www.coe.int/TCY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, le 8 juillet 2019 T-CY(2019)4

Comité de la Convention sur la cybercriminalité (T-CY)

T-CY Note d'orientation #9
Aspects de l'ingérence électorale au moyen de systèmes informatiques couverts par la Convention de Budapest

Adoptée lors de la 21e réunion plénière du T-CY (8 juillet 2019)

Contact

Alexander Seger
Secrétaire exécutif du Comité de la Convention sur la cybercriminalité
Direction générale des droits de l'homme et de l'état de droit
Conseil de l'Europe, Strasbourg, France

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

1 Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention sur la 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.

L'ingérence dans les élections par des cyberactivités malveillantes ciblant les ordinateurs et les données utilisées lors des élections et des campagnes électorales compromet la tenue d'élections libres, équitables et régulières et sape la confiance dans la démocratie. Les opérations de désinformation, telles qu'elles sont vécues en particulier depuis 2016, peuvent recourir à de telles pratiques et avoir le même effet. Les procédures électorales nationales doivent être adaptées aux réalités de la société de l'information et les systèmes informatiques utilisés pour les élections et les campagnes électorales doivent être rendus plus sûrs.

Dans ce contexte, il faut redoubler d'efforts pour poursuivre ces ingérences lorsqu'elles constituent une infraction pénale : une réponse efficace de la justice pénale peut dissuader de se livrer à une ingérence électorale et rassurer l'électorat quant à l'utilisation des technologies de l'information et de la communication dans les élections.

La présente note traite de la manière dont les articles de la Convention peuvent s'appliquer aux aspects de l'ingérence électorale au moyen de systèmes informatiques.

Les infractions matérielles définies dans la Convention peuvent être commises en tant qu'actes d'ingérence électorale ou en tant qu'actes préparatoires facilitant cette ingérence.

En outre, les outils nationaux de procédure et d'entraide judiciaire internationale de la Convention sont disponibles aux fins d'enquêtes et de poursuites liées à l'ingérence électorale. La portée et les limites des pouvoirs procéduraux et des outils de coopération internationale sont définies par les articles 14.2 et 25.1 de la Convention de Budapest :

> Article 14.2
> 2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :
> a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;
> b à toutes les autres infractions pénales commises au moyen d'un système informatique ; et
> c à la collecte des preuves électroniques de toute infraction pénale.
>
> Article 25.1
> Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

Les pouvoirs et procédures énoncés dans la Convention sont soumis aux conditions et sauvegardes prévues à l'article 15.

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

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

2.1 Dispositions procédurales

Les pouvoirs et procédures énoncés dans la Convention (articles 14 à 21) peuvent être appliqués dans le cadre d'une enquête ou d'une procédure pénale spécifique dans tout type d'ingérence électorale, comme prévu à l'article 14.

Les mesures procédurales spécifiques peuvent être très utiles dans les enquêtes pénales pour ingérence électorale. Par exemple, dans ce type d'affaire, un système informatique peut être utilisé pour commettre ou faciliter une infraction, la preuve de cette infraction peut être stockée sous forme électronique, ou un suspect peut être identifiable grâce aux renseignements sur l'abonné, y compris une adresse IP. De même, le financement politique illégal peut être traçable par le biais de courriels préservés, les communications vocales entre conspirateurs peuvent être saisies à la suite d'une interception dûment autorisée, et le mauvais usage des données peut être illustré par des pistes électroniques.

Ainsi, dans les enquêtes pénales portant sur des infractions liées à l'ingérence électorale, les Parties peuvent faire usage de leur pouvoir d'ordonner la conservation rapide des données informatiques stockées et de leurs pouvoirs d'injonction de produire, de perquisition et de saisie de données informatiques stockées, ainsi que d'autres outils permettant la collecte de preuves électroniques aux fins d'investigations et de poursuite de telles infractions.

2.2 Dispositions relatives à l'entraide judiciaire internationale

Les pouvoirs prévus par la Convention en matière de coopération internationale (articles 23 à 35) sont d'une portée similaire et peuvent aider les Parties dans les enquêtes sur les ingérences électorales.

Ainsi, les Parties mettent en œuvre les actions requises – conservation rapide des données informatiques stockées, injonction de produire, perquisition et saisie de données informatiques stockées –, ainsi que d'autres dispositifs de coopération internationale.

2.3 Dispositions de droit pénal matériel

Enfin, comme on l'a vu plus haut, l'ingérence électorale peut concerner les types de comportement suivants (lorsqu'ils sont commis sans avoir de fondement légal), érigés en infraction pénale par la Convention sur la cybercriminalité. Le T-CY souligne que les agissements cités ne sont que de simples exemples – l'ingérence électorale est en effet un phénomène qui prend de l'ampleur et peut revêtir des formes multiples, non énumérées ci-dessous. Le comité estime néanmoins que la Convention sur la cybercriminalité est suffisamment souple pour y remédier.

Articles pertinents	**Exemples**
Article 2 – Accès illégal	Un système informatique peut être utilisé illégalement pour obtenir des informations sensibles ou confidentielles relatives à des candidats, des campagnes, des partis politiques ou des électeurs.
Article 3 – Interception	Lors de transmissions non publiques à destination, en provenance ou à

illégale	l'intérieur d'un système informatique, des données informatiques peuvent être interceptées illégalement pour obtenir des informations sensibles ou confidentielles relatives à des candidats, des campagnes, des partis politiques ou des électeurs.
Article 4 – Atteinte à l'intégrité des données	Les données informatiques peuvent être endommagées, effacées, détériorées, altérées ou supprimées pour modifier des sites internet, altérer les listes électorales ou falsifier les résultats des élections, par exemple en manipulant des machines à voter.
Article 5 – Atteinte à l'intégrité du système	Le fonctionnement des systèmes informatiques utilisés lors d'élections ou de campagnes électorales peut être entravé pour interférer avec les messages de la campagne, entraver l'inscription des électeurs, désactiver les dispositifs de vote ou empêcher le décompte des voix par des attaques en déni de service, des logiciels malveillants ou d'autres moyens.
Article 6 – Abus de dispositifs	La vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à un système informatique peuvent faciliter l'ingérence électorale (par exemple vol de données sensibles de candidats politiques, de partis ou de campagnes).
Article 7 – Falsification informatique	Des données informatiques (par exemple les données des listes électorales) peuvent être introduites, altérées, effacées ou supprimées, de sorte que des données non authentiques sont prises en compte ou utilisées à des fins légales comme si elles étaient authentiques. Par exemple, certains pays exigent que les campagnes électorales fassent l'objet d'une déclaration de situation financière publique. La falsification de données informatiques pourrait donner l'impression de divulgations inexactes ou cacher des sources douteuses de fonds de campagne.
Article 11 – Tentative et complicité	La tentative de commettre l'une quelconque des infractions définies dans le traité, ou tout acte de complicité par aide ou assistance, en vue d'exercer une ingérence électorale.
Article 12 – Responsabilité des personnes morales	L'une quelconque des infractions visées aux articles 2 à 11 de la Convention peut être commise, en vue d'exercer une ingérence électorale, par des personnes morales qui pourraient être tenues pour responsables en vertu de l'article 12.
Article 13 – Sanctions et mesures	Les infractions visées par la Convention peuvent constituer une menace pour les individus et la société, en particulier lorsque ces infractions sont dirigées contre les fondements de la vie politique, comme les élections. Les actes criminels et leurs effets peuvent différer d'un pays à l'autre, mais l'ingérence électorale peut miner la confiance dans les processus démocratiques, modifier le résultat d'une élection, obliger à organiser un second scrutin avec les coûts et les éventuels troubles que cela comporte, voire provoquer des violences physiques entre les partisans de la tenue d'élections et d'autres citoyens. Une Partie peut prévoir dans son droit interne une sanction trop clémente

	pour des actes visés aux articles 2 à 11 commis dans le cadre d'élections, et ne pas autoriser la prise en compte de circonstances aggravantes ou des notions de tentative et de complicité. Dans cette hypothèse, elle devrait envisager de modifier les dispositions pertinentes. Les Parties doivent veiller, conformément à l'article 13, à ce que les infractions pénales liées à de tels actes « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Les Parties peuvent également envisager des circonstances aggravantes, par exemple si de tels actes affectent de manière significative une élection ou causent des décès ou des dommages corporels ou des dégâts matériels importants.

3 Déclaration du T-CY

Le T-CY convient que les infractions matérielles définies dans la Convention sont également susceptibles de constituer des actes d'ingérence électorale tels que définis par le droit applicable, c'est-à-dire des agissements portant atteinte à la tenue d'élections libres, équitables et régulières.

Les infractions matérielles définies dans la Convention peuvent être commises dans le but de faciliter, participer à, ou préparer des actes d'ingérence électorale.

Les outils de procédure et d'entraide judiciaire de la Convention peuvent être utilisés pour enquêter sur l'ingérence électorale, sa facilitation et la participation à celle-ci, ou sur les actes préparatoires à ladite ingérence.