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

Purpose

This paper provides further information on the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 (the draft Order) in respect of the issues raised at the Subcommittee meeting on 8 January 2003.

Computer offences proposed to be added and examples

2. The draft Order seeks to add the following three computer offences to the list of offences in section 2(2) of the Criminal Jurisdiction Ordinance (the Ordinance) (Cap. 461) -

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

(b) "destroying or damaging property" relating to the misuse of a computer under sections 59 and 60 of the Crimes Ordinance (Cap. 200); and

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

The intention is to deal with some "pure" or direct" trans-border offences of interference with computers, in the sense that the computers are the main subject of, and not merely incidental to, the offences.

"Unauthorized access to computer by telecommunications"

3. Section 27A of the Telecommunications Ordinance states that "any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence". Hacking, for example, is an offence under this section.

"Destroying or damaging property" relating to the misuse of a computer

4. Section 60 of the Crimes Ordinance states that "a person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence". Section 59 specifies that "'to destroy or damage any property' in relation to a computer includes the misuse of a computer", and "'misuse of a computer' means -

(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner; notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
(b) to alter or erase any program or data held in a computer or in a computer storage medium;
(c) to add any program or data to the contents of a computer or of a computer storage medium,

and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it".

5. For example, if a person "spams" (sends the same message indiscriminately) a computer causing it to cease functioning, that person commits an offence under sections 59 and 60.

"Access to computer with criminal or dishonest intent"

6. Section 161 of the Crimes Ordinance states that "any person who obtains access to a computer -

(a) with intent to commit an offence;
(b) with a dishonest intent to deceive;
(c) with a view to dishonest gain for himself or another; or
(d) with a dishonest intent to cause loss to another,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence".

7. For example, if a person hacks into a company's computer to obtain some commercially sensitive information and forward such information to the company's competitor for a monetary reward, that person commits an offence under section 161.

8. It can be noted that subject to the elements involved in the act committed, a computer offence may be caught by more than one of the above three offences, in which case the prosecution will decide on the appropriate

proceedings to be initiated having regard to the circumstances pertaining to each individual case.

Justification for adding references to the three offences to the Criminal Jurisdiction Ordinance

Traditional jurisdictional rules

9. In the physical world, the perpetrator of a crime is usually present at or near the scene of crime. Therefore, traditionally the concept of jurisdiction is closely associated with geographical boundaries. The jurisdiction of the court is limited to acts done within the geographical boundaries of a country or territory unless otherwise specified. At common law, an offence is regarded as being committed where the last act or event necessary for its completion took place, and jurisdiction is exercised where the offence is committed. An example is provided in paragraph 10 below to illustrate the operation of traditional jurisdictional rules.

10. If a person in Hong Kong spreads computer viruses causing computers **within** Hong Kong to cease functioning, that person commits an offence and is triable in Hong Kong courts. However, if that person spreads computer viruses causing only computers **outside** Hong Kong to cease functioning, he/she is not regarded as having committed an offence in Hong Kong as the last act for the completion of the offence takes place outside Hong Kong, and Hong Kong courts cannot exercise jurisdiction over him/her.

The Criminal Jurisdiction Ordinance

11. The advent of communications has bred cross-border offences together with the jurisdictional problem associated with such offences which involve transactions and events having taken place in more than one jurisdiction. In this regard, the Criminal Jurisdiction Ordinance was enacted in 1994 to deal with international fraud, enabling Hong Kong courts to exercise jurisdiction over offences of fraud and dishonesty -

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

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

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

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

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

12. In simple words, if a person in Hong Kong perpetrates a crime outside Hong Kong, or if a person outside Hong Kong perpetrates a crime in Hong Kong, that person is triable in Hong Kong courts.

Adding references to the three computer offences to the Ordinance

13. Many computer offences are trans-border in nature but are currently not covered by the Ordinance. Taking the example quoted in paragraph 10 above, under traditional jurisdictional rules, the offenders are not triable in Hong Kong even if they are present within the Hong Kong territories. These loopholes should be plugged early to improve the legislative regime for tackling computer crime and to avoid exploitation by computer criminals.

14. To address the issue, we have accepted the recommendation of the Inter-departmental Working Group on Computer Related Crime (the Working Group) that the coverage of the Ordinance should be expanded to the offences of "unauthorized access to computer by telecommunications" and "access to computer with criminal or dishonest intent" as set out in paragraphs 2(a) and (c) above respectively. We have further considered it necessary to include the offence of "destroying or damaging property" relating to the misuse of a computer as mentioned in paragraph 2(b) above, as some computer offences may not involve dishonesty and would fall outside the scope of the two offences in paragraphs 2(a) and (c). The example quoted in paragraph 5 above is a case in point.

Operation of the Criminal Jurisdiction Ordinance in respect of the three offences

15. The addition of the references to the three offences to the Ordinance will enable Hong Kong courts to exercise jurisdiction over the interference with

computer offences, when these offences are committed or planned outside the geographical boundaries of Hong Kong but are connected to or intended to cause damage in Hong Kong. In other words, the offences will be triable in Hong Kong if either the person who obtained access to the computer or the computer to which access was obtained is in Hong Kong. Referring back to the example in paragraph 10 above where a person in Hong Kong spreads computer viruses causing computers outside Hong Kong to cease functioning, he will be regarded as having committed an offence upon addition of the three computer offences to the Ordinance and will be triable in Hong Kong.

Legislation in other jurisdictions and international developments

16. Many other jurisdictions have recognized the jurisdictional problem associated with computer crime. For example, the Computer Misuse Act 1990 of the United Kingdom (sections 4 to 9) provides that the courts have jurisdiction over offences covered by the Act if either the victim or perpetrator of the crime is in the United Kingdom. The offences include unauthorized access to computer program or data, unauthorized access with intent to commit or facilitate the commission of a further offence and unauthorized modification of any computer contents. A copy of the Act is at **Annex A**.

17. Similarly, the Computer Misuse Act of Singapore (section 11) allows prosecution for computer related offences committed within or outside Singapore, when the offender was in Singapore at the material time; or the computer, program or data was in Singapore at the material time. The offences include unauthorized access to computer material; access with intent to commit or facilitate the commission of a further offence; unauthorized modification of computer material; unauthorized use or interception of computer service; unauthorized obstruction of use of computer; and unauthorized disclosure of access code. A copy of the Act is at **Annex B**.

18. In Australia, the Criminal Code Act 1995 as amended by the Cybercrime Act 2001 (sections 15.1 and 476.3) extends jurisdiction over computer offences where the conduct constituting the offence occurs wholly or partly in Australia or on board an Australian ship or aircraft, or where the result of the conduct constituting the offence occurs wholly or partly in Australia or on board an Australian ship or aircraft, or the person committing the offence is an Australian citizen or an Australian company. This means that regardless of where a conduct constituting an offence occurs, if the results of that conduct affect Australia the person responsible would generally be liable to prosecution in Australia. The offences include unauthorized access and modification of computer data or impairment of electronic communication to/from a computer

with intent to commit a serious offence; unauthorized modification of computer data to cause impairment; unauthorized impairment of electronic communication to/from a computer; unauthorized access to, or modification of, restricted computer data; unauthorized impairment of data held in a computer disk etc; possession or control of data with intent to commit a computer offence; and producing, supplying or obtaining data with intent to commit a computer offence. Relevant extracts of the Act are at **Annex C**.

19. In the United States, Code Title 18 (section 1030(e)(2)) as amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act 2001 (section 814(d)) defines "protected computer"[note] to include a computer outside the United States. Thus the definition of a protected computer includes government computers, financial institution computers and any computer which is used in United States interstate or foreign commerce or communication. This broad definition includes nearly all networked computers around the world. Jurisdiction can thus be exercised over computer offences in which the offender is in the United States or the protected computer is in the United States. The offences include intentional access of a computer to obtain information from any protected computer involved in interstate or foreign communication without authorization or in excess of authorization; access of a protected computer without authorization or in excess of authorization with the intent to defraud; knowingly causing the transmission of a program, information, code, or command and as a result of such conduct, intentionally causing damage without authorization, to a protected computer; intentional access to a protected computer without authorization, and as result of such conduct, causing damage; and transmission of communication containing any threat to cause damage to a protected computer. Relevant extracts of section 1030 of the United States Code Title 18 and the USA PATRIOT Act 2001 amending section 1030 are at **Annex D**.

[note] A "protected computer" defined under section 1030(e) as amended by the USA PATRIOT Act 2001 means a computer –

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offence affects the use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

20. The Convention on Cybercrime, concluded by the Council of Europe in November 2001, requires each State Party to establish jurisdiction over computer offences when they are committed in its territory, or on board a ship flying its flag, or on board an aircraft registered under its law, or by its nationals if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. The relevant extract of the Convention is at **Annex E**. In October 2002, the APEC Leaders made the Statement on Fighting Terrorism and Promoting Growth, stating their commitment to endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that is consistent with the provisions of international legal instruments, including the Convention on Cybercrime. A copy of the Statement is at **Annex F**.

21. Following the examples quoted in the preceding paragraphs, the proposed draft Order for establishing extra-territorial jurisdiction over specified computer offences is consistent with international practices.

Number of reported cases

22. In 2002, we received three cases from overseas law enforcement agencies in which our assistance is requested for investigation purposes. The matters under investigation included the spreading of computer viruses, obstruction of transmission of messages and hacking originating from computers situated in Hong Kong. During the same period, we also requested assistance from overseas law enforcement agencies for investigation into 11 cases which mainly involved damage of webpages and hacking originating from computers outside of Hong Kong.

General review of jurisdictional rules

23. The Working Group recommended that consideration be given to conducting a further study of the subject of jurisdictional rules in general. As the Working Group acknowledged, the Ordinance is meant to provide exception to the normal jurisdictional rules under the common law. The present approach of the Ordinance is to specify each offence to be covered by it. Any attempt to cover in effect almost all criminal offences would be changing the ambit of the Ordinance fundamentally. It is considered not necessary at the moment to undertake a revision of the jurisdictional rules of the criminal law.

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

24. Clause 11 of the National Security (Legislative Provisions) Bill amends section 18 of the Official Secrets Ordinance (Cap. 521), adding a new subsection (5A). The new subsection (5A) provides that a person has "illegal access" to information if such information comes into his possession by virtue of any six offences specified. Section 27A (unauthorized access to computer by telecommunications) of the Telecommunications Ordinance and section 161 (access to computer with criminal or dishonest intent) of the Crimes Ordinance are among the six offences specified. The relevant extract of clause 11 of the Bill is at **Annex G**.

Advice sought

25. Members are invited to note this paper.

Security Bureau
February 2003

Annex A

Computer Misuse Act 1990 (c. 18)

1990 c. 18 - *continued*

back to previous page

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

[29th June 1990]

Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Computer misuse offences

Unauthorised access to computer material.

1.—(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

Unauthorised access with intent to commit or facilitate commission of further offences.

2.—(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Unauthorised modification of computer material.

3.—(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Jurisdiction

Territorial scope of offences under this Act.

4.—(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1 or 3 above—

(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or

(b) whether the accused was in the home country concerned at the time of any such act or event.

(2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.

(4) Subject to section 8 below, where—

(a) any such link does in fact exist in the case of an offence under section 1 above; and

(b) commission of that offence is alleged in proceedings for an offence under section 2 above;

section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.

(5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.

(6) References in this Act to the home country concerned are references—

(a) in the application of this Act to England and Wales, to England and Wales;

(b) in the application of this Act to Scotland, to Scotland; and

(c) in the application of this Act to Northern Ireland, to Northern Ireland.

Significant links with domestic jurisdiction.

5.—(1) The following provisions of this section apply for the interpretation of section 4 above.

(2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function; or

(b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the home country concerned at that time.

(3) In relation to an offence under section 3, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the act which caused the unauthorised modification; or

(b) that the unauthorised modification took place in the home country concerned.

Territorial scope of inchoate offences related to offences under this Act.

6.—(1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's guilt—

(a) the question where any person became a party to the conspiracy; and

(b) the question whether any act, omission or other event occurred in the home country concerned.

(2) On a charge of attempting to commit an offence under section 3 above the following questions are immaterial to the accused's guilt—

(a) the question where the attempt was made; and

(b) the question whether it had an effect in the home country concerned.

(3) On a charge of incitement to commit an offence under this Act the question where the incitement took place is immaterial to the accused's guilt.

(4) This section does not extend to Scotland.

Territorial scope of inchoate offences related to offences under external law corresponding to offences under this Act.

7.—(1) The following subsections shall be inserted after subsection (1) of section 1 of the [1977 c. 45.] Criminal Law Act 1977—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an agreement, this Part of this Act has effect in relation to it as it has effect in relation to an agreement falling within subsection (1) above.

(1B) Subsection (1A) above applies to an agreement if—

(a) a party to it, or a party's agent, did anything in England and Wales in relation to it before its formation; or

(b) a party to it became a party in England and Wales (by joining it either in person or through an agent); or

(c) a party to it, or a party's agent, did or omitted anything in England and Wales in pursuance of it;

and the agreement would fall within subsection (1) above as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in England and Wales if committed in accordance with the parties' intentions."

.

(2) The following subsections shall be inserted after subsection (4) of that section—

"(5) In the application of this Part of this Act to an agreement to which subsection (1A) above applies any reference to an offence shall be read as a reference to what would be the computer misuse offence in question but for the fact that it is not an offence triable in England and Wales.

(6) In this section "computer misuse offence" means an offence under the Computer Misuse Act 1990."

.

(3) The following subsections shall be inserted after section 1(1) of the [1981 c. 47.] Criminal Attempts Act 1981—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an act, what the person doing it had in view shall be treated as an offence to which this section applies.

(1B) Subsection (1A) above applies to an act if—

(a) it is done in England and Wales; and

(b) it would fall within subsection (1) above as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in England and Wales.

"

.

(4) Subject to section 8 below, if any act done by a person in England and Wales would amount to the offence of incitement to commit an offence under this Act but for the fact that what he had in view would not be an offence triable in England and Wales—

(a) what he had in view shall be treated as an offence under this Act for the purposes of any charge of incitement brought in respect of that act; and

(b) any such charge shall accordingly be triable in England and Wales.

Relevance of external law.

8.—(1) A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or

facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(2) A person is guilty of an offence triable by virtue of section 1(1A) of the [1977 c. 45.] Criminal Law Act 1977 only if the pursuit of the agreed course of conduct would at some stage involve—

(a) an act or omission by one or more of the parties; or

(b) the happening of some other event;

constituting an offence under the law in force where the act, omission or other event was intended to take place.

(3) A person is guilty of an offence triable by virtue of section 1(1A) of the [1981 c. 47.] Criminal Attempts Act 1981 or by virtue of section 7(4) above only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(4) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.

(5) Subject to subsection (7) below, a condition specified in any of subsections (1) to (3) above shall be taken to be satisfied unless not later than rules of court may provide the defence serve on the prosecution a notice—

(a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;

(b) showing their grounds for that opinion; and

(c) requiring the prosecution to show that it is satisfied.

(6) In subsection (5) above "the relevant conduct" means—

(a) where the condition in subsection (1) above is in question, what the accused intended to do or facilitate;

(b) where the condition in subsection (2) above is in question, the agreed course of conduct; and

(c) where the condition in subsection (3) above is in question, what the accused had in view.

(7) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above.

(8) If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition is satisfied, it shall be competent for the prosecution for that purpose to examine any witness or to put in evidence any production not included in the lists lodged by it.

(9) In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone.

(10) In the High Court of Justiciary and in the sheriff court the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.

British citizenship immaterial.

9.—(1) In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.

(2) This section applies to the following offences—

(a) any offence under this Act;

(b) conspiracy to commit an offence under this Act;

(c) any attempt to commit an offence under section 3 above; and

(d) incitement to commit an offence under this Act.

Miscellaneous and general

Saving for certain law enforcement powers.

10. Section 1(1) above has effect without prejudice to the operation—

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and

(b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure.

Proceedings for offences under section 1.

11.—(1) A magistrates' court shall have jurisdiction to try an offence under section 1 above if—

(a) the accused was within its commission area at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in its commission area at that time.

(2) Subject to subsection (3) below, proceedings for an offence under section 1 above may be brought within a period of six months from the date on which evidence sufficient in the opinion of the prosecutor to warrant the proceedings came to his knowledge.

(3) No such proceedings shall be brought by virtue of this section more than three years after the commission of the offence.

(4) For the purposes of this section, a certificate signed by or on behalf of the prosecutor and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.

(5) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.

(6) In this section "commission area" has the same meaning as in the Justices of the [1979 c. 55.] Peace Act 1979.

(7) This section does not extend to Scotland.

Conviction of an offence under section 1 in proceedings for an offence under section 2 or 3.

12.—(1) If on the trial on indictment of a person charged with—

(a) an offence under section 2 above; or

(b) an offence under section 3 above or any attempt to commit such an offence;

the jury find him not guilty of the offence charged, they may find him guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings.

(2) The Crown Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it of an offence under section 1 above as a magistrates' court would have on convicting him of the offence.

(3) This section is without prejudice to section 6(3) of the [1967 c. 58.] Criminal Law Act 1967 (conviction of alternative indictable offence on trial on indictment).

(4) This section does not extend to Scotland.

Proceedings in Scotland.

13.—(1) A sheriff shall have jurisdiction in respect of an offence under section 1 or 2 above if—

(a) the accused was in the sheriffdom at the time when he

did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the sheriffdom at that time.

(2) A sheriff shall have jurisdiction in respect of an offence under section 3 above if—

(a) the accused was in the sheriffdom at the time when he did the act which caused the unauthorised modification; or

(b) the unauthorised modification took place in the sheriffdom.

(3) Subject to subsection (4) below, summary proceedings for an offence under section 1, 2 or 3 above may be commenced within a period of six months from the date on which evidence sufficient in the opinion of the procurator fiscal to warrant proceedings came to his knowledge.

(4) No such proceedings shall be commenced by virtue of this section more than three years after the commission of the offence.

(5) For the purposes of this section, a certificate signed by or on behalf of the procurator fiscal and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.

(6) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.

(7) Subsection (3) of section 331 of the [1975 c. 21.] Criminal Procedure (Scotland) Act 1975 (date of commencement of proceedings) shall apply for the purposes of this section as it applies for the purposes of that section.

(8) In proceedings in which a person is charged with an offence under section 2 or 3 above and is found not guilty or is acquitted of that charge, he may be found guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence commenced before the expiry of any time limit under this section applicable to such proceedings.

(9) Subsection (8) above shall apply whether or not an offence under section 1 above has been libelled in the complaint or indictment.

(10) A person found guilty of an offence under section 1 above by virtue of subsection (8) above shall be liable, in

respect of that offence, only to the penalties set out in section 1.

(11) This section extends to Scotland only.

Search warrants for offences under section 1.

14.—(1) Where a circuit judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing—

(a) that an offence under section 1 above has been or is about to be committed in any premises; and

(b) that evidence that such an offence has been or is about to be committed is in those premises;

he may issue a warrant authorising a constable to enter and search the premises, using such reasonable force as is necessary.

(2) The power conferred by subsection (1) above does not extend to authorising a search for material of the kinds mentioned in section 9(2) of the [1984 c. 60.] Police and Criminal Evidence Act 1984 (privileged, excluded and special procedure material).

(3) A warrant under this section—

(a) may authorise persons to accompany any constable executing the warrant; and

(b) remains in force for twenty-eight days from the date of its issue.

(4) In executing a warrant issued under this section a constable may seize an article if he reasonably believes that it is evidence that an offence under section 1 above has been or is about to be committed.

(5) In this section "premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.

(6) This section does not extend to Scotland.

Extradition where Schedule 1 to the Extradition Act 1989 applies.

15. The offences to which an Order in Council under section 2 of the [1870 c. 52.] Extradition Act 1870 can apply shall include—

(a) offences under section 2 or 3 above;

(b) any conspiracy to commit such an offence; and

(c) any attempt to commit an offence under section 3 above.

Application to Northern Ireland.

16.—(1) The following provisions of this section have effect for applying this Act in relation to Northern Ireland with the modifications there mentioned.

(2) In section 2(2)(b)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980 shall be read as a reference to Article 46(4) of the [S.I. 1981/1675 (N.I.26).] Magistrates' Courts (Northern Ireland) Order 1981.

(3) The reference in section 3(6) to the [1971 c. 48.] Criminal Damage Act 1971 shall be read as a reference to the [S.I. 1977/426 (N.I.4).] Criminal Damage (Northern Ireland) Order 1977.

(4) Subsections (5) to (7) below apply in substitution for subsections (1) to (3) of section 7; and any reference in subsection (4) of that section to England and Wales shall be read as a reference to Northern Ireland.

(5) The following paragraphs shall be inserted after paragraph (1) of Article 9 of the [S.I. 1983/1120 (N.I.13).] Criminal Attempts and Conspiracy (Northern Ireland) Order 1983—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an agreement, this Part has effect in relation to it as it has effect in relation to an agreement falling within paragraph (1).

(1B) Paragraph (1A) applies to an agreement if—

(a) a party to it, or a party's agent, did anything in Northern Ireland in relation to it before its formation;

(b) a party to it became a party in Northern Ireland (by joining it either in person or through an agent); or

(c) a party to it, or a party's agent, did or omitted anything in Northern Ireland in pursuance of it;

and the agreement would fall within paragraph (1) as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in Northern Ireland if committed in accordance with the parties' intentions."

.

(6) The following paragraph shall be inserted after paragraph (4) of that Article—

"(5) In the application of this Part to an agreement to which paragraph (1A) applies any reference to an offence shall be read as a reference to what would be the computer misuse offence in question but for the fact that it is not an offence triable in Northern Ireland.

(6) In this Article "computer misuse offence" means an offence under the Computer Misuse Act 1990."

.

(7) The following paragraphs shall be inserted after Article 3(1) of that Order—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an act, what the person doing it had in view shall be treated as an offence to which this Article applies.

(1B) Paragraph (1A) above applies to an act if—

(a) it is done in Northern Ireland; and

(b) it would fall within paragraph (1) as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in Northern Ireland.

"

.

(8) In section 8—

(a) the reference in subsection (2) to section 1(1A) of the [1977 c. 45.] Criminal Law Act 1977 shall be read as a reference to Article 9(1A) of that Order; and

(b) the reference in subsection (3) to section 1(1A) of the [1981 c. 47.] Criminal Attempts Act 1981 shall be read as a reference to Article 3(1A) of that Order.

(9) The references in sections 9(1) and 10 to England and Wales shall be read as references to Northern Ireland.

(10) In section 11, for subsection (1) there shall be substituted—

"(1) A magistrates' court for a county division in Northern Ireland may hear and determine a complaint charging an offence under section 1 above or conduct a preliminary investigation or preliminary inquiry into an offence under that section if—

(a) the accused was in that division at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in that division at that time.

"

;

and subsection (6) shall be omitted.

(11) The reference in section 12(3) to section 6(3) of the [1967 c. 58.] Criminal Law Act 1967 shall be read as a reference to section 6(2) of the [1967 c. 18 (N.I.).] Criminal Law Act (Northern Ireland) 1967.

(12) In section 14—

(a) the reference in subsection (1) to a circuit judge shall be read as a reference to a county court judge; and

(b) the reference in subsection (2) to section 9(2) of the [1984 c. 60.] Police and Criminal Evidence Act 1984 shall be read as a reference to Article 11(2) of the [S.I. 1989/13 (N.I. 12).] Police and Criminal Evidence (Northern Ireland) Order 1989.

Interpretation.

17.—(1) The following provisions of this section apply for the interpretation of this Act.

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d) above—

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) Access of any kind by any person to any program or data held in a computer is unauthorised if—

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(a) any program or data held in the computer concerned is altered or erased; or

(b) any program or data is added to its contents;

and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Such a modification is unauthorised if—

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(9) References to the home country concerned shall be read in accordance with section 4(6) above.

(10) References to a program include references to part of a program.

Citation, commencement etc.

18.—(1) This Act may be cited as the Computer Misuse Act 1990.

(2) This Act shall come into force at the end of the period of two months beginning with the day on which it is passed.

(3) An offence is not committed under this Act unless every act or other event proof of which is required for conviction of the offence takes place after this Act comes into force.

Previous **Contents**

Other UK Acts | Home | Scotland Legislation | Wales Legislation | Northern Ireland Legislation | Her Majesty's Stationery Office

 Prepared 20th September 2000

PART I

PRELIMINARY

Short title

1. This Act may be cited as the Computer Misuse Act.

Interpretation

2. --(1) In this Act, unless the context otherwise requires --

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include --

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the Gazette, prescribe;

嬪omputer output or 垦utput琎eans a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact --

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"damage" means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that --

(a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the Gazette, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

"data" means representations of information or of concepts that are being prepared

or have been prepared in a form suitable for use in a computer;

"electronic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

"intercept" , in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

"program or computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

[21/98]

--(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he --

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner),

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2) (c), a person uses a program if the function he causes the computer to perform --

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2) (d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if --

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) A reference in this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the

time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer --

(a) any program or data held in the computer concerned is altered or erased;

(b) any program or data is added to its contents; or

(c) any act occurs which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

[S 92/97]

(8) Any modification referred to in subsection (7) is unauthorised if --

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(9) A reference in this Act to a program includes a reference to part of a program.

PART II

OFFENCES

Unauthorised access to computer material

3. --(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

[21/98]

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[21/98]

(3) For the purposes of this section, it is immaterial that the act in question is not directed at --

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Access with intent to commit or facilitate commission of offence

4. --(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

[21/98]

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

[21/98]

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

[21/98]

(4) For the purposes of this section, it is immaterial whether --

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

[21/98]

Unauthorised modification of computer material

5. --(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[21/98]

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[21/98]

(3) For the purposes of this section, it is immaterial that the act in question is not directed at --

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

Unauthorised use or interception of computer service

6. --(1) Subject to subsection (2), any person who knowingly --

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[21/98]

--(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[21/98]

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at --

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Unauthorised obstruction of use of computer

7. --(1) Any person who, knowingly and without authority or lawful excuse --

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[21/98]

--(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[21/98]

Unauthorised disclosure of access code

8. --(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so --

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

[21/98]

--(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[6B

[21/98]

Enhanced punishment for offences involving protected computers

9. --(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

[21/98]

(2) For the purposes of subsection (1), a computer shall be treated as a 仍rotected computer if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for --

(a) the security, defence or international relations of Singapore;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

[21/98]

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

[6C

[21/98]

Abetments and attempts punishable as offences

10. --(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

[7

PART III

MISCELLANEOUS AND GENERAL

Territorial scope of offences under this Act

11. --(1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.

(2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

(3) For the purposes of this section, this Act shall apply if, for the offence in question --

(a) the accused was in Singapore at the material time; or

(b) the computer, program or data was in Singapore at the material time.

[8

Jurisdiction of Courts

12. A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act.

[9

Order for payment of compensation

13. --(1) The court before which a person is convicted of any offence under this Act may make an order against him for the payment by him of a sum to be fixed by the court by way of compensation to any person for any damage caused to his computer, program or data by the offence for which the sentence is passed.

(2) Any claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order of compensation under this section shall be recoverable as a civil debt.

[10

Saving for investigations by police and law enforcement officers

14. Nothing in this Act shall prohibit a police officer, a person authorised in writing by the Commissioner of Police under section 15 (1) or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to his powers conferred under any written law.

[11

[21/98]

Power of police officer to access computer and data

15. --(1) A police officer or a person authorised in writing by the Commissioner of Police shall --

(a) be entitled at any time to --

(i) have access to and inspect and check the operation of any computer to which this section applies;

(ii) use or cause to be used any such computer to search any data contained in or available to such computer; or

(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;

(b) be entitled to require --

(i) the person by whom or on whose behalf, the police officer or investigation officer has reasonable cause to suspect, any computer to which this section applies is or has been used; or

(ii) any person having charge of, or otherwise concerned with the operation of, such computer,

to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or

(c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

[21/98]

--(2) This section shall apply to a computer which a police officer or a person authorised in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.

[21/98]

(3) The powers referred to in paragraphs (a) (ii) and (iii) and (c) of subsection (1) shall not be exercised except with the consent of the Public Prosecutor.

[21/98]

(4) Any person who obstructs the lawful exercise of the powers under subsection (1) (a) or who fails to comply with a request under subsection (1) (b) or (c) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

[21/98]

(5) For the purposes of this section --

"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;

"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

[14

[21/98]

Arrest by police without warrant

16. Any police officer may arrest without warrant any person reasonably suspected of committing an offence under this Act.

[15

Crimial Code Act 1995 Schedule - The Criminal Code

Division 15—Extended geographical jurisdiction

15.1 Extended geographical jurisdiction—category A

(1) If a law of the Commonwealth provides that this section applies to a particular offence, a person does not commit the offence unless:

(a) the conduct constituting the alleged offence occurs:

(i) wholly or partly in Australia; or

(ii) wholly or partly on board an Australian aircraft or an Australian ship; or

(b) the conduct constituting the alleged offence occurs wholly outside Australia and a result of the conduct occurs:

(i) wholly or partly in Australia; or

(ii) wholly or partly on board an Australian aircraft or an Australian ship; or

(c) the conduct constituting the alleged offence occurs wholly outside Australia and:

(i) at the time of the alleged offence, the person is an Australian citizen; or

(ii) at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or

(d) all of the following conditions are satisfied:

(i) the alleged offence is an ancillary offence;

(ii) the conduct constituting the alleged offence occurs wholly outside Australia;

(iii) the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia or wholly or partly on board an Australian aircraft or an Australian ship.

Note: The expression ***offence*** is given an extended meaning by subsection 11.2(1), section 11.3 and subsection 11.6(1).

Defence—primary offence

(2) If a law of the Commonwealth provides that this section applies to a particular offence, a person is not guilty of the offence if:

(aa) the alleged offence is a primary offence; and

(a) the conduct constituting the alleged offence occurs wholly in a foreign country, but not on board an Australian aircraft or an Australian ship; and

(b) the person is neither:

(i) an Australian citizen; nor

(ii) a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; and

(c) there is not in force in:

(i) the foreign country where the conduct constituting the alleged offence occurs; or

(ii) the part of the foreign country where the conduct constituting the alleged offence occurs;

a law of that foreign country, or a law of that part of that foreign country, that creates an offence that corresponds to the first-mentioned offence.

Note: A defendant bears an evidential burden in relation to the matters in subsection (2). See subsection 13.3(3).

(3) For the purposes of the application of subsection 13.3(3) to an offence, subsection (2) of this section is taken to be an exception provided by the law creating the offence.

Defence—ancillary offence

(4) If a law of the Commonwealth provides that this section applies to a particular offence, a person is not guilty of the offence if:

(a) the alleged offence is an ancillary offence; and

(b) the conduct constituting the alleged offence occurs wholly in a foreign country, but not on board an Australian aircraft or an Australian ship; and

(c) the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly in a foreign

country, but not on board an Australian aircraft or an Australian ship; and

(d) the person is neither:

(i) an Australian citizen; nor

(ii) a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; and

(e) there is not in force in:

(i) the foreign country where the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur; or

(ii) the part of the foreign country where the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur;

a law of that foreign country, or a law of that part of that foreign country, that creates an offence that corresponds to the primary offence.

Note: A defendant bears an evidential burden in relation to the matters in subsection (4). See subsection 13.3(3).

(5) For the purposes of the application of subsection 13.3(3) to an offence, subsection (4) of this section is taken to be an exception provided by the law creating the offence.

Part 10.7—Computer offences
Division 476—Preliminary
476.1 Definitions

(1) In this Part:

access to data held in a computer means:

(a) the display of the data by the computer or any other output of the data from the computer; or

(b) the copying or moving of the data to any other place in the computer or to a data storage device; or

(c) in the case of a program—the execution of the program.

Commonwealth computer means a computer owned, leased or operated by a Commonwealth entity.

data includes:

(a) information in any form; or

(b) any program (or part of a program).

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; or

(b) data held in a data storage device on a computer network of which the computer forms a part.

data storage device means a thing (for example, a disk or file server) containing, or designed to contain, data for use by a computer.

electronic communication means a communication of information in any form by means of guided or unguided electromagnetic energy.

impairment of electronic communication to or from a computer includes:

(a) the prevention of any such communication; or

(b) the impairment of any such communication on an electronic link or network used by the computer;

but does not include a mere interception of any such communication.

modification, in respect of data held in a computer, means:

(a) the alteration or removal of the data; or

(b) an addition to the data.

telecommunications service means a service for carrying communications by means of guided or unguided electromagnetic energy or both.

unauthorised access, modification or impairment has the meaning given in section 476.2.

(2) In this Part, a reference to:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer;

is limited to such access, modification or impairment caused, whether directly or indirectly, by the execution of a function of a computer.

476.2 Meaning of unauthorised access, modification or impairment

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

(2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to it.

(4) For the purposes of subsection (1), if:

(a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and

(b) the person does so under a warrant issued under the law of the Commonwealth, a State or a Territory;

the person is entitled to cause that access, modification or impairment.

476.3 Geographical jurisdiction

Section 15.1 (extended geographical jurisdiction—Category A) applies to offences under this Part.

476.4 Saving of other laws

(1) This Part is not intended to exclude or limit the operation of any other law of the Commonwealth, a State or a Territory.

(2) Subsection (1) has effect subject to section 476.5.

476.5 Liability for certain acts

(1) A staff member or agent of ASIS or DSD (the *agency*) is not subject to any civil or criminal liability for any computer-related act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the act:

(i) taken together with a computer-related act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but

(ii) in the absence of that computer-related act, event, circumstance or result, would not amount to an offence; and

(c) the act is done in the proper performance of a function of the agency.

(2A) Subsection (2) is not intended to permit any act in relation to premises, persons, computers, things, or telecommunications services in Australia, being:

(a) an act that ASIO could not do without a Minister authorising it by warrant issued under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* or under Part III of the *Telecommunications (Interception) Act 1979*; or

(b) an act to obtain information that ASIO could not obtain other than in accordance with section 283 of the *Telecommunications Act 1997*.

(2B) The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether an act was done in the proper performance of a function of an agency.

(2C) In any proceedings, a certificate given under subsection (2B) is prima facie evidence of the facts certified.

(3) In this section:

ASIS means the Australian Secret Intelligence Service.

civil or criminal liability means any civil or criminal liability (whether under this Part, under another law or otherwise).

computer-related act, event, circumstance or result means an act, event, circumstance or result involving:

(a) the reliability, security or operation of a computer; or

(b) access to, or modification of, data held in a computer or on a data storage device; or

(c) electronic communication to or from a computer; or

(d) the reliability, security or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; or

(e) possession or control of data held in a computer or on a data storage device; or

(f) producing, supplying or obtaining data held in a computer or on a data storage device.

DSD means that part of the Department of Defence known as the Defence Signals Directorate.

staff member means:

(a) in relation to ASIS—the Director-General of ASIS or a member of the staff of ASIS (whether an employee of ASIS, a consultant to ASIS, or a person who is made available by another Commonwealth or State authority or other person to perform services for ASIS); and

(b) in relation to DSD—the Director of DSD or a member of the staff of DSD (whether an employee of DSD, a consultant to DSD, or a person who is made available by another Commonwealth or State authority or other person to perform services for DSD).

Division 477—Serious computer offences

477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

Intention to commit a serious Commonwealth, State or Territory offence

(1) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a telecommunications service; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

(2) Absolute liability applies to paragraph (1)(b).

(3) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the offence was:

(a) an offence against a law of the Commonwealth, a State or a Territory; or

(b) a serious offence.

Intention to commit a serious Commonwealth offence

(4) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the person knows the access, modification or impairment is unauthorised; and

(c) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth (whether by that person or another person) by the access, modification or impairment.

(5) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the offence was:

(a) an offence against a law of the Commonwealth; or

(b) a serious offence.

Penalty

(6) A person who is guilty of an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence.

Impossibility

(7) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

No offence of attempt

(8) It is not an offence to attempt to commit an offence against this section.

Meaning of serious offence

(9) In this section:

serious offence means an offence that is punishable by imprisonment for life or a period of 5 or more years.

477.2 Unauthorised modification of data to cause impairment

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised modification of data held in a computer; and

(b) the person knows the modification is unauthorised; and

(c) the person is reckless as to whether the modification impairs or will impair:

(i) access to that or any other data held in any computer; or

(ii) the reliability, security or operation, of any such data; and

(d) one or more of the following applies:

(i) the data that is modified is held in a Commonwealth computer;

(ii) the data that is modified is held on behalf of the Commonwealth in a computer;

(iii) the modification of the data is caused by means of a telecommunications service;

(iv) the modification of the data is caused by means of a Commonwealth computer;

(v) the modification of the data impairs access to, or the reliability, security or operation of, other data held in a Commonwealth computer;

(vi) the modification of the data impairs access to, or the reliability, security or operation of, other data held on behalf of the Commonwealth in a computer;

(vii) the modification of the data impairs access to, or the reliability, security or operation of, other data by means of a telecommunications service.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:

(a) access to data held in a computer; or

(b) the reliability, security or operation, of any such data.

(4) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.3 (unauthorised impairment of electronic communication).

477.3 Unauthorised impairment of electronic communication

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised impairment of electronic communication to or from a computer; and

(b) the person knows that the impairment is unauthorised; and

(c) one or both of the following applies:

(i) the electronic communication is sent to or from the computer by means of a telecommunications service;

(ii) the electronic communication is sent to or from a Commonwealth computer.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(c).

(3) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.2 (unauthorised modification of data to cause impairment).

Division 478—Other computer offences

478.1 Unauthorised access to, or modification of, restricted data

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised access to, or modification of, restricted data; and

(b) the person intends to cause the access or modification; and

(c) the person knows that the access or modification is unauthorised; and

(d) one or more of the following applies:

(i) the restricted data is held in a Commonwealth computer;

(ii) the restricted data is held on behalf of the Commonwealth;

(iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) In this section:

restricted data means data:

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

478.2 Unauthorised impairment of data held on a computer disk etc.

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised impairment of the reliability, security or operation of data held on:

(i) a computer disk; or

(ii) a credit card; or

(iii) another device used to store data by electronic means; and

(b) the person intends to cause the impairment; and

(c) the person knows that the impairment is unauthorised; and

(d) the computer disk, credit card or other device is owned or leased by a Commonwealth entity.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

478.3 Possession or control of data with intent to commit a computer offence

(1) A person is guilty of an offence if:

(a) the person has possession or control of data; and

(b) the person has that possession or control with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of possession or control of data

(4) In this section, a reference to a person having possession or control of data includes a reference to the person:

(a) having possession of a computer or data storage device that holds or contains the data; or

(b) having possession of a document in which the data is recorded; or

(c) having control of data held in a computer that is in the possession of another person (whether inside or outside Australia).

478.4 Producing, supplying or obtaining data with intent to commit a computer offence

(1) A person is guilty of an offence if:

(a) the person produces, supplies or obtains data; and

(b) the person does so with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of producing, supplying or obtaining data

(4) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person:

(a) producing, supplying or obtaining data held or contained in a computer or data storage device; or

(b) producing, supplying or obtaining a document in which the data is recorded.

Extracts of USA PATRIOT Act 2001
amending section 1030 of the United States Code Title 18

SEC. 814. DETERRENCE AND PREVENTION OF CYBERTERRORISM.

(a) CLARIFICATION OF PROTECTION OF PROTECTED COMPUTERS- Section 1030(a)(5) of title 18, United States Code, is amended--

(1) by inserting `(i)' after `(A)';

(2) by redesignating subparagraphs (B) and (C) as clauses (ii) and (iii), respectively;

(3) by adding `and' at the end of clause (iii), as so redesignated; and

(4) by adding at the end the following:

`(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

`(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

`(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

`(iii) physical injury to any person;

`(iv) a threat to public health or safety; or

`(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;'.

(b) PROTECTION FROM EXTORTION- Section 1030(a)(7) of title 18, United States Code, is amended by striking `, firm, association, educational institution, financial institution, government entity, or other legal entity,'.

(c) PENALTIES- Section 1030(c) of title 18, United States Code, is amended--

(1) in paragraph (2)--

(A) in subparagraph (A) --

(i) by inserting `except as provided in subparagraph (B),' before `a fine';

(ii) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and

(iii) by striking `and' at the end;

(B) in subparagraph (B), by inserting `or an attempt to commit an offense punishable under this subparagraph,' after `subsection (a)(2),' in the matter preceding clause (i); and

(C) in subparagraph (C), by striking `and' at the end;

(2) in paragraph (3)--

(A) by striking `, (a)(5)(A), (a)(5)(B),' both places it appears; and

(B) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and

(3) by adding at the end the following:

`(4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

`(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

`(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.'.

(d) DEFINITIONS- Section 1030(e) of title 18, United States Code is amended--

(1) in paragraph (2)(B), by inserting `, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States' before the semicolon;

(2) in paragraph (7), by striking `and' at the end;

(3) by striking paragraph (8) and inserting the following:

`(8) the term `damage' means any impairment to the integrity or availability of data, a program, a system, or information;';

(4) in paragraph (9), by striking the period at the end and inserting a semicolon; and

(5) by adding at the end the following:

`(10) the term `conviction' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

`(11) the term `loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

`(12) the term `person' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.'.

(e) DAMAGES IN CIVIL ACTIONS- Section 1030(g) of title 18, United States Code is amended--

(1) by striking the second sentence and inserting the following: `A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.'; and

(2) by adding at the end the following: `No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.'.

(f) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER FRAUD AND ABUSE- Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall amend the Federal sentencing guidelines to ensure that any individual convicted of a violation of section 1030 of title 18, United States Code, can be subjected to appropriate penalties, without regard to any mandatory minimum term of imprisonment.

Annex D

Prev | Next

TITLE 18 > PART I > CHAPTER 47 > Sec. 1030.

Sec. 1030. - Fraud and related activity in connection with computers

(a)

Whoever -

(1)

having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2)

intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A)

information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B)

information from any department or agency of the United States; or

(C)

information from any protected computer if the conduct involved an interstate or foreign communication;

(3)

intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United

States and such conduct affects that use by or for the Government of the United States;

(4)

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A)

knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B)

intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C)

intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6)

knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -

(A)

such trafficking affects interstate or foreign commerce; or

(B)

such computer is used by or for the Government of the United States; [1] "or".

(7)

with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b)

Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c)

The punishment for an offense under subsection (a) or (b) of this section is -

(1)

(A)

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense

punishable under this subparagraph; and

(B)

a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A)

a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and [2]

(B)

a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if -

(i)

the offense was committed for purposes of commercial advantage or private financial gain;

(ii)

the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii)

the value of the information obtained exceeds $5,000; [3] So in original. Probably should be followed by "and".

(C)

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)

(A)

a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and [4]

(d)

The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be

entered into by the Secretary of the Treasury and the Attorney General.

(e)

As used in this section -

(1)

the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2)

the term "protected computer" means a computer -

(A)

exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B)

which is used in interstate or foreign commerce or communication;

(3)

the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4)

the term "financial institution" means -

(A)

an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B)

the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C)

a credit union with accounts insured by the National Credit Union Administration;

(D)

a member of the Federal home loan bank system and any home loan bank;

(E)

any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F)

a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G)

the Securities Investor Protection Corporation;

(H)

a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I)

an organization operating under section 25 or section 25(a) [5] of the Federal Reserve Act. (FOOTNOTE 6) [6] So in original. The period probably should be a semicolon.

(5)

the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6)

the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7)

the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5; and [7]

(8)

the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that -

(A)

causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

(B)

modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C)

causes physical injury to any person; or

(D)

threatens public health or safety; and

(9)

the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.

(f)

This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g)

Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as

defined in subsection (e)(8)(A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h)

The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5)

---

[1] So in original. Probably should be followed by

[2] So in original. The word "and" probably should not appear.

[3]

[4] So in original. The "; and" probably should be a period.

[5] See References in Text note below.

[7] So in original. The word "and" probably should not appear.

Prev | Next

Annex E

Extract of Convention on Cybercrime of the Council of Europe

Section 3 - Jurisdiction

Article 22 - Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Annex F

STATEMENT ON FIGHTING TERRORISM AND PROMOTING GROWTH

Los Cabos, Mexico
26 october 2002

One year ago in Shanghai, meeting in the shadow of the attacks of September 11, 2001, we condemned international terror in the strongest terms and resolved to strengthen our cooperation in combating terror. In the year since, much has been accomplished. Yet much more remains to be done, and today we declare our strong commitment to put in place – as soon as possible – specific, additional measures needed to fully implement the broad principles we stated in the Shanghai Counter-Terrorism Statement.

The recent terrorist bombing in Bali, Indonesia carried out on October 12, 2002 reminds us of terrorism's brutality and the global imperative to oppose and fight this threat wherever it may be found. We condemn this mass slaughter of the innocent, many of whom were Indonesian and Australian citizens, and offer our deepest sympathies and condolences to the victims and their families.

Terrorism is a direct challenge to APEC's goals of free, open and prosperous economies and an affront to the fundamental values that APEC members share. We are united in our determination to end the threat that terrorism poses to our shared goals and committed to accelerate our progress towards the anti-terror goals and programs set forth last year in Shanghai.

Progress Since Shanghai

A year ago, we promised to strengthen cooperation at all levels in combating terrorism in a comprehensive manner and to faithfully implement our obligations under the United Nations. Since Shanghai, we have made important progress in working individually, bilaterally, regionally and globally, to meet our United Nations obligations, break up terrorist cells, and disrupt terrorist financing.

We are implementing the measures called for in relevant U.N. Security Council Resolutions, and are putting in place the legal and regulatory mechanisms to implement Resolution 1373.

Each of the relevant members of APEC has signed and ratified -- or is proceeding to ratify immediately -- the International U.N. Convention for the Suppression of the Financing of Terrorism.

We have established improved subregional and regional counter-terrorism mechanisms, significantly increasing the sharing of information between enforcement and intelligence officials.

We have upgraded security at the region's major ports and airports.

Collectively, we are working in APEC to introduce more effective baggage screening in airports in the region, improve coordination between immigration officials, implement new cyber security standards, advance the Energy Security Initiative to address disruptions in energy markets, and enhance anti-piracy cooperation.

Joint Commitment to Fully Implement Shanghai Counter-terror Statement

These measures have made important contributions to the fight against global terror. But more is needed. As we accelerate our progress against terrorism, APEC economies must also move to meet the challenge of encouraging global economic growth and bringing the benefits of global markets to all our peoples.

Consequently, we must grow our economies even as we protect our borders and find new ways to secure our key economic infrastructure from terrorist attacks.

Accordingly, we, the Leaders of APEC, agree to the following additional joint actions to fully implement the broad commitments we made last year in Shanghai. We endeavor to ensure that key Pacific Rim infrastructure in the areas of trade, finance and information systems is protected by:

ENHANCING SECURE TRADE IN THE APEC REGION ("STAR")

APEC represents 60 percent of the world's GDP and half of its trade. Most of the world's top megaports are in APEC economies, as are most of the world's busiest airports. We will work together to secure the flow of goods and people through measures to:

- **Protect cargo by**
  - Implementing expeditiously a container security regime that would assure in-transit integrity of containers, identify and examine high-risk containers, and working within international organizations to require the provision of advance electronic information on container content to customs, port, and shipping officials as early as possible in the supply chain, while taking into consideration the facilitation of legitimate trade.
  - Implementing by 2005 wherever possible the common standards for electronic customs reporting developed by the World Customs Organization that provide data to target high-risk shipments and facilitate trade.
  - Promoting private-sector adoption of high standards of supply chain security, as developed by the private sector and law enforcement officials.
- **Protect ships engaged in international voyages by**
  - Promoting ship and port security plans by July 2004 and installation of automatic identification systems on certain ships by December 2004.*
  - Enhancing cooperation on fighting piracy in the region between APEC fora and organizations such as the International Maritime Bureau Piracy Reporting Center and International Maritime Organization (IMO).
- **Protect international aviation by**
  - Improving airline passenger and crew safety by introducing, highly effective baggage screening procedures and equipment in all APEC international airports as soon as possible, and in any case by 2005; accelerating implementation of

standards for reinforced flight deck doors for passenger aircraft by April 2003 wherever possible; and supporting International Civil Aviation Organization (ICAO) mandatory aviation security audits.

- Enhancing air cargo security by promoting adoption of the guidelines developed by ICAO and the International Air Transport Association (IATA).

- **Protect people in transit by**

  - Implementing as expeditiously as possible a common global standard based on UN EDIFACT for the collection and transmission of advance passenger information.

  - Adopting standards for application of biometrics in entry and (where applicable) exit procedures and travel documents such as those being developed by the ICAO and the International Standards Organization.

  - Assuring the highest possible integrity of all government officials who are involved in border operations.

HALTING TERRORIST FINANCING

We will jointly work to deny terrorists access to the world's financial system and use the money trail to locate and apprehend terrorists, in line with the comprehensive approach adopted by our Finance Ministers in September, including through measures to:

- **Fully implement U.N. and other international instruments by**

  - Endeavoring to ratify the International Convention for the Suppression of the Financing of Terrorism no later than October 2003.

  - Implementing quickly and decisively all measures needed to prevent terrorists and their supporters from accessing the international financial system, as called for in U.N. Security Council Resolutions 1373 and 1390. These measures include:

    - effective blocking of terrorist assets;
    - criminalization of the financing of terrorism;
    - increased efforts to investigate and prosecute money launderers and terrorist financiers;
    - preventive steps to protect the integrity of the financial system by regulating and supervising the financial sector consistent with international standards;
    - joint identification and designation of targets of regional interest.

  - Supporting the FATF's Eight Special Recommendations on terrorist financing and pledging to comply as quickly as possible with the recommendations; calling on the IMF and World Bank, in coordination with FATF, to begin conducting integrated and comprehensive assessments of countries' efforts to implement these recommendations and identifying jurisdictions which need technical assistance.

- **Promote better monitoring of alternative remittance systems and non-profit organizations by**

  - Supporting the work of APEC finance officials and regional bodies on alternative remittance systems, including an analysis of the factors that encourage their use.

  - Protecting non-profit organizations and well-meaning donors from having their funds misused by terrorist financiers, and endorsing FATF's recently announced best practices for preventing abuse of charitable institutions by terrorists.

- **Enhance law enforcement and regulatory capabilities by**

  - Establishing or identifying by October 2003 a financial intelligence unit (FIU) in each member economy, and taking steps to enhance information sharing with other FIUs.

  - Supporting private sector initiatives such as the Wolfsberg Statement on the Suppression of the Financing of Terrorism and endorsing cooperation between financial institutions and governments.

PROMOTING CYBER SECURITY

Citizens of APEC economies now account for over half of the world's Internet users. The global communications network is only as secure as its weakest link, and we collectively commit to:

- Endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003.

- Identify national cybercrime units and international high-technology assistance points of contact and create such capabilities to the extent they do not already exist, by October 2003.

- Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003.

We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime.

IMPLEMENTATION AND CAPACITY BUILDING

Building an APEC region – and a global economic system – that is both more secure and more efficient is a monumental undertaking – and one that is critically important to the peace and prosperity of our planet. Success in fulfilling this vision will require enhanced cooperation, new procedures, and greater use of advanced technology.

We call on APEC officials to continue to cooperate in implementation of the joint actions outlined above and monitor progress of implementation. It is also important that all APEC economies develop the capacity to participate fully in this endeavor.

Accordingly Leaders commit to work cooperatively to build capacity throughout the region so that all economies can benefit from the resulting gains in security and prosperity.

To build on the considerable counter-terrorism-related training and other assistance already being undertaken in the APEC region, we:

- Welcome new commitments by APEC members to contribute further to these capacity-building efforts,
- Commend current efforts by the international financial institutions to build counter-terrorism capacity in APEC economies and call on them to work with APEC members to further improve APEC member capacity,
- Encourage the private sector to work in partnership with APEC economies to implement secure trade measures, and
- Emphasize that counter-terrorism capacity-building in APEC needs to be demand-driven.

* Russia supports promoting ship and port security plans by July 2004 and installation of Automatic Identification Systems on certain ships by December 2004, but notes that technical issues relating to Russia may require extending the timeframe to no later than December 2006.

Extract of clause 11 of the National Security (Legislative Provisions) Bill

11. Information resulting from unauthorized disclosures or illegal access or information entrusted in confidence

(1) Section 18(2) is amended—

(*a*) in paragraph (*b*), by repealing "or" at the end;

(*b*) in paragraph (*c*), by repealing the full stop and substituting "; or";

(*c*) by adding—

"(*d*) acquired by means of illegal access (whether by himself or another) to it,

and for the purposes of paragraphs (*a*) and (*b*), "public servant or government contractor" includes a person who was formerly a public servant or government contractor where the information, document or article came into his possession when he was such a public servant or government contractor.".

(2) Section 18 is amended by adding—

"(5A) For the purposes of subsection (2), a person has illegal access to information or a document or article if—

(*a*) the information, document or article, as the case may be, comes into or remains in his possession by virtue of an offence under—

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

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

(iii) section 9 (theft), 10 (robbery) or 11 (burglary) of the Theft Ordinance (Cap. 210),

committed by him in relation to the information, document or article, as the case may be; or

(*b*) the information, document or article, as the case may be, comes into or remains in his possession in exchange for an advantage the offer or acceptance of which is an offence under section 4 (bribery) of the Prevention of Bribery Ordinance (Cap. 201).".

(3) Section 18(6)(*a*) is amended by repealing "or international relations" and substituting ", international relations or affairs concerning the Hong Kong Special Administrative Region which are, under the Basic Law, within the responsibility of the Central Authorities".

(4) Section 18(6) is amended by repealing "to 16" and substituting "to 16A".

《國家安全(立法條文)條例草案》第 11 條摘錄

11. 因未經授權的披露或違法取覽所得的資料或在機密情況下託付的資料

(1) 第 18(2) 條現予修訂——

(*a*) 在 (*b*) 段中，廢除末處的"或"；

(*b*) 在 (*c*) 段中，廢除句號而代以"；或"；

(*c*) 加入——

"(*d*) 它藉着 (不論被該有關人士或另一人) 違法取覽而被取得，

而就 (*a*) 及 (*b*) 段而言，"公務人員或政府承辦商"在有關資料、文件或物品是在某前任公務人員或前任政府承辦商仍是公務人員或政府承辦商期間落入他的管有的情況下，包括該前任公務人員或前任政府承辦商。"。

(2) 第 18 條現予修訂，加入——

"(5A) 就第 (2) 款而言，如有以下情況，有關的人即屬違法取覽資料、文件或物品——

(*a*) 有關的資料、文件或物品 (視屬何情況而定) 憑藉該人就該資料、文件或物品 (視屬何情況而定) 所犯的下列罪行，而落入他的管有或維持由他管有——

(i) 《電訊條例》(第 106 章) 第 27A 條 (藉電訊而在未獲授權下取用電腦資料) 所訂罪行；

(ii) 《刑事罪行條例》(第 200 章) 第 161 條 (有犯罪或不誠實意圖而取用電腦) 所訂罪行；或

(iii) 《盜竊罪條例》(第 210 章) 第 9 (盜竊罪)、10 (搶劫罪) 或 11 (入屋犯法罪) 條所訂罪行；或

(*b*) 有關的資料、文件或物品 (視屬何情況而定) 以一項利益作為交換而落入他的管有或維持由他管有，而提供或接受該項利益屬《防止賄賂條例》(第 201 章) 第 4 條 (賄賂) 所訂罪行。"。

(3) 第 18(6)(*a*) 條現予修訂，廢除"或防務或國際關係"而代以"、防務、國際關係或與香港特別行政區有關而根據《基本法》是由中央管理的事務"。

(4) 第 18(6) 條現予修訂，廢除"至 16"而代以"至 16A"。