www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 5 juin 2013 T-CY (2013) 6F Rev

Comité de la Convention Cybercriminalité (T-CY)

Note d'orientation n° 2 du T-CY
Dispositions de la Convention de Budapest visant les botnets

Adoptée lors de la 9ème réunion plénière du T-CY (4-5 juin 2013)

Contact

Alexander Seger
Secrétaire du Comité de la Convention sur la cybercriminalité
Chef de la Division Protection des données et cybercriminalité
Direction Générale des droits de l'homme et de l'Etat de droit
Conseil de l'Europe, Strasbourg, France,

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

1 Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies [1].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note traite de la question des botnets.

La convention « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »[2], et ce pour que de nouvelles formes de logiciels malveillants ou de délits soient toujours couvertes par la convention.

La présente note d'orientation montre dans quelle mesure différents articles de la convention s'appliquent aux botnets.

2 Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STE n° 185)

Le terme « botnet » peut désigner :

> « un groupe d'ordinateurs qui ont été contaminés par des logiciels malveillants (virus informatiques). Un tel réseau d'ordinateurs compromis ("zombies") peut être activé pour exécuter certaines actions, comme attaquer des systèmes d'information (cyberattaques). Les "zombies" peuvent être contrôlés, souvent à l'insu des utilisateurs de ces ordinateurs, par un autre ordinateur, également appelé "centre de commande et de contrôle" ».[3]

Des ordinateurs peuvent être reliés entre eux à des fins criminelles ou pour de bonnes causes[4]. Le fait que les botnets soient constitués d'ordinateurs reliés entre eux n'est donc pas un critère pertinent. L'élément essentiel est que les ordinateurs des botnets sont utilisés sans autorisation, à des fins criminelles et pour causer des dégâts majeurs.

Les botnets sont visés par certains articles de la convention, en fonction de l'action précise qu'ils accomplissent. Ces articles sont énumérés ci-dessous. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse », etc.), dont la preuve devrait être apportée sans difficulté en présence de botnets.

[1] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[2] Paragraphe 36 du rapport explicatif.

[3] Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre du Conseil 2005/222/JAI (COM (2010) 517 final).

[4] Des réseaux d'ordinateurs peuvent être sciemment créés à des fins criminelles. Les infractions commises par ces réseaux sont couvertes par la convention, mais ne sont pas examinées dans la présente note.

Article pertinent	Exemples
Article 2 – Accès illégal	La création et l'exploitation d'un botnet nécessitent un accès illégal à des systèmes informatiques[5]. Les botnets peuvent servir à accéder illégalement à d'autres systèmes informatiques.
Article 3 – Interception illégale	Les botnets peuvent utiliser des moyens techniques pour intercepter des transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique.
Article 4 – Atteinte à l'intégrité des données	La création d'un botnet altère toujours et peut endommager, effacer, dégrader ou supprimer des données informatiques. Les botnets eux-mêmes endommagent, effacent, dégradent, altèrent ou suppriment des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les botnets peuvent entraver le fonctionnement d'un système informatique, notamment au moyen d'attaques par déni de service distribué[6].
Article 6 – Abus de dispositifs	Les botnets sont tous des dispositifs relevant de la définition figurant à l'article 6, car ils sont conçus ou adaptés avant tout pour commettre les infractions visées aux articles 2 à 5[7]. Les programmes utilisés pour créer et exploiter des botnets entrent aussi dans le champ de l'article 6. Par conséquent, l'article 6 érige en infractions pénales la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mises à disposition des dispositifs que sont les botnets ou les programmes utilisés pour leur création ou leur exploitation.
Article 7 – Falsification informatique	Selon la façon dont il a été conçu, le botnet peut introduire, altérer, effacer ou supprimer des données informatiques, engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.
Article 8 – Fraude informatique	Les botnets peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 9 – Pornographie enfantine	Les botnets peuvent diffuser des contenus qui relèvent de l'exploitation d'enfants.
Article 10 – Atteinte à la propriété intellectuelle et aux droits connexes	Les botnets peuvent diffuser illégalement des données qui sont protégées par les lois relatives à la propriété intellectuelle.

[5] Voir également la note d'orientation n° 1 relative à la notion de « système informatique ».

[6] Voir la note d'orientation sur ce sujet.

[7] Les Parties qui émettent des réserves concernant l'article 6 doivent néanmoins toujours ériger en infraction pénale la vente, la diffusion ou la mise à disposition de dispositifs visés par ledit article.

Article 11 – Tentative et complicité	Les botnets peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans le traité ou pour se rendre complice de leur commission.
Article 13 – Sanctions	Les botnets sont utilisés à de multiples fins criminelles, dont certaines ont une incidence grave sur les personnes, les institutions publiques ou privées ou les infrastructures essentielles. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des infractions liées aux botnets soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées aux botnets « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les botnets portent atteinte à un nombre important de systèmes ou que les attaques causent des dégâts majeurs, y compris des décès, des blessures physiques ou l'endommagement d'infrastructures essentielles.

3 Déclaration du T-CY

La liste des articles concernant les botnets présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen des botnets et les dispositions pénales qui pourraient s'appliquer.

Par conséquent, le T-CY s'accorde à dire que les botnets, sous leurs différents aspects, sont couverts par la Convention de Budapest.

4 Annexe : Extraits de la Convention de Budapest

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.