www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 19 February 2013 (draft for discussion) T-CY (2013) 6 E

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #2
Provisions of the Budapest Convention covering botnets

Proposal prepared by the Bureau
for comments by T-CY members and observers
and for consideration by the 9th Plenary of the T-CY (June 2013)

Comments on this draft Guidance Note should be sent to:

Alexander Seger	Tel	+33-3-9021-4506
Secretary Cybercrime Convention Committee	Fax	+33-3-9021-5650
Head of Data Protection and Cybercrime Division	Email	alexander.seger@coe.int
Directorate General of Human Rights and Rule of Law		
Council of Europe, Strasbourg, France		

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 botnets.

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 botnets.

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

The term 'botnet' may be understood to indicate:

> "a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'".[3]

Computers may be linked for criminal or good purposes.[4] Therefore, the fact that botnets consist of computers that are linked is not relevant. The relevant factors are that the computers in botnets are used without consent and are used for criminal purposes and to cause major impact.

Botnets are covered by the following sections of the convention, depending on what each botnet actually does. Each provision contains an intent standard ("without right", "with intent to defraud" etc.) which should be readily provable when botnets are involved.

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

[2] Paragraph 36 of the Explanatory Report

[3] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (com (2010) 517 final)

[4] Networks of computers may be created voluntarily for a criminal purpose. The crimes committed by such networks are covered by the Convention but are not discussed in this Note.

Relevant Articles	Examples
Article 2 – Illegal access	The creation and operation of a botnet requires illegal access to computer systems.[5] Botnets may be used to illegally access other computer systems.
Article 3 – Illegal interception	Botnets may use technical means to intercept non-public transmissions of computer data to, from, or within a computer system.
Article 4 – Data interference	The creation of a botnet always alters and may damage, delete, deteriorate or suppress computer data. Botnets themselves damage, delete, deteriorate, alter or suppress computer data.
Article 5 – System interference	Botnets may hinder the functioning of a computer system. This includes distributed denial of service attacks.[6]
Article 6 – Misuse of devices	All botnets are devices as defined in Article 6 because they are designed or adapted primarily to commit the offences established by Articles 2 through 5.[7] Programmes themselves that are used for the creation and operation of botnets also fall under Article 6. Therefore, Article 6 criminalizes the production, sale, procurement for use, import, distribution or otherwise making available as well as the possession of devices such as botnets or programmes used for their creation or operation.
Article7 – Computer-related forgery	Depending on the botnet's design, it may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Article 8 – Computer-related fraud	Botnets may cause one person to lose property and cause another person to obtain an economic benefit from the inputting, altering, deleting, or suppressing of computer data and/or interfering with the function of a computer system.
Article 9 – Child pornography	Botnets may distribute child exploitation materials.
Article 10 – Infringements related to copyrights and related rights	Botnets may illegally distribute data that is protected by intellectual property laws.
Article 11 – Attempt, aiding and abetting	Botnets may be used to attempt or to aid or abet several crimes specified in the treaty.

[5] See also Guidance Note 1 on the Notion of „Computer System"

[6] See separate Guidance Note.

[7] Parties that take reservations to Article 6 must still criminalize the sale, distribution or making available of devices covered by this Article.

Article 13 – Sanctions	Botnets serve multiple criminal purposes some of which have serious impact on individuals, on public or private sector institutions or on critical infrastructure. A Party may foresee, however, in its domestic law a sanction that is unsuitably lenient for botnet-related crime, and it may not permit the consideration of aggravated circumstances, attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Therefore, Parties should ensure, pursuant to Article 13, that criminal offences related to botnets "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. Parties may also consider aggravating circumstances, for example, if botnets affect a significant number of systems or attacks causing considerable damage, including deaths or physical injuries, or damage to critical infrastructure.[8]

3 T-CY statement

The above list of Articles related to botnets illustrates the multi-functional criminal use of botnets and applicable crimes.

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

[8] See also Article 10 draft EU Directive

4 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 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.

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.
