www.coe.int/TCY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, le 6 juin 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 visés par la Convention de Budapest

Projet établi par le Bureau pour examen par T-CY 21 (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

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

1 Introduction

Le Comité de la Convention sur la cybercriminalité (T-CY) a décidé, lors de sa 8e session plénière (décembre 2012), de publier des notes d'orientation visant à faciliter l'utilisation et la mise en œuvre efficaces de la Convention de Budapest sur la cybercriminalité, également à la lumière des développements juridiques, politiques et technologiques.[1]

Les Notes d'orientation représentent l'interprétation commune des Parties au présent traité en ce qui concerne l'utilisation de la Convention.

L'ingérence dans les élections par des attaques contre les ordinateurs et les données utilisées lors des élections et des campagnes électorales viole les règles visant à garantir des élections libres, justes et propres et des attaques et sape la confiance dans la démocratie. Les opérations de désinformation, telles qu'elles sont vécues en particulier depuis 2016, peuvent faire de même. Les règles électorales doivent être adaptées aux réalités de la société de l'information et les systèmes informatiques utilisés pour les élections et les campagnes électorales connexes 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 toute 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 pénales de fond prévues par 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 pour les enquêtes et les poursuites liées à l'ingérence électorale. La portée et les limites des pouvoirs et outils procéduraux en matière 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 ;
> 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 preuves sous forme électronique d'une infraction pénale.

Les pouvoirs procéduraux de la Convention sont soumis aux conditions et garanties de 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 de procédure

Les pouvoirs procéduraux de la Convention (articles 14 à 21) peuvent être utilisés dans le cadre d'une enquête ou d'une procédure pénale spécifique dans tout type d'ingérence électorale, comme le prévoit l'article 14.

Les mesures procédurales spécifiques peuvent être très utiles dans les enquêtes criminelles sur l'ingérence électorale. Par exemple, en cas d'ingérence électorale, 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 retraçable 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 criminelles sur l'ingérence électorale, les Parties peuvent utiliser la conservation accélérée des données informatiques stockées, les ordonnances de production, les perquisitions et saisies de données informatiques stockées et d'autres outils pour recueillir les preuves électroniques nécessaires aux enquêtes et aux poursuites relatives à ces infractions.

2.2 Dispositions relatives à l'entraide judiciaire internationale

Les pouvoirs de coopération internationale de la Convention (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 à disposition une conservation accélérée des données informatiques stockées, des ordonnances de production, des perquisitions et des saisies de données informatiques stockées, ainsi que d'autres dispositions relatives à la coopération internationale.

2.3 Dispositions de droit pénal matériel

Enfin, comme on l'a vu plus haut, l'ingérence électorale peut impliquer les types de comportement suivants, érigés en infraction pénale par la Convention sur la cybercriminalité. Le T-CY souligne que les exemples ci-dessous ne sont que des exemples - c'est-à-dire que, comme l'ingérence électorale est un phénomène en développement, elle peut apparaître sous de nombreuses formes non énumérées ci-dessous. Toutefois, le T-CY s'attend à ce que la Convention sur la cybercriminalité soit 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 ou des partis politiques.
Article 3 - Interception illégale	Les transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique peuvent être interceptées illégalement pour obtenir des informations sensibles ou confidentielles relatives à des candidats, des campagnes ou des partis politiques.

Article 4 - Atteinte à l'intégrité des données	Les données informatiques peuvent être endommagées, supprimées, détériorées, altérées ou supprimées pour diffuser des informations modifiées dans le cadre de campagnes de désinformation, pour modifier les bases de données des électeurs ou pour manipuler les résultats des votes 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, empêcher le dépouillement des votes ou empêcher le décompte des voix par des attaques par déni de service, des logiciels malveillants ou d'autres moyens.
Article 6 – Abus de dispositifs	La vente, l'acquisition pour utilisation, l'importation, la distribution ou d'autres actes mettant à disposition des mots de passe informatiques, des codes d'accès ou des données similaires permettant d'accéder à des systèmes informatiques peuvent faciliter l'ingérence électorale comme le vol de données sensibles de candidats politiques, de partis ou de campagnes.
Article 7 - Falsification informatique	Les données informatiques (par exemple les données utilisées dans les bases de données des électeurs) peuvent être saisies, modifiées, supprimées, de sorte que les données non authentiques sont considérées ou utilisées à des fins juridiques 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	Les crimes spécifiés dans le traité peuvent être tentés, aidés ou complices dans la poursuite de l'ingérence électorale.
Article 12 - Responsabilité des personnes morales	Les infractions visées aux articles 2 à 11 de la Convention en raison d'immixtions électorales peuvent être commises par des personnes morales qui seraient responsables en vertu de l'article 12.
Article 13 – Sanctions et mesures	Les crimes visés par la Convention peuvent constituer une menace pour les individus et la société, en particulier lorsque ces crimes sont dirigés contre les fondements de la vie politique, comme les élections. Les actions criminelles 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, nécessiter le coût et le bouleversement d'une deuxième élection ou provoquer des violences physiques entre les partisans électoraux et les communautés. Une Partie peut prévoir dans son droit interne une sanction qui n'est pas forcément indulgente à l'égard des actes liés aux élections visés aux articles 2 à 11, et elle ne peut permettre l'examen de circonstances aggravantes ou de tentative, d'aide ou de complicité. Cela peut signifier que les Parties doivent envisager d'apporter des amendements à leur législation nationale. Les Parties devraient 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, qui incluent la privation 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 matériels importants.

3 Déclaration du T-CY

Le T-CY convient que les infractions de fond prévues par la Convention peuvent également être des actes d'ingérence électorale au sens de la loi applicable, c'est-à-dire des infractions contre des élections libres, régulières et honnêtes.

Les crimes au sens de la Convention peuvent être commis dans le but de faciliter des actes d'ingérence électorale, d'y participer ou de préparer des actes d'ingérence électorale.

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