www.coe.int/TCY

Strasbourg, 10 May 2015 T-CY (2015)03

Cybercrime Convention Committee (T-CY)

Assessing implementation of the Budapest Convention on Cybercrime

Questionnaire on Sanctions and Measures (Article 13)

[DRAFT for consideration by the 13th Plenary of the T-CY]

Background:

The purpose of the questionnaire is to allow the T-CY Plenary to assess the implementation of Article 13 of the Budapest Convention on Cybercrime by State Parties in line with Article 2 of the T-CY Rules of Procedure.

The Cybercrime Convention Committee (T-CY), in its 11th Plenary Session (17-18 June 2014) decided to dedicate the 3rd round of assessments to Article 13 (sanctions and measures). The 13th Plenary (2-3 December 2014 invited the Bureau to prepare a draft questionnaire for consideration by the 13th Plenary (June 2015).

Implementation:

T-CY representatives are invited to prepare/compile consolidated replies to this questionnaire from their respective country.

Replies should be submitted no later than **15 October 2015** in electronic form and in English or French to:

Alexander Seger, Executive Secretary of the Cybercrime Convention Committee, Council of Europe
Email: alexander.seger@coe.int

The Bureau will then provide an initial summary to T-CY 14 (December 2015), and a full draft report by March 2016 for consideration by T-CY 15 (June 2016).

1 Criminal sanctions

1.1 General provisions

Q 1.1.1 Please provide the text of your general provisions regarding criminal liability and sanctions

Intent, negligence/recklessness	
Aggravating/mitigating circumstances	
Requirements for suspension	
Minimum/maximum penalty	
Alternative or cumulative sanctions	
Multiple crimes, recidivism	
Incitement, aiding, abetting and attempt	
Other general provisions	

1.2 Criminal sanctions for natural persons

Q 1.2.1 Sanctions for illegal access to a computer system

Budapest Convention **Art. 2 Illegal access to a computer system**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum, maximum penalty	
Attempt	
Additional comments	

Q 1.2.2 Sanctions for illegal interception

Budapest Convention **Art. 3 Illegal interception**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.3 Sanctions for data interference

Budapest Convention **Art. 4 Data interference**	1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.4 Sanctions for system interference

Budapest Convention **Art. 5 System interference**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.5 Sanctions for misuse of devices

Budapest Convention **Art. 6 Misuse of Devices**	See appendix
Corresponding domestic provision:	
Intent, negligence/recklessness	

Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.6 Sanctions for computer-related forgery

Budapest Convention Art. 7 Computer-related forgery	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.7 Sanctions for computer-related fraud

Budapest Convention Art. 8 Computer-related fraud	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.8 Sanctions for computer-related fraud

Budapest Convention Art. 9 Child pornography	See appendix

Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.9 Sanctions for Offences related to infringements of copyright and related rights

Budapest Convention **Art. 10 Offences related to infringements of copyright and related rights**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.10 Are there any Domestic Guidelines for Judges while imposing certain criminal sanction, specifically for the crimes enshrined in Articles 2-11 of the Convention on Cybercrime?

Q 1.2.11 Does national legislation allow for using a combination of several criminal sanctions (e.g deprivation of liberty, fine,) against natural persons for crimes described in Articles 2-11 of the Convention on Cybercrime and under what circumstances?

1.3 Liability of legal persons

Q 1.3.1 Are legal persons liable for the crimes corresponding to those enshrined in Articles 2-11 of the Convention on Cybercrime?

Q 1.3.2 What are the corresponding applicable sanctions?

2 Other measures

2.1 Confiscation

Q 2.1.1 Does national legislation allow confiscation of the means that have been used to commit a criminal offence?

Q 2.1.2 What are the legal requirements?

Q 2.1.3 Does national legislation allow confiscation of the crime proceed, including from third persons?

Q 2.1.4 What are the legal requirements?

3 Statistics on sanctions and measures

Q 3.1.1 Please provide, if available data/statistics on sanction and measures

4 Case law

4.1 Typical examples of sanctions for natural persons

Q 4.1.1 Please provide examples of sanctions for natural persons? What have been average sanctions for natural persons? Suspended sentences, probation?

4.2 Typical examples of sanctions for legal persons

Q 4.2.1 Please provide examples of sanctions for legal persons? What have been average sanctions for legal persons?

4.3 Practice concerning confiscation

Q 4.3.1 What is the case law regarding confiscation?

Appendix: Extracts of the Budapest Convention on Cybercrime

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Explanatory Report

Sanctions and measures (Article 13)

128. This article is closely related to Articles 2-11, which define various computer- or computer-related crimes that should be made punishable under criminal law. In accordance with the obligations imposed by those articles, this provision obliges the Contracting Parties to draw consequences from the serious nature of these offences by providing for criminal sanctions that are 'effective, proportionate and dissuasive' and, in the case of natural persons, include the possibility of imposing prison sentences.

129. Legal persons whose liability is to be established in accordance with Article 12 shall also be subject to sanctions that are 'effective, proportionate and dissuasive', which can be criminal, administrative or civil in nature. Contracting Parties are compelled, under paragraph 2, to provide for the possibility of imposing monetary sanctions on legal persons.

130. The article leaves open the possibility of other sanctions or measures reflecting the seriousness of the offences, for example, measures could include injunction or forfeiture. It leaves to the Parties the discretionary power to create a system of criminal offences and sanctions that is compatible with their existing national legal systems.

Substantive criminal law provisions

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require

that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

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 intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.