiny by two different committees concurrently, some members expressed concern about the interface of the work of the two committees. They considered that consideration of the draft Order should be deferred until completion of the scrutiny of the Bill, as approval of the draft Order ahead of passage of the Bill would pre-empt deliberation on the extra-territorial application of the relevant offences under the Bill. The Administration deferred to the Subcommittee whether it would require more time to consider the draft Order, notwithstanding concurrent scrutiny of the Bill by the Bills Committee.

13. On 7 July 2003, the Government decided to defer the resumption of the second reading debate of the Bill. On 2 October 2003, the Secretary for Security wrote to advise the Chairman of the House Committee that the Administration would not give notice to resume the Second Reading debate of the Bill, and that the Bill would lapse at the end of the current term of the Council, pursuant to Rule 11(4) of the Legislative Council Rules of Procedure and section 9(4) of the Legislative Council Ordinance (Cap. 542).

Justifications for adding the three computer offences in CJO

14. In response to the request of the Subcommittee, the Administration has provided detailed justifications for adding the three computer offences in CJO.

Traditional jurisdictional rules

15. 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. In relation to inchoate offences such as conspiracy and attempt, the common law rules would enable a perpetrator in one jurisdiction to plan and organize the commission of offences elsewhere, safe from prosecution in that jurisdiction.

Enactment of CJO

16. The Administration has explained that the advent of communications has bred cross-border offences and the jurisdictional problem associated with such offences which involve transactions and events having taken place in more than one jurisdiction. CJO was enacted in December 1994 to address the jurisdictional problems associated with international fraud, enabling Hong Kong courts to exercise jurisdiction over specified offences in the following circumstances -

- (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.

17. Simply put, if a person in Hong Kong perpetrates a specified offence outside Hong Kong, or if a person outside Hong Kong perpetrates that offence in Hong Kong, that person is triable in Hong Kong courts.

Adding the three computer offences under the CJO

18. The addition of the three computer offences under the CJO will apply the rules set out in paragraph 16(a) to (e) to the offences, thus enabling Hong Kong courts to exercise jurisdiction over the offences when they are committed or planned outside the geographical boundaries of Hong Kong but are connected to or intended to cause damage in Hong Kong, or vice versa. In other words, the offences will be triable in Hong Kong if either the person who obtained access to the computer or the computer to which access was obtained is in Hong Kong.

Comparison of the provisions of CJO with the UK Computer Misuse Act 1990

19. The Subcommittee has noted that in the United Kingdom (UK), provisions about the jurisdiction of courts in relation to computer offences are contained in a separate piece of legislation known as the Computer Misuse Act 1990 (the UK Act). In response to the request of the Subcommittee, the legal adviser has provided a paper to compare the provisions in the CJO with those in the UK Act to assist members to consider whether jurisdiction rules of computer offences should be contained in a separate piece of legislation.

20. CJO makes provisions about the jurisdiction of courts in Hong Kong in relation to two groups of offences specified in section 2 of the Ordinance, referred to therein as Group A and Group B offences. Group A offences are theft or deception related offences in the Theft Ordinance (Cap. 210), and forgery related offences in the Crimes Ordinance (Cap. 200). Group B offences are conspiracy, attempting or incitement to commit a Group A offence, and conspiracy to defraud.

21. The objects of the draft Order are to add three computer offences to the Ordinance as Group A offences so that the jurisdiction rules in the Ordinance apply to those computer offences (paragraph 5 above refers).

22. The UK Act deals with the following three computer offences -

- (a) unauthorised access to computer material;
- (b) unauthorised access with intent to commit or facilitate commission of further offences; and
- (c) unauthorised modification of computer material.

23. It is the conclusion of legal adviser that the jurisdiction rules in the UK Act are essentially the same as in the CJO. Thus when the three computer offences are added to CJO, the effect would be that the jurisdiction rules in relation to them are essentially the same as for the computer offences included in the UK Act. The legal adviser has also pointed out that the UK Computer Misuse Act 1990 was enacted three years before the enactment of the Criminal Justice Act 1993, the UK equivalent of CJO.

Views of legal professional bodies

24. The Subcommittee has invited views from the two legal professional bodies on the draft Order. The Hong Kong Bar Association has indicated that it has no objection in principle to the proposed amendment in the draft Order. However, the Bar Association considers that the proposed amendment exposes the inadequate collection of legislation which criminalizes misuse of computers in Hong Kong, that there is an urgent need to undertake a fundamental review of Hong Kong legislation on computer offences, and there would be greater merit including extra territorial provisions in specifically tailored legislation rather than shoe-horn these provisions into the CJO.

25. The Law Society of Hong Kong has pointed out that section 2 of the UK Computer Misuse Act was more carefully drafted to differentiate between adult and juvenile offenders. The Law Society has also raised concerns on the way law enforcement agencies are seizing computers during investigation of offences and the possible adverse effects to a business.

Offence of "access to computer with criminal or dishonest intent" under section 161 of Crimes Ordinance

26. At the request of the Subcommittee, the Administration has provided some examples of the three proposed computer offences. In relation to the offence of "access to computer with criminal or dishonest intent" under section 161 of Crimes Ordinance, members note that the section 161 states 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".

27. Hon James TO and Hon Margaret NG have raised concern whether section 161 of the Crimes Ordinance criminalizes "mere intent". They have expressed reservation about bringing the offence of "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance within the scope of CJO to provide territorial jurisdiction of the offence.

28. The Administration has explained that section 161 of the Crimes Ordinance was enacted in 1993 by the Computer Crimes Ordinance, based on the recommendations in the report of 1988 of the then Attorney General's Chambers Working Group on Computer-related Crime (the Working Group).

29. The Working Group had observed that under the then existing law, most of the preparatory work for computer-related crime could be performed without committing any offence. It was considered desirable that unequivocal preparatory work which consisted of gaining access to a computer dishonestly and with intent to deceive or to cause loss to another or gain for the wrongdoer should be specifically punishable without waiting for the plan to be carried to completion or for it to amount to an attempt to carry out those offences. The Working Group therefore recommended creating a new computer offence of "dishonest accessing" along the lines that "any person who dishonestly accesses a computer, whether with or without due authority, with intent to deceive or with a view to gain for himself or another or with intent to cause loss to another, shall be guilty of an offence and shall be liable on conviction upon indictment to imprisonment for 5 years."

30. The Administration has advised that the necessary element of the offence is "dishonesty". If the individual does not act dishonestly there is no offence. And

dishonesty has an objective and subjective test as established in the case of R v Ghosh (1982), i.e. it must be dishonest -

- (a) according to the ordinary standards of reasonable and honest people; and
- (b) the defendant himself must have realized that what he was doing was by those standards dishonest.

Section 161 is never construed, nor is it capable of being used, to punish "mere intent".

31. The Administration has further advised that with the advancement of technology, as well as the prevalence and importance of the use of computers, section 161 is legally justifiable and required in the public interest for combating acts of access to computers which are preliminary to commission of further offences, causing loss to another or making gain by the offenders. Section 161 has been operating well since its enactment and there have not been any reported cases of miscarriage of justice in respect of this section. In any event, the court had applied a very high threshold for establishing proof of dishonest intent in relation to the offence in section 161 of the Crimes Ordinance.

VIEWS OF THE SUBCOMMITTEE AND THE ADMINISTRATION

Members' views

32. Members support the Administration's intention to take appropriate and effective measures to tackle transborder computer offences, but have reservations about the approach adopted to extend the territorial jurisdiction of the three computer offences. Hon Margaret NG does not support the draft Order. She requests that the Administration should consider drawing up a consolidated piece of legislation on computer offences and providing for extended jurisdiction in that legislation, instead of bringing them within the scope of CJO. Her view is shared by some other members.

33. Hon James TO considers that the mechanism to amend the list of offences under CJO, i.e. by an order made by the Chief Executive in Council with prior LegCo approval by way of an affirmative resolution, is not as desirable as a three-reading procedure. He has indicated that he is prepared to reconsider his position on the condition that -

- (a) the Administration would delete the proposed offence of "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance from the draft Order; and

- (b) the Administration should give an undertaking to the effect that the approach of adding offences to CJO for the purpose of extending territorial jurisdiction should not be adopted in future, and measures would be taken to enact legislation to deal with the territorial jurisdiction of the offences covered by CJO so that CJO would eventually be repealed.

The Administration's views

Adequacy of existing legislation to tackle computer offences

34. The Administration is of the view that the thrust of the legislative changes in 1993 to deal with computer crime is still along the right lines. Through amendments to the Telecommunications Ordinance (Cap. 106), the Crimes Ordinance (Cap. 200) and the Theft Ordinance (Cap. 210), new offences were created to cover computer crimes. In particular, the two offences of unauthorized access to computer by telecommunications (section 27A of the Telecommunications Ordinance) and access to computer with criminal and dishonest intent (section 161 of the Crimes Ordinance) have enabled many computer offences to be dealt with. In many cases, although no explicit reference to the cyber environment is made, the relevant legislation may be interpreted to cover both the physical and the virtual worlds.

35. Given that the existing legislation is generally adequate in tackling computer offences, the Administration does not consider it necessary to put in place a consolidated piece of legislation on computer offences at this stage.

CJO as the vehicle

36. According to the Administration, CJO has been specifically created to cater for circumstances to extend the normal jurisdictional rules for established offences. It is modelled on the United Kingdom Criminal Justice Act 1993. It is an appropriate vehicle to effect the changes intended under the draft Order.

37. The Administration does not dispute that it would be legally feasible to effect the changes through amendments to the principal ordinances. However, to the extent that all subsidiary legislation may be made through primary legislation, the Administration does not consider that this should in itself be the determining factor. Otherwise, it could lead to the illogical conclusion that all legislation should be effected through primary legislation.

38. The Administration believes that each case should be considered on its own merits. To rule out using the CJO in future (as proposed in paragraph 33(b) above) would amount to abrogating the CJO. This is outside the ambit of the draft Order, and is unreasonable from a legal policy point of view.

39. The Administration also believes that the procedures for making the order with prior approval of LegCo by way of an affirmative resolution have provided sufficient safeguards for ensuring effective legislative scrutiny.

40. In view of the above considerations, the Administration remains of the view that the draft Order is the appropriate means to effect the intended changes to jurisdictional rules for the three offences in question. For future cases, without affecting the generality of the principle that each case should be considered on its own merits, it will adopt the following guidelines -

- (a) careful consideration will be given to whether all the five principles set out in paragraph 16(a) to (e) above need to apply. Only where the answer is affirmative will the use of CJO be contemplated; and
- (b) if the legislative exercise involves not only jurisdictional rules but also other issues which should be dealt with in a principal ordinance, e.g., the evidential rules and law enforcement powers related to an offence, then the general rule would be to effect all the changes, including those concerning jurisdictional rules, through an amending Bill. A relevant example is the Theft (Amendment) Bill 1999, through which the offence of fraud was added to the list of offences under section 2(2) of CJO, instead of through the mechanism under sections 2(4) and (5) of CJO.

41. The Administration has confirmed that it will not give fresh notice for moving a motion to seek the approval of LegCo on the draft Order at the last Council meeting in the current LegCo session. The Administration will continue to consult LegCo on legislative proposals involving jurisdictional rules in the next LegCo term.

RECOMMENDATION

42. The Subcommittee recommends that the Administration should revert to LegCo in the next term on how it proposes to take forward the matter, while addressing members' concern about the approach adopted by the Administration to extend the territorial jurisdiction of the three computer offences.

43. The Subcommittee also recommends that, as computer technology is developing rapidly, the Administration should consider setting up a standing working group to regularly review whether existing legislation is adequate to deal with new computer crimes, and to have interface with the relevant Panel of LegCo to facilitate early and in-depth deliberation.

ADVICE SOUGHT

44. Members are invited to note this paper.

Council Business Division 2
Legislative Council Secretariat
25 June 2004

**Subcommittee on
the draft Criminal Jurisdiction Ordinance
(Amendment of Section 2(2)) Order 2002**

Membership List

Chairman	Hon James TO Kun-sun
Members	Hon Cyd HO Sau-lan Hon Margaret NG Hon CHAN Kwok-keung Hon SIN Chung-kai Hon Ambrose LAU Hon-chuen, GBS, JP (Total : 6 Members)
Clerk	Mrs Percy MA
Legal Adviser	Mr LEE Yu-sung
Date	8 January 2003