www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 5 juin 2013 T-CY (2013)10F Rev

Comité de la Convention Cybercriminalité (T-CY)

Note d'orientation n° 5 du T-CY

sur les attaques DDOS

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

Contact:

Alexander Seger
Secrétaire du Comité de la Convention 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
Télécopie +33-3-9021-5650
Courriel 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'utilisation et la mise en œuvre effectives de la Convention de Budapest sur la cybercriminalité, compte tenu notamment des évolutions du droit, des politiques et des technologies[1].

Les notes d'orientation reflètent la vision commune de toutes les Parties quant à l'utilisation de la Convention.

La présente note est consacrée à la question des attaques par déni de service (DOS) et par déni de service distribué (DDOS).

La Convention de Budapest « 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 les nouvelles formes de logiciels malveillants ou d'infractions soient toujours couvertes par la Convention.

La présente note montre dans quelle mesure plusieurs articles de la Convention s'appliquent aux attaques DOS et DDOS.

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

Les attaques DOS visent à rendre un système informatique indisponible pour ses utilisateurs par divers moyens, dont la saturation des ordinateurs ou réseaux ciblés par des demandes de communication externes, qui ralentit l'accès au service pour les utilisateurs légitimes. Les attaques DDOS sont des attaques par déni de service exécutées par plusieurs ordinateurs en même temps. Il existe actuellement plusieurs manières de lancer des attaques DOS et DDOS, par exemple envoyer des requêtes incorrectes à un système informatique, dépasser le nombre maximal d'utilisateurs ou envoyer un nombre de courriers électroniques supérieur à celui que le serveur peut recevoir et traiter.

Les attaques DOS et DDOS sont visées par certains articles de la Convention, en fonction de ce qu'elles 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 cas d'attaque DOS ou DDOS.

---

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

[2] Paragraphe 36 du rapport explicatif.

3 Interprétation par le T-CY de la criminalisation des attaques DDOS

Articles pertinents	**Exemples**
Article 2 – Accès illégal	Par le biais des attaques DOS et DDOS il est possible d'accéder à un système informatique.
Article 4 – Atteinte à l'intégrité des données	Les attaques DOS et DDOS peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Une attaque DOS ou DDOS vise précisément à entraver gravement le fonctionnement d'un système informatique.
Article 11 – Tentative et complicité	Les attaques DOS et DDOS peuvent être utilisées pour tenter de commettre plusieurs des infractions spécifiées dans la Convention ou pour se rendre complice de leur commission (telles que la falsification informatique, article 7 ; la fraude informatique, article 8 ; les infractions se rapportant à la pornographie enfantine, article 9, et les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes, article 10).
Article 13 – Sanctions et mesures	Les attaques DOS et DDOS peuvent être dangereuses de multiples façons, en particulier lorsqu'elles sont dirigées contre des systèmes qui sont essentiels au quotidien – par exemple, si un système bancaire ou hospitalier est rendu indisponible. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des infractions liées aux attaques DOS et DDOS soit trop clémente et ne permette pas la prise en considération de 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 attaques DOS et DDOS « 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 pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques DOS ou DDOS portent atteinte à un nombre important de systèmes ou causent des dégâts majeurs, y compris des décès, des blessures physiques ou l'endommagement d'infrastructures essentielles.

4 Déclaration du T-CY

La liste des articles concernant les attaques DOS et DDOS présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

Par conséquent, le T-CY estime que les différents aspects de ces attaques sont couverts par la Convention de Budapest.

_____

5 Annexe : extraits de la Convention de Budapest

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.