www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, version 16 May 2013 T-CY (2013)10

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #5

DDOS attacks

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Comments on this draft Guidance Note should be sent to: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
Secretary Cybercrime Convention Committee
Head of Data Protection and Cybercrime Division
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 denial of service (DOS) and distributed denial of service (DDOS) attacks.

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 DOS and DDOS attacks.

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

Denial of service (DOS) attacks are attempts to render a computer unavailable to users through a variety of means. These may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users. Distributed denial of service (DDOS) attacks are denial of service attacks executed by many computers at the same time. There are currently a number of common ways by which DOS and DDOS attacks may be conducted. They include, for example, sending malformed queries to a computer system; exceeding the capacity limit for users; and sending more e-mails to e-mail servers than the system can receive and handle.

DOS and DDOS attacks are covered by the following sections of the convention, depending on what each attack actually does. Each provision contains an intent standard ("without right", "with intent to defraud," etc) which should be readily provable in DOS and DDOS cases.

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

[2] Paragraph 36 of the Explanatory Report

3 T-CY interpretation of the criminalisation of DDOS attacks

Relevant Articles	Examples
Article 2 – Illegal access	DOS and DDOS attacks may access a computer system.
Article 4 – Data interference	DOS and DDOS attacks may damage, delete, deteriorate, alter or suppress computer data.
Article 5 – System interference	The objective of a DOS or DDOS attack is precisely to seriously hinder the functioning of a computer system.
Article 11 – Attempt, aiding and abetting	DOS and DDOS attacks may be used to attempt or to aid or abet several crimes specified in the treaty (such as Computer-related forgery, Article 7; Computer-related fraud, Article 8; Offences related to child pornography, Article 9; and Offences related to infringements of copyright and related rights, Article 10).
Article 13 – Sanctions	DOS and DDOS attacks may be dangerous in many ways, especially when they are directed against systems that are crucial to daily life - for example, if banking or hospital systems become unavailable. A Party may foresee in its domestic law a sanction that is unsuitably lenient for DOS and DDOS attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences related to such attacks "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 DOS or DDOS attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure.[3]

4 T-CY statement

The above list of Articles related to DOS and DDOS attacks illustrates the multi-functional criminal use of such attacks.

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

---

[3] See also Article 10 draft EU Directive

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 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 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.