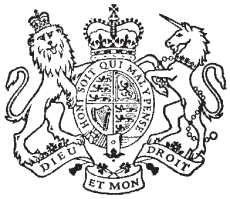

SUPPLEMENT No. 2

TO

THE SOVEREIGN BASE AREAS GAZETTE

No. 1591 of 1st September 2010

LEGISLATION

CONTENTS:

The following LEGISLATION is published in this Supplement which forms part of this Gazette : –

COMPUTER MISUSE ORDINANCE 2010

ARRANGEMENT OF SECTIONS

Part 1
Preliminary

Section

Part 2

Offences against the integrity of computer systems

Part 3

Offences committed using computer systems

Part 4

Miscellaneous

Ordinance 24 of 2010
Published in Gazette No. 1591 of 1st September 2010

COMPUTER MISUSE ORDINANCE 2010

An Ordinance to make provision for securing computer material against unauthorised access, use or modification and for related purposes

J. H. GORDON
ADMINISTRATOR

31st August 2010.

BE it enacted by the Administrator of the Sovereign Base Areas of Akrotiri and Dhekelia as follows:—

Part 1

Preliminary

1. Short title

This Ordinance may be cited as the Computer Misuse Ordinance 2010.

2. Interpretation

In this Ordinance—

"act" includes a series of acts;

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable for causing a computer program to perform a function;

"computer system" means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data.

Part 2

Offences against the integrity of computer systems

3. Unauthorised access to a computer system

(1) A person commits an offence if—

(a) by breaching a security measure, that person causes a computer system to perform any function with intent to secure access to any program or computer data held in any computer system, or to enable any such access to be secured; and

(b) that person is not authorised to secure that access or enable it to be secured and knows he or she is not so authorised.

(2) The intention referred to in subsection (1) need not relate to—

(a) any particular computer system;

(b) any particular program or computer data; or

(c) a program or computer data of any particular kind.

4. Unlawful interception

(1) A person commits an offence if that person—

(a) intentionally intercepts a transmission of computer data to, from or within a computer system; and

(b) is not authorised to intercept that transmission and knows that he or she is not so authorised.

(2) A person intercepts a transmission of computer data to, from or within a computer system if, and only if, that person does any of the following acts so as to make some or all of the contents of the transmission available, while being transmitted, to a person other than the sender or intended recipient of the transmission, namely that person—

(a) modifies or interferes with the system, or its operation; or

(b) monitors the transmission made by means of the system.

(3) References in this Ordinance to the interception of transmissions of computer data do not include references to the interception of any transmissions broadcast for general reception.

(4) For the purposes of this section—

(a) references to the modification of a computer system include references to the attachment of any apparatus to, or other modification of or interference with any part of the system;

(b) transmissions of computer data to, from or within a computer system include electromagnetic emissions or any other type of emission to, from or within the computer system carrying or storing such data.

5. Unlawful alteration or destruction of data

(1) A person commits an offence if that person intentionally—

(a) destroys, deletes, alters or conceals computer data on a computer system; and

(b) that person is not authorised to destroy, delete, alter or conceal that data and knows that he or she is not so authorised.

6. Unlawful interference with computer systems

(1) A person commits an offence if that person intentionally—

(a) does any act which hinders the operation of a computer system; and

(b) that person is not authorised to do the act and knows that he or she is not so authorised.

(2) For the purposes of this section—

(a) an act will hinder the operation of a computer system if it—

(i) impairs the operation of any computer;

(ii) prevents or hinders access to any program or computer data held in any computer; or

(iii) impairs the operation of any such program or the reliability of any such data.

(b) "act" includes entering, transmitting, damaging, altering, suppressing and deleting computer data.

(3) The intention referred to in subsection (1) need not relate to—

(a) any particular computer system;

(b) any particular program or computer data; or

(c) a program or computer data of any particular kind.

7. Articles used for committing offences under sections 3 to 6

(1) A person commits an offence if that person—

(a) intentionally produces, sells, procures for use, imports, distributes or otherwise makes available—

(i) a device, including a computer program, designed or adopted primarily for the commission of an offence under sections 3 to 6;

(ii) a computer password, access code, or computer data by means of which access may be secured to the whole or part of a computer system; and

(b) is not authorised to do the act referred to in paragraph (a) and knows that he or she is not so authorised.

(2) A person commits an offence if that person possesses any item referred to in subsection (1)(a) with the intention of using that item for the commission of an offence under sections 3 to 6.

Part 3

Offences committed using computer systems

8. Computer related forgery

(1) A person commits an offence if that person—

(a) intentionally creates a false entry in a computer system intending that the false entry will be considered or acted upon for any legal purpose as if it were authentic; and

(b) is not authorised to make the false entry and knows that he or she is not so authorised.

(2) A person creates a false entry if that person—

(a) enters, alters, deletes, suppresses or conceals computer data so that inauthentic computer data is thereby generated; and

(b) intends that the inauthentic computer data is acted upon for any legal purpose.

(3) For the purposes of this section, it is not relevant that the false entry generates computer data which is not directly readable.

9. Computer related fraud

(1) A person commits an offence if that person—

(a) intentionally makes a fraudulent entry for the purpose of fraudulently procuring an economic benefit for himself or herself or for any other person;

(b) causes another person to lose property; and

(c) is not authorised to make the fraudulent entry and knows that he or she is not so authorised.

(2) A person creates a fraudulent entry if that person—

(a) enters, alters, deletes, suppresses or conceals computer data; or

(b) interferes with the functioning of the computer system.

Part 4

Miscellaneous

10. Criminal offences

A person who is guilty of an offence under this Ordinance is liable to imprisonment for 5 years or a fine of €34,172 or both.

11. Liability of bodies corporate

(1) A body corporate may be convicted of an offence under this Ordinance if—

(a) the offence is committed for its benefit by a natural person acting either individually or as part of the organisation of that body corporate; and

(b) the natural person has—

(i) power to represent the body corporate;

(ii) authority to take decisions on behalf of the body corporate; or

(iii) authority to exercise control within the body corporate.

(2) Nothing in this section prevents criminal proceedings under this Ordinance being brought against a natural person referred to in subsection (1).

12. Extension of powers of seizure to computerised information

Every power of seizure which is conferred by an Ordinance on a police officer who has entered premises in the exercise of a power conferred by that Ordinance is to be construed as including a power to require information stored in electronic form and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form.

13. Jurisdiction of the courts

The courts of the Areas have jurisdiction to try offences committed under this Ordinance if the offence is committed using a computer system accessed from the Areas.

14. Application to the Crown

(1) This Ordinance does not bind the Crown or agents acting on behalf of the Crown.

(2) For the purposes of this section "the Crown" means Her Majesty in right of Her Government in the United Kingdom and in right of Her Administration in the Areas.

15. Commencement

This Ordinance comes into force on the day it is published in the Gazette.

EXPLANATORY NOTE

(This note does not form part of the Ordinance)

1. This explanatory note relates to the Computer Misuse Ordinance 2010 (the "Ordinance"). It has been prepared by the Office of the Attorney General and Legal Adviser in order to assist the reader of the Ordinance. It does not form part of the Ordinance.

2. The Ordinance replicates in part the effects of the Republican Convention Against Cybercrime (Ratifying) Law of 2004 (Law 22(III)2004).

3. The Ordinance creates a number of new offences in relation to computers. Part 2 deals with offences related to the integrity of computer systems. Section 3 of the Ordinance creates an offence of unauthorised access to a computer system. Section 4 creates an offence of unauthorised interception of a transmission of computer data (such as emails). Section 5 makes it an offence to destroy, delete, alter or conceal data which is held on a computer system. Section 6 creates an offence of hindering the operation of a computer system. This section makes activities such as "spamming" with the intention of damaging the operation of a computer system unlawful. Section 7 makes it unlawful to produce, sell, procure for use, import, distribute or otherwise make available a device, password or access code which can be used for committing an offence under Part 2.

4. Part 3 of the Ordinance deals with offences which can be committed using a computer system. These offences are using a computer to commit forgery (section 8) and fraud (section 9).

5. Section 12 extends powers of seizure which are conferred on a police officer to include power to require any information stored in any electronic form and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form. Those powers are primarily contained in the Criminal Procedure Ordinance (Cap 155). The extension of those powers conferred by in section 12 is of general application. It does not just apply to investigation of offences created under the Ordinance.

(SBA/AG/2/CR/498)

Printed by the Sovereign Base Areas Administration Printing Press.