Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Résumé public de l'interrogatoire à huis clos classifié de : M^me^ Alia Tayyeb et M. Dan Rogers[1]

Des hauts fonctionnaires du **Centre de la sécurité des télécommunications (« CST »)** ont été interrogés par les avocats de la Commission au cours d'une audience à huis clos tenue le 5 mars 2024. Les témoins, Alia Tayyeb et Dan Rogers, ont été interrogés conjointement. Le procureur général du Canada était présent et a eu l'occasion d'interroger les témoins. Ceux-ci ont été entendus en l'absence du public et des autres Participants.

Notes aux lecteurs

- Les segments de texte entre crochets sont des notes explicatives fournies par les avocats de la Commission pour aider le lecteur.
- La rédaction du présent résumé s'appuie sur la sous-division (a)(iii)(C)(II) du mandat de la Commission. Ce résumé divulgue la preuve pertinente aux fins des divisions (a)(i)(A) et (B) du mandat de la Commission qui, selon la Commissaire, ne porterait pas préjudice aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale.
- Le présent résumé contient de l'information qui concerne les divisions (a)(i)(A) et (B) du mandat de la Commission. L'information fournie au cours de l'entrevue se rapportant à d'autres aspects du mandat de la Commission a été omise de ce résumé, mais pourrait être présentée en preuve par la Commission à un stade ultérieur des procédures.

[1] Traduction.

- Ce résumé doit être lu conjointement avec le rapport institutionnel non classifié du CST préparé par le gouvernement du Canada et le résumé non classifié de l'entrevue menée auprès des responsables du CST.

1. Interrogatoire effectué par les avocats de la Commission

[1] Chaque témoin a confirmé l'exactitude de la version classifiée du résumé de l'entrevue (également classifiée) menée auprès du CST, et l'a adoptée comme faisant partie de son témoignage devant la Commission. Le résumé a été déposé comme pièce au dossier de la Commission.

1.1 Rôles et responsabilités

[2] Chaque témoin a décrit les fonctions qu'il ou elle avait assumées au sein du CST à partir de 2018.

[3] M^me^ Tayyeb a commencé à travailler au CST en 2020 et a été nommée chef adjointe du **renseignement électromagnétique (« SIGINT »)** en 2022.

[4] M. Rogers a commencé à travailler au CST comme étudiant au début des années 2000. Il a été nommé chef adjoint du SIGINT en 2018 et sous-chef délégué du CST en 2022. Il a occupé ce poste jusqu'en 2023.

1.2 Renseignement électromagnétique (« SIGINT »)

[5] M. Rogers a décrit le renseignement électromagnétique comme la collecte de renseignement à partir de l'infrastructure mondiale de l'information (plus communément appelée Internet), par des moyens électroniques, pour le compte du gouvernement du Canada. M. Rogers et M^me^ Tayyeb ont ajouté que le CST n'est pas autorisé à diriger ses efforts de collecte vers des Canadiens ou à l'intérieur du pays.

1.3 Mandat et aspects du mandat

[6] M. Rogers et M^me^ Tayyeb ont expliqué que la cybersécurité est un aspect du mandat du CST. Le CST vise à défendre les systèmes du gouvernement du Canada ou d'autres systèmes d'importance contre les cybermenaces, qu'elles soient d'origine nationale ou

étrangère. M. Rogers a confirmé qu'en cas d'attaque, quelle qu'en soit la source, le CST adopterait une posture défensive pour contrer cette attaque.

[7] M. Rogers et M^me^ Tayyeb ont confirmé que le CST accepte la définition d'**ingérence étrangère (« IE »)** énoncée dans la *Loi sur le Service canadien du renseignement de sécurité*[2], bien que la collecte de renseignement du CST soit plus large que celle du **Service canadien du renseignement de sécurité (« SCRS »).** En effet, le CST s'intéresse à l'influence étrangère, un concept plus vaste que l'IE, ainsi qu'à d'autres activités malveillantes.

[8] M. Rogers a confirmé que la répression transnationale serait couverte par le mandat de collecte du CST.

[9] M. Rogers et M^me^ Tayyeb ont expliqué qu'en réponse à la Directive du Cabinet sur les priorités en matière de renseignement, le CST recueille du renseignement d'une manière conforme à son mandat, qui est de soutenir les objectifs du gouvernement. Un effort communautaire plus large vise à affiner la Directive du Cabinet pour établir des priorités précises que le CST peut opérationnaliser. M^me^ Tayyeb a expliqué que ces priorités évoluent au fil du temps et sont modifiées par un processus dirigé par le Bureau du Conseil privé (« BCP »). Ce processus attribue des niveaux aux priorités en matière de renseignement. Les témoins ont confirmé que l'IE était une priorité en ce qui concerne le renseignement au moment des élections fédérales de 2019 et de 2021.

[10] M^me^ Tayyeb a expliqué que le mandat du CST comporte cinq aspects.

a) **Le renseignement électromagnétique.** Le CST collecte du renseignement électromagnétique pour déterminer les motivations, les intentions et les capacités des entités étrangères.

b) **La cybersécurité et l'assurance de l'information.** Cet aspect concerne la défense des systèmes gouvernementaux du Canada et d'autres systèmes d'importance. M. Rogers a fait remarquer que le CST travaille en étroite

[2] L.R.C. 1985, chap. C-23

collaboration avec Élections Canada à la mise en place de mesures préventives pour protéger la cyberinfrastructure électorale.

c) **Les cyberopérations actives.** Le CST peut prendre des mesures pour perturber ou réduire les menaces étrangères en matière d'affaires internationales, de défense et de sécurité. Ces efforts visent généralement des menaces potentielles sur la scène internationale.

d) **Les cyberopérations défensives.** Le CST peut intervenir directement en cas de cyberattaque contre un réseau ou un système d'importance du gouvernement du Canada. M. Rogers et M^me^ Tayyeb ont expliqué que des cyberopérations défensives avaient été planifiées en prévision des élections de 2019 et de 2021. Elles n'ont toutefois pas dû être menées dans ces deux occasions. M. Rogers a expliqué que le **Centre canadien pour la cybersécurité (« Centre pour la cybersécurité »)** a surveillé avec vigilance les systèmes d'Élections Canada et d'autres réseaux connexes au cours des deux périodes électorales. M^me^ Tayyeb a fait remarquer que des acteurs hostiles étrangers tentent constamment de compromettre les réseaux du gouvernement canadien. Les deux témoins ont confirmé qu'aucune cyberattaque visant les réseaux électoraux n'a réussi, que ce soit lors des élections de 2019 ou de 2021.

e) **Le mandat d'assistance.** Le CST fournit une assistance opérationnelle et technique à d'autres organismes. Le CST est tenu d'agir dans le cadre du mandat et des pouvoirs de l'organisme qu'il assiste, plutôt qu'en fonction de son propre mandat. Lorsque le CST assiste un autre organisme, comme le SCRS, le renseignement qu'il recueille appartient au SCRS et non pas au CST. Le CST utilise parfois des techniques sensibles pour collecter du renseignement dans le cadre de son mandat d'assistance. Ces techniques sensibles peuvent faire l'objet de contrôles ou de conditions supplémentaires imposés par des partenaires en matière de renseignement.

derrière sont, de manière plus générale, dans la mire du CST, de telle sorte que l'IE est nécessairement comprise dans son mandat. Ainsi, lorsque le CST est en mesure de détecter une campagne orchestrée par un gouvernement étranger, menée de l'extérieur du Canada, cela relève de son mandat.

[20] Les témoins ont expliqué le rôle joué par le CST dans l'évaluation des données fournies par **Affaires mondiales Canada (« AMC »)** par l'intermédiaire du **Mécanisme de réponse rapide (« MRR »)** relativement à de possibles campagnes de désinformation ou de mésinformation en 2019 et 2021. Ils ont confirmé que peu avant l'élection de 2019, le CST avait été mandaté pour évaluer les données collectées par le MRR – en lien avec l'ingérence potentielle d'un État étranger dans les processus démocratiques canadiens au moyen des médias sociaux. Les témoins ont expliqué que le CST est parfois incapable d'évaluer les enquêtes de sources ouvertes du MRR. M. Rogers a précisé que lorsque le CST n'est pas en mesure d'obtenir certains détails techniques qui, souvent, ne sont pas accessibles au moyen de sources ouvertes, celui-ci ne peut pas attribuer de manière concluante une campagne en ligne à un État étranger.

[21] En réponse à la question de savoir si le CST avait enquêté sur les allégations selon lesquelles la RPC aurait mené une campagne dans les médias sociaux contre le Parti conservateur du Canada – à l'endroit d'Erin O'Toole et de Kenny Chiu en particulier – pendant la période électorale de 2021, M. Rogers a répondu que le CST était au courant de ces allégations en raison de sa participation au Groupe de travail. Il a souligné que le CST n'est pas autorisé à collecter du renseignement électromagnétique sur des Canadiens ou sur des personnes vivant au Canada qui publient des messages dans les médias sociaux, même lorsque ces messages sont publiés sur des plateformes étrangères telles que WeChat. M^{me} Tayyeb a ajouté que si AMC était en mesure de fournir au CST des adresses IP laissant croire que l'activité sur l'une de ces plateformes est d'origine étrangère, le CST aurait le pouvoir d'enquêter.