www.coe.int/TCY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 3 December 2014 T-CY(2014)20

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #8

SPAM

Adopted by the 12th Plenary of the T-CY (2-3 December 2014)

Contact

Alexander Seger
Executive Secretary Cybercrime Convention Committee
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[1]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of spam. The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[2] This is to ensure that new forms of malware or crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to spam.

2 Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

Spam is often defined as unsolicited bulk email, where a message is sent to a significant number of email addresses, where the recipient's personal identity is irrelevant because the message is equally targeted at many other recipients without distinction.

There are separate issues relating to:

- the content of spam,
- the action of sending spam, and
- the mechanism used to transmit spam.

The content of spam may or may not be illegal, and where the content is illegal (such as offering fake medicines or fraudulent financial offerings) the offence may fall under the relevant national legislation for those offences. The action of transmitting spam (including bulk transmission of non-objectionable content) may be a civil or criminal offence in jurisdictions.

The Convention does not cover spam the contents of which is not illegal and does not cause system interference, but may be a nuisance to end-users.

The tools used to transmit spam may be illegal under the Budapest Convention, and spam may be associated with other offences not listed in the matrix below (see, for example, Article 7).

As with other guidance notes, each provision contains an intent standard ("without right", "with intent to defraud," etc). In some spam cases this intent may be difficult to prove.

[1] See the mandate of the T-CY (Article 46 Budapest Convention).

[2] Paragraph 36 of the Explanatory Report

3 T-CY interpretation of provisions addressing spam

Relevant Articles	Examples
Article 2 – Illegal access	Spam may contain malware that may access or enable access to a computer system.
Article 3 – Illegal interception	Spam may contain malware that may illegally intercept or enable the illegal interception of transmissions of computer data.
Article 4 – Data interference	Spam may contain malware that may damage, delete, deteriorate, alter or suppress computer data.
Article 5 – System interference	The transmission of spam may seriously hinder the functioning of computer systems. Spam may contain malware that seriously hinders the functioning of computer systems.
Article 6 – Misuse of devices	Devices as defined by Article 6 may be used for the transmission of spam. Spam may contain devices as defined by Article 6.
Article 8 – Computer-related fraud	Spam may be used as a device for input, alteration, deletion or suppression of computer data or interference with the functioning of a computer system for procuring illegal economic benefit.
Article 10 – Offences related to infringements of copyright	Spam may be used for advertising the sale of fake goods, including software and other items protected by copyright.
Article 11 – Attempt, aiding and abetting	Spam and the transmission of spam may be used to attempt or to aid or abet several crimes specified in the treaty (such as Article 7 on computer-related forgery or Article 8 on computer-related fraud).
Article 13 – Sanctions	Spam may serve multiple criminal purposes some of which have serious impact on individuals, or public or private sector institutions. Even if a Party does not criminalise spam *per se*, it should criminalise spam-related conduct such as the above offences, and it may consider aggravated circumstances. Parties should ensure, pursuant to Article 13, that criminal offences related to spam "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions.

4 T-CY statement

The above list of Articles illustrates the multi-functional criminal use of spam and spam-related offences.

Therefore, the T-CY agrees that these aspects of spam are covered by the Budapest Convention.

5 Appendix: Extracts of the Budapest Convention

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 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 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.

Article 11 – Attempt and aiding or abetting

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, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 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, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

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.