立法會
Legislative Council

LC Paper No. CB(2)823/02-03(03)

Ref : CB2/SS/3/02

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

Background brief prepared by the Legislative Council Secretariat

Report of the Inter-departmental Working Group on Computer Related Crime

Purpose

This paper gives a summary of issues and concerns raised by Members on the report of the Inter-departmental Working Group on Computer Related Crime (the Working Group).

The Working Group's recommendations

2. At its meeting on 7 December 2000, the Panel on Security was consulted on the report of the Working Group and its recommendations. The Working Group has recommended, inter alia, that the following offences, as modified to take into account the recommendations in the report, should be covered by the Criminal Jurisdiction Ordinance (Cap. 461) -

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

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

Issues and concerns raised by Members

3. At the meeting on 7 December 2000, Members raised a number of issues and concerns relating to the Working Group's report. These included -

(a) whether the existing legislation was adequate to deal with the problems of copyright infringement, illegal gambling and pornographic materials on the Internet;

(b) the jurisdictional problem in removing offending materials on websites;

(c) whether there were international organisations promoting the adoption of common standards and goals in combating computer-related crime;

(d) whether there was in place a mechanism to protect critical infrastructures against cyber attacks; and

(e) whether it was proper to make it compulsory for a person to disclose decryption tools or decrypted text.

4. The Administration had not mentioned the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 at the meeting and there were no comments from Members directly related to the addition of offences to the Ordinance.

5. The Panel met with 12 organisations/individuals at its meeting on 10 February 2001. These organisations/individuals were in general supportive of the direction in dealing with computer-related crime. They had put forward various views and suggestions on the technical aspects of the Working Group's report and related policy aspects. However, the discussions were not specific on the draft Order.

6. Members may wish to refer to the extracts from the minutes of the Panel meetings on 7 December 2000 and 10 February 2001 in **Appendices I and II** respectively for details of the discussions.

Way forward in respect of the Working Group's recommendations

7. The Administration issued a Legislative Council (LegCo) Brief on the way forward in respect of the Working Group's recommendations on 16 July 2001. The Panel on Security has not discussed the way forward. The LegCo Brief is in **Appendix III** for members' ease of reference.

Council Business Division 2
Legislative Council Secretariat
7 January 2003

Appendix I

EXTRACT

立法會
Legislative Council

LC Paper No. CB(2) 682/00-01
(These minutes have been seen by
the Administration)

Ref : CB2/PL/SE/1

LegCo Panel on Security

Minutes of meeting
held on Thursday, 7 December 2000 at 2:30 pm
in Conference Room A of the Legislative Council Building

Members present	:	Hon LAU Kong-wah (Chairman) Hon James TO Kun-sun (Deputy Chairman) Hon Margaret NG Hon Mrs Selina CHOW LIANG Shuk-yee, JP Hon CHEUNG Man-kwong Hon Andrew WONG Wang-fat, JP Hon Ambrose LAU Hon-chuen, JP Hon IP Kwok-him, JP
Members attending	:	Hon SIN Chung-kai Hon Henry WU King-cheong, BBS
Members absent	:	Hon Albert HO Chun-yan Dr Hon LUI Ming-wah, JP Hon Howard YOUNG, JP Hon WONG Sing-chi
Public Officers attending	:	Item III Miss CHEUNG Siu-hing Deputy Secretary for Security (Special Duties) Mr LEE Ka-chiu Chief Assistant Secretary for Security F

Item IV

Mrs Jennie CHOK
Deputy Secretary for Security 2

Mr David WONG
Principal Assistant Secretary for Security B

Mr CHAN Chun-yan
Assistant Commissioner of Correctional Services

Mr William HUI
Civil Secretary
Correctional Services Department

Clerk in attendance : Mrs Sharon TONG
Chief Assistant Secretary (2)1

Staff in attendance : Mr Raymond LAM
Senior Assistant Secretary (2)5

Action

X X X X X X

III. Interdepartmental Working Group on Computer Related Crime : Follow up
(Report of Interdepartmental Working Group on Computer Related Crime and LegCo Brief Ref. : SBCR 14/3231/88 Pt.14)

6. At the invitation of the Chairman, Deputy Secretary for Security (Special Duties) (DS for S(SD)) briefed Members on the Report of the Interdepartmental Working Group on Computer Related Crime (the Report).

Jurisdictional problem

7. Referring to paragraph 8.30 of the Report, Mr CHEUNG Man-kwong asked whether existing legislation was adequate for dealing with the problems of copyright infringing articles, illegal gambling and pornographic materials transmitted through the Internet. He expressed concern about the jurisdictional problem in respect of the removal of offending materials or web sites. He said that some activities which were illegal in Hong Kong, such as gambling on football matches, might not be illegal in some other countries. He asked how the problem would be addressed by the

Administration.

8. DS for S(SD) said that as these offences could also be committed through other means besides the Internet, they should be dealt with under the relevant policy context by the respective policy bureaux concerned. As an example, she cited the consultation paper entitled "Protection of Youth from Obscene and Indecent Materials : 2000 Review of the Control of Obscene and Indecent Articles Ordinance(COIAO)" — COIAO was applicable to electronic publications, and 10 out of 12 prosecutions under COIAO between January 1996 and April 2000 against electronic publications had been successful. She said that the Working Group had indeed considered the possibility of amending the offences covered by the Criminal Jurisdiction Ordinance (Cap. 461) (CJO) to all offences triable on indictment. As this might also change the jurisdictional rules regarding non-computer related offences, the Working Group recommended that consideration should be given to conducting a thorough in-depth study of the subject of jurisdictional rules in general. She pointed out that the Working Group had also recommended bringing some individual computer-related offences to be covered by CJO. As regards the removal of offending materials or web sites, she said that the Working Group had suggested that reference could be made to legislation related to copyright in the United States (US) in the formulation of take-down procedures.

Approach for implementation of recommendations

9. Mr SIN Chung-kai expressed support for the Administration's study of legislative and administrative measures against computer-related crime. He considered that non-controversial recommendations of the Working Group, such as better defining the term "computer", should be implemented as soon as possible while more controversial recommendations could be further studied. DS for S(SD) said that it was the Administration's intention to implement the recommendations in phases. However, the Administration considered it more appropriate to consult the public on the Report as a whole because it outlined a framework. Depending on the feedback received during the consultation exercise, the priority for implementing the recommendations would be decided. Mr SIN suggested that the Administration should classify the recommendations as short-term, medium-term and long-term ones to facilitate studying of the recommendations of the Working Group.

Consultation period

10. Mr SIN Chung-kai considered that the consultation period of two months for the recommendations of the Working Group was too short. He suggested that it should be extended by one month to allow more time for studying the Report. Mr Henry WU shared the same view. DS for S(SD) responded that if there was a consensus among members on the consultation period, she saw no objection to extending the consultation period to three months.

Protection of critical infrastructures from cyber attacks

11. On the protection of critical infrastructures from cyber attacks, Mr James TO said that paragraphs 9.15 and 9.17 of the Report reflected that the Working Group seemed to have no knowledge about the existing situation regarding the protection of infrastructures against cyber attacks. He considered that the Police, which was also represented in the Working Group, should have been following the matter closely and aware of the existing situation. He asked whether the Working Group had contacted individual organisations to understand their plans for protection of critical infrastructures against cyber attacks.

12. DS for S(SD) responded that the Working Group had not carried out an in-depth study of the security of critical infrastructures. However, informal enquiries made by the Working Group indicated that there were contingency plans for most critical infrastructures, although there was currently no mechanism for the coordination of these plans. She said that there was not even an agreed list of critical infrastructures in Hong Kong. She added that the protection of critical infrastructure was a huge task. In US, the Commission on Critical Infrastructure Protection, which had over 60 supporting staff, took 16 months to complete its report. Referring to paragraph 9.18 of the Report, she pointed out that the Working Group recommended the establishment of a standing central coordinating mechanism to protect critical infrastructures from cyber attacks.

13. In response to Mr James TO's comment that there seemed to be no recommendation in the Report for the establishment of a committee to oversee the protection of critical infrastructures, DS for S(SD) said that the Administration was inclined to tackling the issue through existing mechanisms where feasible. A possibility was to assign the task to the subcommittee or task force that the Working Group had recommended to be established under the Fight Crime Committee (FCC). The detailed arrangements would be worked out after the overall institutional framework for addressing computer-related crime had been finalized.

Computer-related commercial crime

14. Mr Henry WU said that there was a lack of reference to computer-related commercial crime in the Report. DS for S(SD) said that a breakdown of reported cases of computer crime could be found in paragraph 1.2 of the Report.

15. Mr Henry WU said that with the development of trading of securities on the Internet, the Administration should put more effort in the prevention of computer-related crime in respect of such trading.

International co-operation against computer-related crime

16. In response to Mr Henry WU's question about whether there were international organizations promoting the adoption of common standards and goals in combating computer-related crime, DS for S(SD) said that there was currently no international organization established for such a purpose. However, various organizations, such as the Council of Europe which was preparing a Draft Convention on Cyber Crime, was

working in this direction. She added that the establishment of an international contact point system among the law enforcement agencies of different countries would much facilitate combating computer-related crime. In response to Mrs Selina CHOW's question about the adequacy of the existing contact point system, DS for S(SD) said that a comprehensive international contact point system was not yet in place. The Administration would seriously consider participating in such a system when it was established.

Consultation

17. Miss Margaret NG asked whether consultation had been made by the Working Group in the discussion process. She also asked whether consultation had been made in respect of the proposed compulsory disclosure of the decryption tools or decrypted text of encoded computer records, as referred to in paragraph 8(g) of the LegCo Brief. DS for S(SD) said that the Working Group had not conducted formal public consultation in its discussion process. Since the commencement of the consultation exercise in the afternoon of 1 December 2000, no submission had been received, although there were one to two comments in newspapers.

18. Mr Henry WU declared interest as the Chairman of the Eastern District FCC. He asked whether the Administration would brief district FCCs on the recommendations in the Report. DS for S(SD) responded that a briefing had been scheduled for the chairmen of district FCCs on 22 December 2000.

Compulsory disclosure of decryption tools or decrypted text

19. Miss Margaret NG questioned whether it was proper to make it compulsory for a person to disclose decryption tools or decrypted text. DS for S(SD) said that the Working Group had considered other options, for example, depositing the decryption tools or decrypted text with an independent body but noted that privacy issues might arise from such an arrangement. She stressed that the requirement would only apply to more serious offences. Judicial authorization would also be needed for compulsory disclosure. She added that in the United Kingdom, judicial authorization was not a must and the involvement in a serious offence was not required for compulsory disclosure. Miss NG considered that the issue was related to an individual's fundamental right, rather than a person's privacy.

Other issues

20. Mr SIN Chung-kai said that the term "Internet Service Providers" was too narrow. It should be amended as "On-line Service Providers", as in US. DS for S(SD) undertook to consider the suggestion. Adm

21. Referring to paragraph 14.2 of the Report, Mr SIN Chung-kai said that while the Administration had quoted the Draft Convention on Cyber Crime issued by the Council of Europe in April 2000, it had not pointed out that a further document issued by the Council of Europe in October 2000 revealed that about 30 organizations were opposed

to the Draft Convention. DS for S(SD) explained that the Report was completed in September 2000, which was before the issue of the October version of the Draft Convention. She added that a further version was released by the Council of Europe in November 2000. She stressed that the Draft Convention only served as a reference for the Working Group.

22. Mrs Selina CHOW considered it important to educate the public on the prevention of computer-related crime. She asked about the resources allocated for the prevention of computer-related crime and the adequacy of Police manpower in combating computer-related crime. DS for S(SD) said that she had no information on hand about the amount of resource allocated. Such resource was also very difficult to quantify. She acknowledged that the adequacy of manpower resource was difficult to assess in view of the rapidly changing situation regarding computer crime. Nonetheless, should there be a need for additional manpower, requests would be submitted in the normal manner. She stressed that the prevention of computer-related crime was a key recommendation of the Report.

23. In response to Mrs Selina CHOW's question about the participation of the private sector in the prevention of computer-related crime, DS for S(SD) said that there was currently no standing mechanism for such participation. She informed Members that consideration was being given to putting more effort in this respect.

24. Miss Margaret NG commented that the Report was very technical in nature. She suggested that the legal profession and relevant industries should be invited to give their views on the subject. Members agreed that a special meeting be held on 10 February 2001 from 9:00 am to 12:00 noon to receive public views on the Report. They also agreed that all other LegCo Members would be invited to the meeting.

X X X X X X

Legislative Council Secretariat
15 January 2001

Appendix II

立法會
Legislative Council

LC Paper No. CB(2) 2120/00-01
(These minutes have been seen
by the Administration)

Ref : CB2/PL/SE/1

LegCo Panel on Security

Minutes of special meeting
held on Saturday, 10 February 2001 at 9:00 am
in the Chamber of the Legislative Council Building

Members present :
Hon LAU Kong-wah (Chairman)
Hon James TO Kun-sun (Deputy Chairman)
Hon Margaret NG
Hon Howard YOUNG, JP
Hon Ambrose LAU Hon-chuen, JP
Hon IP Kwok-him, JP

Members attending :
Hon Eric LI Ka-cheung, JP
Hon SIN Chung-kai
Hon Audrey EU Yuet-mee, SC, JP

Members absent :
Hon Albert HO Chun-yan
Dr Hon LUI Ming-wah, JP
Hon CHEUNG Man-kwong
Hon Mrs Selina CHOW LIANG Shuk-yee, JP
Hon Andrew WONG Wang-fat, JP
Hon WONG Sing-chi

Public Officers attending :
Miss CHEUNG Siu-hing
Deputy Secretary for Security (Special Duties)

Mr John LEE Ka-chiu
Chief Assistant Secretary for Security

Attendance by Invitation : The Law Society of Hong Kong

Mr Kevin STEEL
Member, Criminal Law & Procedure Committee

Hong Kong Internet Service Providers Association

Mr Chester SOONG
Chairman

The Institution of Electrical and Electronics Engineers, Hong Kong Section (Computer Chapter)

Dr Joseph NG Kee-yin
Chairman

Hong Kong Computer Society

Dr Louis MA
Vice President (Membership)

Mr Bill FOK
Director of Community Service

International Federation of the Phonographic Industry (Hong Kong Group)

Mr Ricky FUNG Tim-chee
Chief Executive Officer

Hong Kong Information Technology Federation

Mr LEE Kheng-joo
Council Member

Hong Kong Society of Accountants

Mr Michael K H CHAN
Chairman of Information Technology Committee

Mr Peter TISMAN
Deputy Director (Professional Practices)

Hong Kong Information Systems Audit and Control Association (Hong Kong Chapter)

Ms Susanna CHIU
Vice President

Mr William GEE
Membership Director

Hong Kong Institution of Engineers (Information Technology Division)

Ir Jolly WONG
Past Chairman

Ir K C LAI
Hon Secretary

Webmaster (Hong Kong) Association

Ms Elizabeth QUAT
President and Co-founder

Mr Ringo LAM
Co-founder & Past President

Information Security and Forensics Society

Mr Ricci IEONG
Secretary

Individual

		Mr Wanbil LEE
Clerk in attendance	:	Mrs Sharon TONG Chief Assistant Secretary (2)1
Staff in attendance	:	Mr Raymond LAM Senior Assistant Secretary (2)5

Action

I. To receive public views on the issues raised and recommendations made in the Report of the Inter-departmental Working Group on Computer Related Crime (the Report)

Meeting with representative of the Law Society of Hong Kong
(LC Paper No. CB(2) 846/00-01(01))

Mr Kevin STEEL presented the views as detailed in the submission of the Law Society of Hong Kong.

Meeting with representative of the Hong Kong Internet Service Providers Association
(LC Paper No. CB(2) 811/00-01(01))

2. Mr Chester SOONG presented the views as detailed in the submission of the Hong Kong Internet Service Providers Association (HKISPA).

Meeting with representative of the Institution of Electrical and Electronics Engineers, Hong Kong Section (Computer Chapter)
(LC Paper No. CB(2) 828/00-01(01))

3. Dr Joseph NG Kee-yin presented the views as detailed in the submission of the Institution of Electrical and Electronics Engineers, Hong Kong Section (Computer Chapter).

Meeting with representatives of the Hong Kong Computer Society
(LC Paper No. CB(2) 811/00-01(02))

4. Dr Louis MA presented the views as detailed in the submission of the Hong Kong Computer Society.

5. Mr Bill FOK informed Members that the word "escorted" as referred to in the third paragraph of the second page of the submission should read

"escrowed".

Meeting with representative of International Federation of the Phonographic Industry (Hong Kong Group)
(LC Paper No. CB(2) 811/00-01(03))

6. Mr Ricky FUNG Tim-chee presented the views as detailed in the submission of International Federation of the Phonographic Industry (Hong Kong Group) (IFPI).

Meeting with representative of the Hong Kong Information Technology Federation
(LC Paper No. CB(2) 832/00-01(01))

7. Mr LEE Kheng-joo presented the views as detailed in the submission of the Hong Kong Information Technology Federation (HKITF).

Meeting with representatives of the Hong Kong Society of Accountants and the Hong Kong Information Systems Audit and Control Association (Hong Kong Chapter)
(LC Paper No. CB(2) 828/00-01(02))

8. Mr Michael CHAN, Mr Peter TISMAN, Mr William GEE and Ms Susanna CHIU presented the views as detailed in the joint submission of the Hong Kong Society of Accountants and the Hong Kong Information Systems Audit and Control Association (Hong Kong Chapter).

Meeting with representatives of the Hong Kong Institution of Engineers (Information Technology Division)
(LC Paper No. CB(2) 828/00-01(03))

9. Ir Jolly WONG presented the views as detailed in the submission of the Information Technology Division of the Hong Kong Institution of Engineers.

Meeting with representatives of the Webmaster (Hong Kong) Association
(LC Paper No. CB(2) 811/00-01(04))

10. Mr Ringo LAM presented the views as detailed in the submission of the Webmaster (Hong Kong) Association.

Meeting with Mr Wanbil LEE
(LC Paper No. CB(2) 828/00-01(04))

11. Mr Wanbil LEE presented the views as detailed in his submission for the meeting.

Meeting with representative of the Information Security and Forensic Society
(LC Paper No. CB(2) 841/00-01(01))

12. Mr Ricci IEONG presented the views as detailed in the submission of the Information Security and Forensic Society.

Issues raised by Members

13. Mr Howard YOUNG pointed out that HKITF suggested that the log records of accounts be kept by Internet service providers (ISPs) for less than three months, while the Webmaster (Hong Kong) Association considered that keeping the log records for a longer time would not result in a substantial increase in cost for ISPs. He asked about the rationale for keeping log records for a period of less than three months.

14. Mr LEE Kheng-joo responded that according to past experience and in consultation with HKISPA, HKITF considered that keeping a log record for three months was sufficient and feasible. Mr Howard YOUNG expressed concern that keeping the log records for three months or less might not be sufficient, as computer-related crime sometimes took a long time to detect.

15. Mr SIN Chung-kai said that computer-related crime might be difficult to define, as a person could use a local computer to activate a computer in overseas to hack a computer system in Hong Kong. He expressed concern that the Report had been compiled by the Inter-departmental Working Group on Computer Related Crime (the Working Group) without the assistance of the business sector and professional associations. He sought the attending deputation's views on whether the Administration should refer the issues raised in the Report to the Fight Crime Committee (FCC) for further examination. He added that while legislative amendments on computer-related crime might offer more protection, it might also hinder information technology (IT) development. Given that the subject of jurisdictional rules was still to be studied, he asked how computer related crime should be addressed and whether it was the appropriate time to introduce legislative amendments.

16. Deputy Secretary for Security (Special Duties) (DS for S(SD)) responded that the Administration would analyse the views received in the consultation exercise before determining the way forward. She said that even if the legislative amendments were to be introduced as proposed in the Report, it would be unlikely that a single piece of legislation would be introduced. While some legislative amendments could be introduced earlier, other legislative amendments such as those related to encryption might need more time to study. Bodies such as The Law Reform Commission would also take at least two to three years to study the jurisdictional rules.

17. Mr Chester SOONG considered that the issues raised in the Report

should be referred to FCC for further examination and consultation with the relevant parties should be conducted. This would assist the Government in better assessing the situation before the introduction of legislative amendments.

18. Mr Ricky FUNG Tim-chee said that besides the introduction of legislation on computer related crime, the Copyright Ordinance should also be amended.

19. Mr Ringo LAM commented that the Report had placed too much emphasis on legislative amendments. He considered that instead of forming different inter-departmental working groups to address different subjects such as computer-related crime, Internet gambling and copyright on the Internet, a new institution should be established under the Information Technology and Broadcasting Bureau (ITBB) to coordinate all work and address issues related to computer related crime and the Internet, including copyright on the Internet. He informed Members that legislation on copyright in the United States had been found inadequate for addressing copyright problems on the Internet. Many pieces of legislation had thus been enacted in the area in recent years. Ms Elizabeth QUAT said that the establishment of such an institution under ITBB would be more effective than the current arrangement of addressing problems on a piece meal basis.

20. Mr Bill FOK considered that instead of placing too much emphasis on legislative amendments at this stage, public education on information security should be stepped up.

21. Mr LEE Kheng-joo said that existing legislation had already set out the foundations for addressing various crimes. Discussions on computer-related crime would be ongoing. It was thus not possible to have one piece of comprehensive legislation on computer-related crime.

22. Mr Michael CHAN supported the view that an institution should be established under ITBB. He said that such a suggestion had been made by the Hong Kong Society of Accountants in the past when ITBB was first established. He added that both short-term and long-term solutions were needed for addressing the problem of computer related crime.

23. Mr William GEE said that it was difficult for the enactment of legislation to catch up with the rapid development of technology. Besides the enactment of legislation, everyone had a responsibility to safeguard the security of his own computer system. Codes of practice on computer security should be drawn up by the relevant professional bodies and organisations. Public education on information security should also be strengthened.

24. Dr Joseph NG said that as the enactment of legislation would take time, public education should be stepped up. He added that actions should be taken

in respect of short-term solutions identified in the Report, while the more fundamental issues could be examined at the same time.

25. Ms Audrey EU sought the views of attending deputations on the problem of Internet gambling. She asked whether it was technically viable to address the problem.

26. Mr LEE Kheng-joo said that it would be very difficult to take actions against bookmakers located overseas. Dr Joseph NG said that although it was technically viable to block certain web sites, offenders could easily establish another site on the Internet. He considered that little could be done in respect of enforcement against Internet gambling. Public education might be a more effective means in addressing the gambling problem. Mr Ricci IEONG said that the blocking of a web site would need the collaborative effort of all local universities and ISPs. Mr William GEE said that although the blocking of a web site would need the collaborative effort of all parties concerned, the question of who should be responsible for coordinating the blocking of a web site would have to be considered. He added that even if access to an overseas web site was completely blocked, a user could still establish connection with an overseas web site by means of a long distance call. It was thus very difficult to prevent Internet gambling. He considered that it would be more effective to address the problem through other means.

27. DS for S(SD) said that the Working Group had focussed its work on the macro problems of computer-related crime, such as encryption, jurisdictional rules and the adequacy of resources of law enforcement agencies. With the very rapid development of computer technology, the examination of all crimes that might be committed via the computer or the Internet, such as Internet gambling and pornographic materials, would be an endless task. Thus, the Working Group did not seek to deal with all crimes that might be committed via the computer or the Internet. They would be dealt with under the relevant policy context by the respective policy beaux concerned. She added that the Working Group comprised representatives from various government bureaux and departments, including ITBB. As regards denial of service, she said that prosecution had been made in the past under the Crimes Ordinance. However, it might not be possible under existing legislation to prosecute overseas hackers because of the jurisdictional problem.

28. Mr Ringo LAM said that from the perspective of a general public, he was concerned that the meaning of national security was unclear. He added that one might unintentionally breach the laws of the Mainland, as most people had little knowledge about Mainland laws.

29. Miss Margaret NG said that in the promotion of IT, it was important to create a safe environment that facilitated the privacy and freedom from surveillance. She considered that the recommendation in the Report in respect

of decryption was unacceptable. There should be a balance between protection against crime and the maintenance of a safe environment. With the compulsory disclosure of decryption tools or decrypted text and the maintenance of log records by ISPs, a safe environment could not be achieved because all users would be exposed to total surveillance. She hoped that a code of practice would soon be developed to facilitate a safe environment that provided protection against both crime and surveillance. She expressed concern that computer-related crime was suggested to be so broadly defined that innocent persons might be wrongly criminalised. In her view, it was important to ensure that compliance was viable before an act was criminalized. Problems related to jurisdictional rules should be dealt with speedily. As regards extraterritorial gambling, she said that the issue was being studied by the Bills Committee on Gambling (Amendment) Bill 2000. She invited the views of deputations on the drawing up of a code of practice to build up a safe environment.

30. Mr Bill FOK said that codes of practice were practical solutions to problems especially given that the enactment of legislation would take some time. In fact, there were already well established codes of practice and guidelines that complied with international standards in Hong Kong, although the majority of people in Hong Kong had not paid much attention to such codes.

31. Ms Susanna CHIU said that the removal of an offending web site should be carried out by the Commercial Crime Bureau of the Police rather than ISPs. She added that the commercial sector and the public seldom paid attention to codes of practice. Many small or medium sized companies lacked resources to introduce information security measures. Legislation were thus needed for a deterrent effect.

32. Mr William GEE said that as the environment of Internet was an insecure one, encryption and surveillance were needed for ensuring safety. He said that although closed circuit television systems could be found in many companies, they were intended for creating a deterrent effect rather than genuine surveillance. He added that codes of practice would facilitate building up a safe environment. He said that many codes of practice, best practices and guidelines were already in place in Hong Kong. Many international standards, such as ISO 17799, were under development. However, it was not possible to apply one single code of practice across different industries. The code of practice that should be adopted might be different from one industry to another. He added that besides putting in place codes of practice, a third party was also needed for monitoring compliance with the codes.

33. Mr Ricci IEONG said that the keeping of log records by ISPs was necessary because one could not know the identity of the person to whom communication was made. He informed Members that a hacker was found to have used the IP address of his former colleague to hack a certain important infrastructure. Without the log, it would have been very difficult to identify

who had performed the hacking. As regards denial of service, he said that existing legislation might not be adequate for dealing with situations where a hacker merely brought a system to a halt.

34. Mr Ricky FUNG Tim-chee said that although codes of practice were useful, IFPI hoped that legislation on "take down" procedures would be enacted.

35. Mr LEE Kheng-joo said that there was a lot of exchange between local and overseas ISPs on codes of practice. There was also peer group pressure for compliance with the codes of practice.

36. Mr Wanbil LEE said that the computer was a good tool in that it could extend one's intellectual power, although whether it would benefit or cause harm to the community would depend on how it was used. As regards blockage of web sites, it would be necessary to examine the information in the web site before a decision was made on whether blockage should be carried out. He said that the enactment of laws was always lagging behind events. While the discussions at the meeting had focussed on solutions and implementation aspects, he considered that the problem should be more clearly defined. As the process would be a lengthy one, short-term solutions should be introduced for the time being in parallel with the examination of the problem in a systematic way.

37. Mr James TO expressed concern that section 33 of the Telecommunications Ordinance had not been implemented after its enactment in 1997. He sought the views of deputations on whether there were legislative measures that should be introduced within a year's time. The Chairman said that the attending deputations could provide a written response after the meeting.

38. DS for S (SD) said that she believed that both the Administration and attending deputations shared the view that a good environment conducive to the legitimate use of the computer and the Internet should be provided. She pointed out that although the first few chapters of the Report focussed on legislative measures, the recommendations of the Working Group were not confined to such measures. The Working Group had in fact pointed out that administrative measures, which would require more sustained effort to implement, might be more effective in addressing the problem. Nevertheless, legislative measures would serve as a safety net.

39. The Chairman thanked the deputations for attending the meeting. He welcomed the deputations to provide further views, if any, to the Panel in writing.

40. The meeting ended at 12:05 pm.

Legislative Council Secretariat
17 July 2001

Appendix III

Ref. : SBCR 14/3231/88 Pt. 21

LEGISLATIVE COUNCIL BRIEF

REPORT OF INTER-DEPARTMENTAL WORKING GROUP ON COMPUTER RELATED CRIME

INTRODUCTION

At the meeting of the Executive Council on 10 July 2001, the Council ADVISED and the Acting Chief Executive ORDERED that the way forward set out in paragraphs 8 to 29 below should be adopted.

BACKGROUND AND ARGUMENT

General Background

2. On 30 November 2000, we submitted a Legislative Council brief on the report of Inter-departmental Working Group on Computer Related Crime (WG). The report identified a number of existing inadequacies. On the legislative side, for example, the penalties for certain computer offences such as hacking are on the low side compared to those for theft and deception, which are offences of similar nature. In addition, the application of certain legal concepts has yet to take into full account requirements of the information age. A case in point is the question of jurisdiction. Traditional jurisdictional rules are based on geographical boundaries, whereas computer crime knows no borders. A stark inadequacy is the unclear jurisdiction over hacking originated from outside Hong Kong. The increasing use of encryption technologies also presents problems to making sense of encrypted computer evidence. On the administrative side, the WG identified the need to better enlist the help of Internet service providers (ISPs), the private sector in general as well as overseas law enforcement agencies to combat computer crime. In addition, the resilience of our critical infrastructures to cyber attacks has to be thoroughly assessed and properly sustained. The WG also considered that existing institutional arrangements for tackling computer crime should be strengthened.

3. We subsequently released the WG's report for public consultation on 1 December 2000. At the request of the Legislative

Council Panel on Security, the consultation period was extended from the original two months to three months, i.e., lasting until 28 February 2001.

Analysis of Submissions and Government's Response

(A) General

A

B

4. Altogether we have received 46 written submissions. A full list of the respondents is at Annex A. While some comments are brief and are targeted at one or two specific recommendations of the report, many are fairly detailed and cover a number of issues. A summary table of the written comments received set against the major recommendation categories of the report is at Annex B.

5. According to the written submissions received as well as views gathered at various briefing sessions and discussion forums, Government's effort to put together the framework outlined in the report is in general well appreciated, especially by the information technology industry and professionals. Many are encouraged by Government's recognition of the crime problems brought about by the digital age. Although a few respondents take the view that the report could have devoted more coverage to issues like online copyright infringement, most respondents consider that the report has covered the main issues associated with computer crime.

6. Many of the report's recommendations, especially those on increasing public education and the private sector's role in preventing and combating computer crime, have received across-the-board support. There is also general agreement on the need to increase the resilience of our critical infrastructures against cyber attacks. Many agree that ISPs might play a useful role in helping criminal investigations into computer crime, although views differ on the extent and details. Comments on the proposed legislative changes are varied. While the majority support strengthening the legislative framework, there are different views regarding the penalty levels and the exact matters to be provided for. Nonetheless, insofar as many of the comments seek to address the operational aspects of the proposed legislative changes, there appears to be general acceptance of the underlying principles.

7. Our broad-brush analysis of the comments and views gathered in respect of the WG's specific recommendations and our response are set out in paragraphs 8 to 29 below.

(B) Specific Recommendations

(a) Defining “computer” in law

8. The WG recommended using the term “information system” as defined in the Electronic Transactions Ordinance (ETO) in place of “computer”, which is usually undefined in our current legislation. There are opposite views on this recommendation. Some respondents support it, as they consider that the term “information system” is more comprehensive. Others, however, feel that the term “computer” should be left to be interpreted by the court or that it covers more than “information system”.

9. The comments received indicate that there are indeed many different interpretations of the term “computer”. We therefore agree with the WG that we should set out in our laws some parameters within which the concept of “computer” should be interpreted. The term “information system” as defined in the ETO should be a starting point for the purpose. As the Administration is committed to reviewing the ETO to take into account latest technological developments and international practice, the WG’s recommendation to peg the definition of “information system” to that in the ETO provides a ready mechanism for review and updating as necessary. In addition, as the WG suggested, opting out from the general amendment exercise will be allowed where appropriate. On balance, therefore, we accept the WG’s recommendation.

(b) Jurisdiction

10. The WG pointed out that traditional jurisdiction rules, being largely based on geographical boundaries, would need review to take into account requirements of the information age. Given that a computer crime may well involve two or more jurisdictions, most respondents agree that the question of jurisdiction should be tackled. Some consider that the time required for a thorough study by a body such as the Law Reform Commission as recommended by the WG is too long, but accept that the issues are complex. Among those who have commented on the issue, there is general agreement with the WG that we should as a first step bring unauthorized access to computers and access to computers with criminal or dishonest intent within the scope of the Criminal Jurisdiction Ordinance, so that extended jurisdictional rules may apply to these offences. Accordingly, we accept in principle the WG’s recommendations in this regard. As regards the more general review of jurisdictional rules, however, we recognize that the Law Reform

Commission is already committed to a number of projects. We will therefore task the Department of Justice to conduct the initial legal research in the first instance.

(c) Encryption

11. The WG considered it necessary to enable law enforcement to comprehend encoded computer information relevant to an investigation. It therefore recommended introducing requirements for the compulsory disclosure of the decrypted text or decryption tool for encrypted computer information, subject to safeguards such as judicial oversight. Given privacy concerns, most respondents have pointed to the need to approach the subject with caution. Many respondents do not query the underlying principles, but are mainly concerned that sufficient safeguards are in place to prevent abuse of the proposed power. A few respondents, however, object to the proposal for compulsory disclosure on grounds of principle because of the perceived breach of privacy rights involved and concern at possible self-incrimination. Across the spectrum of views, there is almost unanimous support for the WG's proposals to introduce judicial scrutiny of the exercise of the power of compulsory disclosure, and to confine the power to more serious crimes.

12. We accept the WG's premise that it is necessary to enable law enforcement to make sense of lawfully obtained evidence. We also agree that any additional powers should be proportionate, and that appropriate safeguards should be put in place. The WG's recommendations on encryption already strike the right balance between law enforcement facilitation and respect for privacy. As such, we accept them as the framework for taking the subject forward. Given that the WG's recommendations only set out the main principles, however, it is critically important to ensure that the resultant regulatory regime is enforceable. For this purpose, different scenarios involving different parties to the encryption process should be fully thrashed out. Ideally, overseas experience in this regard should also be taken into account. To our knowledge, the United Kingdom is the only developed economy that has passed legislation providing for similar powers. This legislation has yet to be brought into effect pending the promulgation of a code of practice governing its operation. We will therefore work out the implementation details, including the coverage and procedures, taking into account the suggestions received so far and further consulting relevant parties as appropriate, before any draft legislation is prepared. We will also closely monitor relevant overseas developments.

(d) Protection of computer data

13. The WG recommended strengthening existing legislative provisions to better protect computer data. For example, it recommended protecting all computer data at all stages of storage or transmission via a computer or the Internet; and better defining the concepts of access and unauthorized access to the computer. At the same time, the WG found it unnecessary to legislate against hacking tools (programs that may enable unauthorized access to computer data or programs). In general, the spirit of the recommendations is accepted by respondents. There are different views on some details. For example, some consider that the concept of "unauthorized access" should be defined to protect unwitting intruders. A few respondents believe that data transmitted by open networks, and not the Internet alone, should also be protected. With the significant exception of the recording industry, there is firm support for the WG's view that we should not control hacking tools. A few have suggested that, in addition to the WG's proposals on hacking, port scanning and host scanning (probing of computer systems) should be outlawed, because in some cases they may be preludes to hacking. Others however believe that the mere act of scanning should not be criminalized as there may be legitimate reasons for the act. Some consider that there should be express provisions against the spreading of computer viruses and denial of service attacks, as they impair the proper functioning of computers.

14. The suggestions received are useful. For example, we agree with the point that instead of "the Internet", we should use the more embracing and neutral term "open network". As regards the spreading of computer viruses and denial of service attacks, they are currently covered by provisions against criminal damage to property, including computers. We agree, however, that consideration may be given to whether the law should be made more explicit in this regard. We also agree that we should ensure that there are sufficient safeguards to prevent criminalizing innocent computer users. It follows that we are not inclined to prohibit port scanning and host scanning, as these activities may well serve legitimate purposes. Nonetheless, we should better clarify to interested parties that attempted hacking is already an offence. As regards hacking tools, while we consider that in general they should not be regulated, this should not preclude additional protection to specific industries against circumvention tools or techniques where justified. On balance, therefore, we accept the thrust of the WG's recommendations on protecting computer data, and will take the comments received into account when drafting the detailed proposals.

(e) Deception of computers

15. Only a few respondents have commented on the issue. They all agree with the WG that the legal concept that only humans may be deceived, and that machines cannot be deceived should be updated to take into account technological developments. We also agree with the WG's proposal that the matter be considered. As with the question of jurisdiction, however, we will task the Department of Justice to undertake the initial legal research in the first instance.

(f) Penalties for offences

16. The WG recommended rationalizing the penalties for various computer related offences. For example, it suggested that the penalty for unauthorized access to the computer should be not less than that for theft (ten years' imprisonment); while that for accessing a computer with criminal and dishonest intent should reflect the different nature of the acts encompassed in the offence. The principle that penalties for cyber crimes should be on par with those for physical crimes of a similar nature is generally accepted by respondents. Many concur that it is necessary to have sufficiently strong deterrents to curb computer crime. At the same time, a few respondents are not convinced that stiff penalties are warranted if no damage was intended or incurred.

17. We agree with the WG that we should avoid sending the wrong message that computer crime is less serious than physical crime. Given the characteristics of computer crime, damage may result even if it was not intended, and the consequences could be very serious. We therefore agree with the WG that a custodial term should be included in the penalty for intentional unauthorized access to the computer. In view of the comments received, and having regard to overseas examples, however, we believe that the penalty does not necessarily have to be pitched at the same level as that for theft. It would also be useful to allow sufficient differentiation between unauthorized access without criminal or dishonest intent and access with such intent. We are therefore inclined to pitch the penalty level at, say, three years, at least initially, for intentional unauthorized access without criminal or dishonest intent.

18. We agree with and accept the WG's proposals regarding the penalty levels for the offence of accessing a computer with criminal and dishonest intent.

(g) Assistance from ISPs

19. The WG proposed various administrative measures to better tap the assistance of ISPs in criminal investigations. These have attracted a number of comments. Many accept that guidelines should be drawn up for ISPs to follow for assisting law enforcement on a need basis, although some query the practical usefulness of such guidelines. The ISP industry has indicated its willingness to cooperate with law enforcement as far as possible. At the same time, it is concerned about the cost of compliance as well as the need to protect privacy. Privacy concerns also feature in many other respondents' comments. In particular, the Privacy Commissioner has provided useful comments on the privacy principles to be observed. There are also a number of comments on the technical details involved in implementing the recommendations. In addition, there is much support for and interest in the proposed forum of exchange between law enforcement and ISPs, with suggestions that the forum should be open to other interested parties as well. Indeed, some point to the important role of other players in the communications chain, for example, web hosting companies, and hence the need to avoid concentrating on ISPs alone.

20. The extent to which ISPs or communications service providers should facilitate computer crime investigation is an extensively discussed and often hotly debated subject overseas. We are therefore encouraged by the generally positive response that we have received. There is little opposition in principle to the WG's proposal that guidelines for cooperation between law enforcement and ISPs should be drawn up. As the WG pointed out, such details as the period for which records should be kept and the types of records that should be kept should be further discussed. These discussions should be geared towards standardizing record keeping practices and the better use of such records, and not towards the keeping of records solely for law enforcement purposes. They should take into consideration, among other things, the cost of compliance, the privacy angle and the views of the stakeholders. As regards the latter, we agree that other players in the communications chain should also be involved, but a balance has to be struck between comprehensiveness and manageability. Subject to these observations, we accept in principle the WG's proposals on assistance from ISPs. The many comments received will be taken into account in drawing up the implementation details.

(h) Protection of critical infrastructures

21. The WG recommended strengthening the ability of our critical infrastructures to withstand and recover from cyber attacks, both individually and collectively. There is almost unanimous support for this principle among respondents who have commented on the subject. We also agree with the WG that there should be an adequate response and recovery mechanism. The WG emphasized that its proposals on this subject should be geared towards increasing coordination and preventing vulnerabilities. Existing resources should be leveraged upon where possible. We agree with this approach. On this basis, the WG's proposals regarding critical infrastructure protection are adopted.

(i) Public education and private sector's role

22. There is a large measure of agreement with the WG's stance that public education is critical to the effort of preventing computer crime and that the private sector has an important role to play in such effort. The WG's recommendations to strengthen public education and increase private sector participation are supported almost unanimously. Indeed, many respondent organizations indicate their willingness to undertake more work and cooperate with Government in this regard. Some respondents point out that Government should take the lead not only with regard to education, but also with regard to setting certification standards.

23. Many of the comments received will be useful in drawing up the implementation details. For example, we will have to see how best to draw on the offer of assistance of organizations such as the Consumer Council and various business associations in raising user awareness of cyber security. We agree with the WG's view that the private sector should take the lead in setting industry-specific information security standards. At the same time, we appreciate the concern that Government may have to play some facilitating role. The WG's proposals are therefore adopted as the framework within which private sector-led efforts are supplemented by support and facilitation measures by the public sector.

(j) Resources and capabilities

24. The WG made various recommendations to ensure an adequate response to computer crime from law enforcement. There is broad agreement on the proposed measures such as increased sharing of intelligence, stepped-up international liaison, and a standard set of

procedures for handling computer evidence. We also agree that the WG's proposals on the subject provide a good basis for future work, and should be adopted.

(k) Future institutional arrangements

25. The WG recommended the establishment of a mechanism to follow up on future work and monitor developments related to computer crime. Specifically, it suggested that a sub-committee under the Fight Crime Committee (FCC) should be set up for the purpose. The concept of a standing mechanism is welcome by many respondents. Indeed, some have asked to be represented on it. However, in general, there is no strong preference on how it should be constituted. The FCC itself does not favour the establishment of a sub-committee under it because the FCC is not an executive committee. Given the complexity of computer crime issues, it considers that the relevant Government bureaux and departments should undertake the necessary follow up and keep the FCC informed of progress and developments from time to time.

26. We respect the FCC's views and will not pursue the FCC sub-committee idea. Given the positive feedback received on the WG's recommendation, however, we will establish a mechanism involving the public and private sectors on computer crime policy matters outside the FCC framework. The mechanism should be geared towards keeping in view overall progress and discussing policy issues, with the executive work undertaken by the relevant Government bureaux and departments.

27. For ease of reference, a summary table setting out our response to the WG's recommendations (paragraphs 8 to 26 above) is at Annex C. C

(C) Implementation Plan

28. Given the large number of recommendations and the varying complexity involved, we will adopt a phased approach in implementing the accepted recommendations. The implementation plan will take into account such factors as the complexity and urgency of the issue as well as the possible need to secure resources for implementation. As a first step, we will start to put in place some of the administrative arrangements and to tackle the relatively straightforward legislative amendments. Issues requiring more research or planning and sustained input will be pursued as the next step, while items calling for more deliberation or study will be pursued in the even longer term. On this basis, a **tentative** implementation plan is at Annex D. The plan is no more than a handy checklist, and is not meant to be a rigid timetable. Indeed, it is likely that the timetable will have to be refined and revised after more detailed proposals for implementing individual recommendations are mapped out. D

29. Successful implementation of the accepted recommendations of the WG requires the contribution from and sustained effort of a number of Government bureaux and departments, relevant public sector bodies as well as the private sector. The proposed standing committee on computer crime (paragraph 26 above) will be well placed to oversee this work and ensure coordination. The formal establishment of such a committee is likely to take some time, however. To maintain the momentum in the interim, we will establish an inter-departmental task force led by Security Bureau to undertake the initial follow up work, especially those tasks earmarked for implementation in the short to medium term.

FINANCIAL AND STAFFING IMPLICATIONS

30. The first stage of implementation will involve the preparation of relatively straightforward draft legislation and laying the groundwork for certain administrative arrangements. The work will be absorbed by existing resources. The financial and staffing implications of other stages of implementation will need to be assessed after the detailed arrangements have been worked out. We will adopt the guiding principle of leveraging on existing resources where practicable. However, it is possible that additional resources may still be required for taking forward some of the recommendations. For example, the

recommendations on protecting our critical infrastructures against cyber attacks will likely carry resource implications, especially at the initial stage of putting in place the mechanism for coordinating vulnerability assessments and preparation of protection and recovery plans. The creation of a standing committee on computer crime policy matters will also likely have recurrent resource implications. We will secure additional resources in the normal manner before implementation of these recommendations if the resource requirements cannot be met by internal redeployment.

ECONOMIC IMPLICATIONS

31. A more secure cyber environment should help enhance Hong Kong's attractiveness as an e-commerce hub. The proposed measures for strengthening information security should therefore have a positive effect on facilitating business and increasing our overall competitiveness.

PUBLIC CONSULTATION

32. The report was released for public consultation from December 2000 to February 2001. During the period, we held a number of briefings for and discussions with various interested parties such as the Legislative Council Panels on Security and on Information Technology and Broadcasting, the FCC, representatives of the District Councils, District FCCs, the information technology industry as well as academics in the field. A summary of these consultation activities is at Annex E. E

PUBLICITY

33. A press release on the Government's decision will be issued on 16 July 2001. A spokesman will be available to answer enquiries.

File Reference : SBCR 14/3231/88 Pt. 21

Subject Officer : Mrs. CHOI WONG Fung-yee, AS(S)F1 (Tel. : 2810 2973)

Security Bureau
16 July 2001

REPORT OF
INTER-DEPARTMENTAL WORKING GROUP ON
COMPUTER RELATED CRIME : ANNEXES

Annex A

List of Respondents

(A) Information Technology Industry, Firms or Representative Associations

(1) Hong Kong Broadband Network Limited

(2) Hong Kong Internet Service Providers Association

(3) Hutchison E-commerce Limited

(4) Hutchison Global Crossing Limited

(5) Hutchison Telephone Company Limited

(6) Pacific Century CyberWorks Limited

(7) Webmaster (Hong Kong) Association

(B) Professional Associations

(8) Hong Kong Computer Society

(9) Hong Kong Information Technology Federation

(10) Hong Kong Society of Accountants and Information Systems Audit and Control Association (Joint Submission)

(11) Information Security and Forensics Society

(12) Institute of Electrical and Electronics Engineers (HK Section) Computer Chapter

(13) The British Computer Society (Hong Kong Section)

(14) The Hong Kong Institution of Engineers

(15) The Law Society of Hong Kong

(C) Business Associations/Other Industries

(16) AXA China Region Insurance Co. Ltd.

(17) Hong Kong General Chamber of Commerce

(18) International Chamber of Commerce – Hong Kong, China Business Council

(19) International Federation of Phonographic Industry (IFPI) (Hong Kong Group) Limited

(20) The Chinese Manufacturers' Association of Hong Kong

(21) The Hong Kong Association of Banks

(D) Other Organizations

(22) Consumer Council

(23) Democratic Alliance for Betterment of Hong Kong

(24) Free Net Hong Kong

(25) Hospital Authority

(26) Law Reform Commission Secretariat

(27) Office of Privacy Commissioner for Personal Data

(28) Sham Shui Po District Fight Crime Committee

(E) Individuals

(29)-(46) 18 individuals, including information technology professionals, academics, etc.

Annex B

Summary of Feedback

The following table provides a statistical summary of the written feedback received on the recommendations of the Inter-departmental Working Group on Computer Related Crime (the Working Group). It is intended to provide no more than a quick reference. The quantitative summary of necessity does not capture the numerous qualitative comments made, or those comments that do not express a relatively clear preference one way or the other.

2. In the following table, each written submission from organizations, irrespective of size or membership, is counted as one. Similarly each submission from individuals is counted as one.

Working Group's Recommendations*		**Agree**	**Disagree**
Definition			
1.	Defining "computer" in law.	7	8
Jurisdiction			
2.	Conducting in-depth study of jurisdictional rules.	7	0
3.	Including specified offences under Criminal Jurisdiction Ordinance.	3	0
Encryption #			
4 – 8.	Mandating disclosure of decrypted text or decryption tool of encoded computer information for investigation, subject to judicial scrutiny and other safeguards.	16	7

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report, a copy of which is enclosed to this annex.

# Two submissions express support for some recommendations, and opposition to others, under this heading. Their categorization has been done on the basis of the relative weight of the support or opposition expressed.

Working Group's Recommendations*		Agree	Disagree
Protection of computer data			
9 – 14, 16.	Improving existing legislative provisions to remove ambiguity, better protect against unauthorized access and prevent trafficking in passwords etc.	10	2
15.	Not legislating against hacking tools.	8	1
Deception of computers			
17.	Rectifying the gap in law regarding "deception" of machines.	4	0
Penalties for offences			
18 – 20.	Rationalizing penalties for specified computer offences.	9	1
Assistance from Internet Service Providers (ISPs) ☆			
21 – 30.	Increasing cooperation with ISPs in combating computer crime on various fronts – drawing up guidelines, setting up contact point system, exploring feasibility of take-down procedures etc.	14	4
Protection of Critical Infrastructures			
31 – 36.	Conducting risk and vulnerability assessments, strengthening coordination in protection and recovery plans, and improving emergency response capability.	13	0

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report, a copy of which is enclosed to this annex.

☆ Four submissions express support for some recommendations, and opposition to others, under this heading. Their categorization has been done on the basis of the relative weight of the support or opposition expressed.

Annex B

Working Group’s Recommendations*		**Agree**	**Disagree**
Public education			
37.	Introducing mechanism for information sharing, facilitating cross-agency participation, mapping out overall public sector education strategy on computer crime.	13	0
The private sector’s role			
38 – 43.	Increasing private sector participation and involvement in education, information sharing and policy formulation.	7	0
44.	Exploring feasibility of audit mechanism to certify information security standards.	11	0
Resources and Capabilities			
45 – 50.	Ensuring sufficient resources and capability to deal with computer crime.	8	0
51 – 52.	Working out standard procedures for handling computer evidence and promulgating them.	5	0
53.	Establishing central computer forensic examination unit in the long run.	4	0
Future Institutional Arrangements			
54 – 55.	Setting up a committee on computer crime with representatives from law enforcement and private sector.	9	0
General			
56 – 57.	Ensuring that new or amendment legislation is technology and medium neutral, ensuring sufficient consultation with interested parties.	3	0

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group’s report, a copy of which is enclosed to this annex.

Enclosure to Annex B

Summary of Recommendations

The recommendations of the Working Group are summarized below.

Defining "Computer" in Law

1. There is merit in setting out in our law some parameters within which the concept of "computer" should be interpreted. The term "information system" as defined in the Electronic Transactions Ordinance (Cap. 553) should be used in place of the term "computer" (paragraph 3.9). In principle, to ensure consistency, this amendment should apply across the board to all references to the term "computer" in our legislation (paragraph 3.10).

Jurisdiction

2. Consideration should be given to conducting a thorough in-depth study of the subject of jurisdictional rules in general to take account of the greatly increased ease of transportation and communications (paragraph 4.10).

3. The following offences, as modified to take into account the recommendations in this Report, should be covered by the Criminal Jurisdiction Ordinance (Cap. 461) –

   – unauthorized access to computer by telecommunication (S. 27A, Telecommunications Ordinance (Cap. 106)); and

   – access to computer with a criminal or dishonest intent (S. 161, Crimes Ordinance (Cap. 200))

   (paragraphs 4.15 and 4.17).

Encryption

4. Legislation should be introduced to enable law enforcement agencies to be provided with the decryption tool or the decrypted text of encoded computer records where necessary and justified (paragraph 5.14).

5. The compulsory disclosure requirement should be subject to judicial scrutiny (paragraph 5.18). A process similar to that for applying for "production orders" under Section 4 of the Organized and Serious Crimes Ordinance (Cap. 455) should be adopted for the purpose (paragraph 5.22).

6. The disclosure power should apply to offences of a more serious nature. Only offences attracting a maximum penalty on conviction of not less than, say, two years' imprisonment should be subject to the disclosure requirement (paragraph 5.25).

7. There should be suitable legal protection of the confidentiality of the information obtained through the disclosure procedures. The evidence obtained as a result of compulsory disclosure should be admissible in court (paragraph 5.26).

8. The penalties for non-compliance with the disclosure requirement should in principle be commensurate with those for the specific offence under investigation (paragraph 5.27).

Protection of Computer Data

9. Existing legislative provisions on unauthorized access to the computer, while covering much of what needs to be protected in terms of computer data, should be further improved (paragraphs 6.18 and 6.19).

10. All computer data at all stages of storage or transmission via a computer or the Internet should be covered (paragraph 6.19).

11. The term "access to computer" should be clarified to include access to a computer as well as the programs and data stored therein (paragraph 6.19).

12. Unauthorized access to the computer by any means instead of by telecommunication only should be unlawful (paragraph 6. 19).

13. Receiving, retaining and handling/trafficking of computer data known to have been obtained through unauthorized access to the computer should be prohibited (paragraph 6.19).

14. It should be illegal to sell, distribute and make available any computer password or access code for wrongful gain for oneself or another, an unlawful purpose or causing wrongful loss to another (paragraph 6.19).

15. It is unnecessary and impracticable to legislate against hacking tools. The proposal should not be pursued (paragraph 6.23).

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

16. It is necessary for any anomalous situation between the treatment of computer data and physical data to be studied and rectified as appropriate (paragraph 6.25).

"Deception" of Computers

17. Existing legislation is adequate to deal with "deceptions" of computers (paragraph 7.9). However, consideration should be given to studying and rectifying the gap in our law where at present the "deception" of a machine other than a computer is not an offence (paragraph 7.10).

Penalties for Offences

18. The penalty for unauthorized access to the computer should include a custodial term. A sufficient deterrent should not be less than that for theft (paragraphs 2.7 and 6.22).

19. The current penalty of 5 years' imprisonment for accessing a computer with the intent to commit an offence, S. 161(1)(a) of the Crimes Ordinance (Cap. 200), should be amended, to the effect that it should be decided having regard to the severity of the offence to be committed (paragraph 4.16).

20. The current penalty of 5 years' imprisonment for the deception and dishonest intent parts of S. 161 of the Crimes Ordinance (Cap. 200) (i.e. S. 161(b), (c) and (d)) should be amended, so that the maximum sentence will not be less than 10 years (paragraph 7.11).

Assistance from Internet Service Providers (ISPs)

21. The existing practice of tracing the transactions of specific accounts suspected of involvement in computer crime on a need basis only should continue (paragraph 8.22).

22. ISPs should be encouraged to keep log records including the calling numbers as a good management practice. However, the proposal to impose a mandatory requirement for all Internet transactions to be tracked by the caller line identification function or caller number display function should be put on hold (paragraph 8.22).

23. Administrative guidelines on record-keeping by ISPs should be drawn up to cover, among others –

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

- subscriber details to be inspected on opening of an account and those which should be kept;

- details to be captured by log records – these should include at least the time of logging in and logging out as well as the Internet protocol address assigned for an Internet transaction, and preferably the caller number; and

- the period for which records should be kept – say, six months,

to facilitate computer crime investigation (paragraphs 8.16, 8.24 and 8.26).

24. The guidelines should be drawn up in consultation with ISPs (paragraph 8.26.)

25. The guidelines should be given suitable publicity. Consumers should be encouraged to choose ISPs who adopt the good management practices set out in these guidelines (paragraph 8.27).

26. Internet users should be encouraged to make use of the Public Key Infrastructure for enhanced security, although the requirement should not be made mandatory (paragraph 8.23).

27. In principle, take-down procedures for ISPs to remove offending materials should be endorsed. The relevant Policy Bureaux should examine the feasibility of putting in place such procedures in respect of copyright protection, Internet gambling and pornographic materials (paragraph 8.30).

28. ISPs should be encouraged to set their system default to deny multiple log-in, and instead offer the facility only as an option (paragraph 8.31).

29. The market-led approach for dealing with credit limits for on-line shopping should continue. There is no need for legislation to require ISPs to set limits on credit card payment transactions through the Internet (paragraph 8.32).

30. Communication between law enforcement agencies and ISPs should be enhanced by –

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

- establishing a forum of exchange for both sides to discuss matters of mutual concern at the macro level at regular intervals; and

- setting up a contact point system for ISPs and law enforcement agencies for dealing with computer crime investigation requests (paragraph 8.33).

Protection of Critical Infrastructures

31. A thorough risk assessment of our critical infrastructures vis-à-vis cyber attacks should be undertaken (paragraph 9.16).

32. A standing central mechanism capable of coordinating the preparation and synchronization of protection, contingency and recovery plans against computer and Internet-related security threats to our critical infrastructures should be established (paragraph 9.17). The emphasis of this mechanism should be on better coordination across the board in terms of threat and vulnerability assessment, and preparation and regular updating of protection, contingency and recovery plans, both individually and collectively (paragraph 9.18).

33. The Emergency Response System exercises mounted by the Government should include scenarios of cyber attacks to our critical infrastructures (paragraph 9.17).

34. From the point of view of law enforcement facilitation, the setting up of a computer emergency response team (CERT) is supported (paragraph 9.21).

35. Our critical infrastructure operators should be covered by the CERT if and when it is set up (paragraph 9.22).

36. Pending the establishment of the CERT, liaison has to be increased between the Information Technology Services Department and critical infrastructure operators to enable the prompt sharing of information to better deal with emergency situations (paragraph 9.22).

Public Education

37. There should be a mechanism involving all Government departments and other public sector organizations which are currently engaged in education or publicity efforts on information security to –

    - provide a common forum for sharing information;

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group’s report.

- facilitate cross-agency participation in and contribution to each other's programs;

- serve as the focal point for mapping out the public sector's overall education and publicity strategy on information security; and

- coordinate the mobilization and involvement of the private sector in public sector-led programs on information security, and vice versa

(paragraph 10.7).

The Private Sector's Role

38. The market-led approach in developing information security devices or programs should continue (paragraph 11.5).

39. The law enforcement agencies should share with the relevant industries information obtained from computer crime investigation on how security has been breached. The private sector should keep the law enforcement agencies abreast of trends and developments in information security and share their security concerns (paragraph 11.6).

40. The private sector itself should organize information sharing initiatives on information security issues (paragraph 11.6).

41. The private sector, in particular, professional organizations, industry associations and chambers of commerce, should be encouraged to undertake more education and publicity efforts on information security at various levels (paragraphs 11.7 and 11.8).

42. Government and public sector agencies should lend as much support to private sector-led publicity and education initiatives on information security as possible. Similarly, they should actively involve the private sector in their own education efforts (paragraph 11.9).

43. The Government should continue to involve the private sector in the formulation of policies on computer crime and seek its input on a more regular basis (paragraphs 11.10 and 11.11).

44. The feasibility of a commonly accepted audit or assessment mechanism to certify the information security standards for different industries and at different levels should be explored (paragraph 11.12).

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Resources and Capabilities

45. Sufficient resources should be provided for the effort to combat and prevent computer crime (paragraph 12.17).

46. The law enforcement agencies should continue to closely monitor the availability of computer crime investigation and computer forensic examination expertise to ensure that there is no mismatch between demand and supply. Private sector resources and cooperation should be leveraged on as far as possible (paragraph 12.18).

47. The proposal for pooling all law enforcement resources in respect of computer crime to form a central one-stop unit should not be pursued (paragraph 12.19).

48. The cooperation and sharing of intelligence and experience between the law enforcement agencies should continue and be deepened (paragraph 12.20)

49. The law enforcement agencies should step up their liaison with their counterparts outside Hong Kong (paragraph 12.21).

50. Our law enforcement agencies should keep close tabs on international developments regarding procedures for handling computer evidence to ensure that Hong Kong's procedures are in line with the international standards once they are available (paragraph 12.22).

51. A standard set of procedures for handling computer evidence among all law enforcement agencies in Hong Kong should be worked out as soon as possible. The soon to-be-established Police Computer Forensic Laboratory should take the lead in developing this common standard (paragraph 12.23).

52. Once the common standard for handling computer evidence is developed, it should be publicized among judges, the legal profession and other interested parties (paragraph 12.23).

53. In the longer run, consideration should be given to establishing a computer forensic examination unit or laboratory to provide computer forensic service centrally (paragraph 12.24).

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Future Institutional Arrangements

54. A sub-committee under the Fight Crime Committee should be formed to follow up on the Working Group's proposals, monitor relevant developments as they evolve and assess their impact on our policies and measures (paragraph 13.8).

55. The sub-committee should include, among others, senior representatives of law enforcement agencies and some private sector representation (paragraph 13.9).

Others

56. In general, new legislation or amendments to existing legislation should be drawn taking into account the requirements of the information age. As far as possible, legislation should be technology- and medium-neutral (paragraph 14.4).

57. To maximize public acceptance and cooperation, interested parties should be consulted when details of implementing the Working Group's recommendations are being mapped out (paragraph 14.5).

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Annex C

Summary of Government’s Response

Working Group’s Recommendations*		Government’s Response
Definition		
1.	Defining “computer” in law.	Accept.
Jurisdiction		
2.	Conducting in-depth study of jurisdictional rules.	Accept in principle. Initial legal research to be conducted by Department of Justice.
3.	Including specified offences under Criminal Jurisdiction Ordinance.	Accept.
Encryption		
4 – 8.	Mandating disclosure of decrypted text or decryption tool of encoded computer information for investigation, subject to judicial scrutiny and other safeguards.	Accept as framework. Work out proposed implementation details and further consult before draft legislation is prepared.
Protection of computer data		
9 – 14, 16.	Improving existing legislative provisions to remove ambiguity, better protect against unauthorized access and prevent trafficking in passwords etc.	Accept in principle. Take into account comments in submissions in drawing up details.
15.	Not legislating against hacking tools.	Accept.
Deception of computers		
17.	Rectifying the gap in law regarding “deception” of machines.	Accept in principle. Initial legal research to be conducted by Department of Justice

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group’s report.

Annex C

	Working Group's Recommendations*	Government's Response
Penalties for offences		
18 – 20.	Rationalizing penalties for specified computer offences.	Pitch penalty for unauthorized access without criminal or dishonest intent at lower level, say, three years' imprisonment. Otherwise accept.
Assistance from Internet Service Providers (ISPs)		
21 – 30.	Increasing cooperation with ISPs in combating computer crime on various fronts – drawing up guidelines, setting up contact point system, exploring feasibility of take-down procedures etc.	Accept in principle. Involve various stakeholders in addition to ISPs, and address privacy and cost of compliance issues.
Protection of Critical Infrastructures		
31 – 36.	Conducting risk and vulnerability assessments, strengthening coordination in protection and recovery plans, and improving emergency response capability.	Accept.
Public education		
37.	Introducing mechanism for information sharing, facilitating cross-agency participation, mapping out overall public sector education strategy on computer crime.	Accept.

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Annex C

Working Group’s Recommendations*		**Government’s Response**
The private sector’s role		
38 – 43.	Increasing private sector participation and involvement in education, information sharing and policy formulation.	Accept as framework.
44.	Exploring feasibility of audit mechanism to certify information security standards.	Accept. Private sector to take the lead in setting industry-specific standards. Public sector to facilitate and support.
Resources and Capabilities		
45 – 50.	Ensuring sufficient resources and capability to deal with computer crime.	Accept.
51 – 52.	Working out standard procedures for handling computer evidence and promulgating them.	Accept.
53.	Establishing central computer forensic examination unit in the long run.	Accept.
Future Institutional Arrangements		
54 – 55.	Setting up a committee on computer crime with representatives from law enforcement and private sector.	Not pursue Fight Crime Committee sub-committee idea. Set up separate mechanism on computer crime policy issues.
General		
56 – 57.	Ensuring that new or amendment legislation is technology and medium neutral, ensuring sufficient consultation with interested parties.	Accept.

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group’s report.

Annex D

Tentative Implementation Plan

Working Group's Recommendations*		Action
(A)	**Short term**	
28.	Promoting the denial of multiple log-in.	Write to ISPs for cooperation. Promote consumer awareness in this regard.
30.	Increasing communication between law enforcement and ISPs.	Establish forum for exchange between law enforcement and communication service providers.
39.	Stepping up information sharing between law enforcement and private sector.	Include requirement in law enforcement agencies' standard procedures. Invite ideas from private sector on possible additional measures to foster information sharing.
48 – 49.	Continuing and deepening inter-agency cooperation locally and internationally.	Draw up standard procedures to facilitate cooperation and information sharing.
(B)	**Short to medium term**	
1.	Defining "computer" in law.	Prepare draft legislation.
3.	Including specified offences under Criminal Jurisdiction Ordinance.	Prepare draft legislation.

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Annex D

	Working Group's Recommendations*	**Action**
9 – 14, 16.	Improving existing legislative provisions to remove ambiguity, better protect against unauthorized access and prevent trafficking in passwords etc.	Prepare draft legislation.
18 – 20.	Rationalizing penalties for specified computer offences.	Prepare draft legislation.
22 – 25.	Drawing up administrative guidelines on record keeping.	Set up forum for drawing up administrative guidelines. Publicize guidelines when available.
31.	Undertaking thorough risk assessment of critical infrastructures.	Identify critical infrastructures to be covered, draw up steps for conducting the risk assessment.
37.	Introducing mechanism for information sharing, facilitating cross-agency participation, mapping out overall public sector education strategy on computer crime.	Draw up functions, structure and mode of operation of mechanism.
40 – 43.	Encouraging private sector to share information and undertake education efforts; increasing public-private sector collaboration.	Include message in Government publicity programs, probably in conjunction with item 37. Invite major professional organizations and business associations to contribute.
54 – 55.	Setting up a committee on computer crime with representatives from law enforcement and private sector.	Draw up options in respect of proposed functions, structure and mode of operation of mechanism outside of Fight Crime Committee, and examine their relative merits.

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Working Group's Recommendations*		**Action**
(C)	**Medium term**	
27.	Exploring feasibility of take-down procedures.	Examine and, if feasible, adopt in individual policy context.
31.	Undertaking thorough risk assessment of critical infrastructures.	Conduct assessment.
32 – 33.	Establishing mechanism to coordinate preparation and synchronization of protection and recovery plans; including cyber attacks on critical infrastructures in Emergency Response System (ERS).	Having regard to results from item 31, draw up functions, structure and mode of operation of mechanism, and determine relationship between mechanism and ERS.
44.	Exploring feasibility of audit mechanism to certify information security standards.	Invite major professional organizations and business associations to take the lead in setting industry-specific standards. To facilitate and support as necessary.
50 – 52.	Working out standard procedures for handling computer evidence and promulgating them.	Develop common standard. Promulgate standard once available.
54 – 55.	Setting up a committee on computer crime with representatives from law enforcement and private sector.	In light of findings under (B) for these items, set up committee.
(D)	**Medium to long term**	
4 – 8.	Mandating disclosure of decrypted text or decryption tool of encoded computer information for investigation, subject to judicial scrutiny and other safeguards.	Work out proposed implementation details and further consult before draft legislation is prepared.

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Annex D

Working Group’s Recommendations*	Action
(E) Long term	
2. Conducting in-depth study of jurisdictional rules.	Conduct study on legal issues involved.
17. Rectifying the gap in law regarding “deception” of machines.	Conduct study on legal issues involved.
53. Establishing central computer forensic examination unit in the long run.	Consider merging existing computer forensic capabilities among law enforcement agencies.
(F) On-going efforts or no specific action required	
15. Not legislating against hacking tools.	Already the case.
21. Continuing practice of tracing transactions on need basis.	Already the case.
26. Encouraging use of Public Key Infrastructure.	Continue with current effort.
29. Not legislating on credit card payment transactions through the Internet.	Already the case.
34. Setting up a computer emergency response team (CERT).	A Computer Emergency Response Centre (CERC) has been established with Government funding support under the Hong Kong Productivity Council (HKPC).
35. CERT covering critical infrastructures.	The CERC of the HKPC already provides free alerts to interested organizations. Ensure that critical infrastructures are on the CERC’s alert list when list of critical infrastructures is agreed.

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group’s report.

Annex D

Working Group’s Recommendations*		**Action**
36.	Increasing liaison between Information Technology Services Department and critical infrastructure operators pending establishment of CERT.	A CERC has already been established with Government funding support under the HKPC.
38.	Continuing with market-led approach in developing information security devices.	Already the case.
45 – 46.	Providing sufficient resources and ensuring adequate expertise to combat and prevent computer crime.	On-going effort.
47.	Not pursuing central one-stop unit proposal.	No further action required.
56 – 57.	Ensuring that new or amendment legislation is technology and medium neutral, consultation with interested parties.	Take into account as appropriate.

[LC1002D.DOC]

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group’s report.

Summary of Consultation Activities

(A) Briefings and/or briefing papers

(1) Chambers of commerce and business associations

(2) Copyright industry associations

(3) District Councils

(4) District Fight Crime Committees

(5) Fight Crime Committee

(6) Information Infrastructure Advisory Committee

(7) Information security professional associations

(8) Information technology industry associations

(9) Interested individuals

(10) Legislative Council Panel on Security and Panel on Information Technology and Broadcasting

(11) Major infrastructure operators

(12) Media representatives

(13) Professional associations such as the Law Society, Society of Accountants and Information Systems Audit and Control Association

(14) Relevant public bodies such as the Consumer Council, Productivity Council and Trade Development Council

(15) Tertiary education institutes, including departments of computer science, information systems and engineering

(16) Trade and Industry Advisory Board

(B) Direct mailing (by post or e-mail)

(1) Chambers of commerce and business associations

(2) Copyright industry associations

(3) Information security professional associations

(4) Information technology industry associations

(5) Interested individuals

(6) Major infrastructure operators

(7) Professional associations such as the Law Society, Society of Accountants and Information Systems Audit and Control Association

(8) Relevant public bodies such as the Office of Privacy Commissioner for Personal Data and Trade Development Council

(9) Tertiary education institutes, including departments of computer science, information systems and engineering

(C) Briefing-cum-discussion forums

(1) Chambers of commerce and business associations

(2) Copyright industry associations

(3) Information security professional associations

(4) Information technology industry associations

(5) Interested individuals

(6) Major infrastructure operators

(7) Professional associations such as the Hong Kong Computer Society, Information Security and Forensics Society and the Hong Kong Information Technology Federation

(8) Relevant public bodies such as the Consumer Council and Productivity Council

(9) Tertiary education institutes, including departments of computer science, information systems and engineering

(D) Publicity targeted at the general public

(1) Announcements of public interest on radio and television

(2) Hard copies of report for distribution at all District Offices

(3) Press announcement on release of report

(4) Soft copies of report for viewing or downloading at the Security Bureau and Government Information Centre websites