www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 16 mai 2013 T-CY (2013)10

Comité de la Convention Cybercriminalité (T-CY)

Note d'orientation n°6 du T-CY

Attaques visant les infrastructures d'information critiques

Proposition établie par le Bureau
pour observations par les membres et les observateurs du T-CY
et pour examen lors de la 9e réunion plénière du T-CY (juin 2013)

Les remarques sur ce projet de note d'orientation devront être envoyés à :

Alexander Seger
Secrétaire du Comité de la Convention sur la cybercriminalité Tél +33-3-9021-4506
Chef de la Division Protection des données et cybercriminalité Fax +33-3-9021-5650
Direction générale des droits de l'homme et de l'Etat de droit Email alexander.seger@coe.int
Conseil de l'Europe, Strasbourg, France

1 Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention cybercriminalité (T-CY) a décidé de publier 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 est consacrée à la question des attaques visant les infrastructures d'information critiques.

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, afin 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 attaques visant les infrastructures d'information critiques.

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

Les infrastructures critiques désignent en général les systèmes et les actifs, physiques ou virtuels, indispensables à la vie d'un pays et dont l'arrêt ou la destruction aurait un effet dévastateur sur la sécurité, la sécurité économique, la santé ou la sûreté publiques ou n'importe quelle combinaison de ces éléments.[3] La définition des infrastructures critiques varie selon les pays. Toutefois, pour de nombreux pays, les infrastructures critiques englobent l'énergie, l'alimentation, l'eau, les combustibles, les transports, les communications, les finances et les secteurs des services publics.

Les infrastructures critiques sont souvent gérées par des systèmes informatiques, notamment ceux connus sous le nom de systèmes de contrôle industriels (SCI) ou de systèmes de télésurveillance et d'acquisition de données (SCADA). Ces systèmes sont généralement désignés sous le nom d'infrastructures d'information critiques.

Selon des sources privées et gouvernementales, un nombre important mais inconnu d'attaques visant des infrastructures d'information critiques se produit chaque année dans le monde entier. Ces attaques ont recours aux mêmes techniques que celles utilisées par la criminalité électronique. La

---

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

[2] Paragraphe 36 du Rapport explicatif

[3] Voir Directive 2008/114/CE du Conseil de l'Union européenne du 8 décembre 2008 : «Infrastructure critique : un point, système ou partie de celui-ci, situé dans les États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions. »

différence réside dans l'impact de ces attaques sur la société : elles peuvent retirer des fonds du Trésor public, interrompre l'approvisionnement en eau, perturber le contrôle du trafic aérien, etc.
Les formes d'attaques des infrastructures d'information critiques, actuelles et futures, sont visées par les articles de la convention figurant ci-dessous, en fonction de la nature de l'attaque. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse » etc.) dont les autorités devraient tenir compte au moment de qualifier un délit.

3 Interprétation par le T-CY de l'incrimination des attaques visant des infrastructures d'information critiques

Articles pertinents	**Exemples**
Article 2 – Accès illégal	Les attaques contre les infrastructures d'information critiques peuvent s'introduire dans un système informatique.
Article 3 –Interception illégale	Les attaques contre les infrastructures d'information critiques 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	Les attaques contre les infrastructures d'information critiques peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les attaques contre les infrastructures d'information critiques peuvent porter atteinte au fonctionnement d'un système informatique ; il pourrait en fait s'agir de leur objectif premier.
Article 7 – Falsification informatique	Les attaques contre les infrastructures d'information critiques peuvent 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 attaques contre les infrastructures d'information critiques 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 11 – Tentative et complicité	Les attaques contre les infrastructures d'information critiques peuvent être utilisées pour tenter de commettre des infractions spécifiées dans le traité ou pour se rendre complices de leur commission.
Article 13 – Sanctions	Les incidences des attaques contre les infrastructures d'information critiques sont multiples (elles peuvent varier selon les pays pour des raisons techniques, culturelles ou autres) mais les pouvoirs publics s'y intéressent généralement lorsqu'elles entrainent des préjudices graves ou de grande ampleur. Il est possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des attaques contre les infrastructures d'information critiques soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où l'éventuelle nécessité pour ces Parties d'envisager la modification de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à ces attaques « 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 attaques contre les infrastructures d'information critiques portent atteinte à un nombre important de systèmes ou provoquent des dégâts considérables, y compris des décès ou des blessures physiques. [4]

4 Déclaration du T-CY

La liste des articles concernant les attaques contre les infrastructures d'information critiques présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

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

_____

[4] Voir également l'article 10 de la Proposition de Directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JHA du Conseil (com (2010) 517 final).

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 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une 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 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de 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, qu'elles soient ou non

directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

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 de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques ;
b par toute forme d'atteinte au fonctionnement d'un système informatique,,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

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.