Section 16: Cybercrime Offenses

General Commentary

A growing number of states have introduced or are in the process of introducing new legislation on cybercrime offenses. In some post-conflict states, cybercrime offenses have gone unpunished due to the lack of substantive legal provisions criminalizing this conduct.

In 2001 the Council of Europe adopted the Convention on Cybercrime, aimed at deterring "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data" (preamble). Increasingly sophisticated technology has brought with it increasingly sophisticated criminals who have used computer systems, networks, and computers for illegitimate ends. To combat such conduct, the convention requires states parties to criminalize certain forms of conduct and to introduce procedural measures for the investigation of cybercrime (chapter 2, section 2, "Procedural Law") and provisions on international cooperation in the investigation and prosecution of cybercrime offenses (chapter 3, "International Cooperation").

The Convention on Cybercrime contains nine criminal offenses in four different categories: (1) offenses against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related offenses (e.g., computer-related forgery and computer-related fraud); (3) content-related offenses (e.g., offenses related to child pornography); and (4) offenses related to the infringement of copyright and related rights. The creation of common language for cybercrime offenses aims at "establishing a common minimum standard" (explanatory report to the Convention on Cybercrime, paragraph 33). Section 16 of the MCC contains offenses in the first category, namely, illegal access, illegal interception, data interference, system interference, and misuse of devices. Section 5 of the Special Part of the MCC on offenses against children, and specifically Article 117 ("Child Pornography") and Article 118 ("Possession of Child Pornography"), incorporates the third category of offenses.

Close attention should be paid to the explanatory report to the convention for a description of the rationale behind including cybercrime offenses in domestic criminal law and for a discussion on their substantive content. Because the report goes into detail about each of the individual offenses listed in Section 16, the MCC makes

reference to the relevant parts of the report rather than duplicating its content. When a state plans to introduce legislation on cybercrime, it should take into account the complexities involved in training personnel to conduct investigations of these offenses and the inherent complexity in the actual investigation of these offenses. Both activities are very resource intensive and will require a substantial commitment of personnel, money, materials, and equipment, coupled with a comprehensive training agenda.

Articles 14–21 of the Convention on Cybercrime also require states to implement a number of tools to assist in the investigation of cybercrime offenses. Some of these tools have been integrated into the MCCP. Reference should be made to Chapter 8, Part 3, Sections 4 and 5, and their accompanying commentary.

Comprehensive background on and discussion of computer-related crime and national and international initiatives to tackle it is presented in the background paper to Workshop 6: Measures to Combat Computer-Related Crime, prepared for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice. Useful reference may also be made to the Computer Crime Research Centre, a nonprofit, nongovernmental organization established to conduct research into legal, criminal, and criminological problems of cybercrime with the purpose of rendering scientific and methodical aid to states tackling cybercrime.

Article 184: Illegal Access to a Computer System

Article 184.1: Definition of Offense

1. A person commits the criminal offense of illegal access to a computer system when he or she accesses the whole or any part of a computer system without right.
2. For the purposes of Article 184, *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 data.

Commentary

Paragraph 1: The wording of this paragraph comes from Article 2 of the Convention on Cybercrime. For a discussion of the criminal offense of illegal access to a computer system, reference should be made to paragraphs 44–50 of the explanatory report to the Convention on Cybercrime. Paragraph 38 discusses the meaning of *without right*.

Paragraph 2: The wording of this paragraph comes from Article 1(a) of the Convention on Cybercrime. For a discussion of the meaning of *computer system*, reference should be made to paragraphs 23–24 of the explanatory report to the Convention on Cybercrime.

Article 184.2: Penalty

The applicable penalty range for the criminal offense of illegal access to a computer system is two to ten years' imprisonment.

Article 185: Illegal Interception of Computer Data

Article 185.1: Definition of Offense

1. A person commits the criminal offense of illegal interception of computer data when he or she:
   (a) without right; and
   (b) by technical means;
   (c) intercepts nonpublic transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.
2. For the purposes of Article 185:
   (a) *computer system* has the same meaning as in Article 184.1(2); and
   (b) *computer data* means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

Commentary

Paragraph 1: The wording of this paragraph comes from Article 3 of the Council of Europe Convention on Cybercrime. For a discussion of the criminal offense of illegal interception of computer data, reference should be made to paragraphs 51–59 of the

explanatory report to the Convention on Cybercrime. Paragraph 38 discusses the meaning of *without right*.

Paragraph 2(a): The wording of this paragraph comes from Article 1(a) of the Convention on Cybercrime. For a discussion of the meaning of *computer system*, reference should be made to paragraphs 23–24 of the explanatory report to the Convention on Cybercrime.

Paragraph 2(b): The wording of this paragraph comes from Article 1(b) of the Convention on Cybercrime. For a discussion of the meaning of *computer data*, reference should be made to Paragraph 25 of the explanatory report to the Convention on Cybercrime.

Article 185.2: Penalty

The applicable penalty range for the criminal offense of illegal interception of computer data is two to ten years' imprisonment.

Article 186: Interference with Computer Data

Article 186.1: Definition of Offense

1. A person commits the criminal offense of interference with computer data when he or she damages, deletes, deteriorates, alters, or suppresses computer data without right.
2. For the purposes of Article 186, *computer data* has the same meaning as in Article 185.1(2)(b).

Commentary

Paragraph 1: The wording of this paragraph comes from Article 4 of the Council of Europe Convention on Cybercrime. For a discussion of the criminal offense of data interference, reference should be made to paragraphs 60–64 of the explanatory report to the Convention on Cybercrime. Paragraph 38 discusses the meaning of the phrase *without right*.

Paragraph 2: The wording of this paragraph comes from Article 1(b) of the Convention on Cybercrime. For a discussion of the meaning of *computer data*, reference should be made to Paragraph 25 of the explanatory report to the Convention on Cybercrime.

Article 186.2: Penalty

The applicable penalty range for the criminal offense of interference with computer data is two to ten years' imprisonment.

Article 187: Interference with a Computer System

Article 187.1: Definition of Offense

1. A person commits the criminal offense of interference with a computer system when he or she:
   (a) without right;
   (b) seriously hinders the functioning of a computer system;
   (c) by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.
2. For the purposes of Article 187:
   (a) *computer system* has the same meaning as in Article 184.1(2); and
   (b) *computer data* has the same meaning as in Article 185.1(2)(b).

Commentary

Paragraph 1: The wording of this paragraph comes from Article 5 of the Convention on Cybercrime. For a discussion of the criminal offense of interference with a computer system, reference should be made to paragraphs 65–70 of the explanatory report to the Convention on Cybercrime. Paragraph 38 discusses the meaning of *without right*.

Paragraph 2(a): The wording of this paragraph comes from Article 1(a) of the Convention on Cybercrime. For a discussion of the meaning of *computer system*, reference

should be made to paragraphs 23–24 of the explanatory report to the Convention on Cybercrime.

Paragraph 2(b): The wording of this paragraph comes from Article 1(b) of the Convention on Cybercrime. For a discussion of the meaning of *computer data*, reference should be made to Paragraph 25 of the explanatory report to the Convention on Cybercrime.

Article 187.2: Penalty

The applicable penalty range for the criminal offense of interference with a computer system is two to ten years' imprisonment.

Article 188: Misuse of Devices

Article 188.1: Definition of Offense

1. A person commits the criminal offense of misuse of devices when he or she, without right and with the intent that a device be used for the purpose of committing the criminal offense of illegal access to a computer system (Article 184), illegal interception of computer data (Article 185), interference with computer data (Article 186), or interference with a computer system (Article 187):
   (a) produces, sells, procures for use, imports, distributes, or otherwise makes available:
      (i) a device, including a computer program, designed or adapted primarily for the purpose of committing the criminal offense of illegal access to a computer system (Article 184), illegal interception of computer data (Article 185), interference with computer data (Article 186), or interference with a computer system (Article 187); or
      (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with the intent to use; or
   (b) possesses any of the devices, passwords, access codes, or similar data referred to in Paragraphs 1(a)(i) and 1(a)(ii), above.

2. For the purposes of Article 188, *computer system* has the same meaning as in Article 184.1(2).

Commentary

Paragraph 1: For a discussion of the criminal offense of misuse of devices, reference should be made to paragraphs 71–78 of the explanatory report of the Convention on Cybercrime. Paragraph 38 discusses the meaning of the phrase *without right*.

Paragraph 2: For a discussion of the meaning of *computer system*, reference should be made to paragraphs 23–24 of the explanatory report of the Convention on Cybercrime.

Article 188.2: Penalty

The applicable penalty range for the criminal offense of misuse of devices is two to ten years' imprisonment.