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

Complément au résumé d'entrevue: Administration de la Chambre des communes (Hedi Touati and Benoît Dicaire)

Les avocats de la Commission ont mené une entrevue avec Hedi Touati, directeur adjoint de la sécurité des technologies de l'information (« **TI** »), et Benoît Dicaire, dirigeant principal de l'information, le 17 septembre 2024. L'entrevue a eu lieu dans un environnement sécurisé et comportait des références à des informations classifiées. Le présent résumé divulgue la preuve qui, de l'avis de la Commissaire, ne porterait pas préjudice aux intérêts cruciaux du Canada ni de ses alliés, à la défense nationale ou à la sécurité nationale.

Notes aux lecteurs :

- Les segments de texte entre crochets sont des notes explicatives fournies par les avocats de la Commission pour aider le lecteur.

1. Organisation des Services numériques de la Chambre des communes

[1] M. Dicaire est le dirigeant principal de l'information aux Services numériques et biens immobiliers de la Chambre des communes (« **Services numériques** »).

[2] M. Touati a été nommé directeur adjoint, Sécurité des TI, de la Chambre des communes en 2019. En 2021, son poste relevait du dirigeant principal des technologies. M. Dicaire a indiqué qu'en 2023, les Services numériques ont procédé à une réorganisation interne. Le poste de dirigeant principal des technologies a été aboli, de telle sorte que le directeur adjoint de la sécurité des TI relève directement du dirigeant principal de l'information [M. Dicaire]. M. Dicaire a expliqué que cette réorganisation avait pour objectif de permettre aux Services numériques de faire face aux menaces croissantes et de continuer de s'acquitter de leur mandat avec efficacité.

Le poste de directeur adjoint a également été reclassifié au niveau directeur (officier principal de la sécurité de l'information).

2. Renseignement classifié et cybersécurité

[3] M. Dicaire a expliqué que le Sergent d'armes de la Chambre des communes est en relation directe avec le Service canadien du renseignement de sécurité (« **SCRS** »). Les Services numériques et le Centre canadien pour la cybersécurité (« **CCC** ») sont quant à eux parties à un protocole d'entente qui encadre le partage d'information. M. Dicaire a ajouté que le Sergent d'armes et les Services numériques s'échangent des informations de manière régulière. M. Dicaire a indiqué que les processus de transmission d'informations, tant entre le Sergent d'armes et les Services numériques qu'entre les Services numériques et le CCC, étaient efficaces.

[4] M. Touati a expliqué que les Services numériques de la Chambre des communes reçoivent du renseignement classifié à une fréquence variable, en fonction des incidents de cybersécurité et des menaces potentielles. Ce partage d'information favorise la coopération entre les agences de renseignement et la Chambre des communes. Le renseignement classifié est transmis verbalement, dans le cadre de rencontres dans des locaux isolés pour l'information sensible cloisonnée.

[5] M. Touati a ajouté que la transmission de renseignement dont la classification est plus basse (tel que le renseignement classifié Protégé B) est plus fréquente et s'effectue par courriel. Ce renseignement porte le plus souvent sur des questions de nature technique pour des besoins opérationnels.

[6] M. Touati a indiqué qu'il détient une autorisation de sécurité de niveau Très secret. Il a précisé que ce niveau de classification ne lui permet pas d'avoir accès aux informations classifiées dans des compartiments au-delà du niveau Très secret. Il a indiqué que, en raison de son mandat précis, l'Administration de Chambre des communes n'était pas un partenaire traditionnel des agences de renseignement et de sécurité dans ce domaine.

[7] M. Touati a dit que l'accès des Services numériques au renseignement repose sur le principe du « besoin de savoir » et correspond à son mandat, soit de protéger la Chambre des communes et les utilisateurs de son infrastructure informatique contre les cyber menaces. M. Touati a ajouté que les Services numériques n'ont pas le mandat ni les outils et ressources pour traiter et opérationnaliser le renseignement hautement classifié. Aussi, des mesures qu'ils prendraient de leur propre chef en s'appuyant sur des renseignements de cette nature pourraient compromettre les enquêtes et les sources des agences de sécurité nationale.

[8] Selon M. Touati, les renseignements reçus, principalement de nature technique, suffisent pour permettre à la Chambre des communes de déterminer si les mesures qu'elle met en place atténuent les risques. Ils permettent de plus au personnel de la Chambre de communes de comprendre l'apport qu'elle peut fournir afin de contribuer plus efficacement à défendre la Chambre des communes contre les menaces. M. Touati a souligné qu'une meilleure connaissance des moyens employés par les acteurs malveillants contribue à élargir les activités de la Chambre des communes afin de contrer les menaces. Une compréhension du contexte plus large dans lequel se déploient ces menaces est également utile pour des fins de surveillance et de continuité opérationnelles parlementaires.

[9] M. Touati a indiqué que la transmission d'informations entre les agences gouvernementales et les Services numériques est collaborative : les informations que reçoivent les Services numériques leur permettent de contrer les menaces sur les systèmes d'informations de la Chambre des communes et d'enquêter sur celles-ci, alors que les informations qu'ils transmettent aux agences gouvernementales leur permettent d'éclairer leurs propres enquêtes.

[10] M. Touati a indiqué que, dans le cadre de ces échanges, les Services numériques ne peuvent pas partager les informations des députés sans leur consentement préalable. Il n'y a pas de lien d'emploi entre la Chambre des communes et les députés, ces derniers sont indépendants de celle-ci et conservent le contrôle de leurs données.

3. Cyberattaque d'APT31 visant des parlementaires

[11] Les avocats de la Commission ont questionné les représentants de la Chambre des communes en lien avec la chronologie des événements intitulée *Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens*, préparée par le Centre de la sécurité des télécommunications[1].

[12] M. Touati a affirmé être le représentant de la Chambre des communes identifié comme le « Directeur, Sécurité des TI » dans cette chronologie. Il a toutefois précisé que ce titre était inexact, puisqu'il était en fait Directeur adjoint, Sécurité des TI à cette époque.

[13] M. Touati a affirmé être le représentant de la Chambre des communes ayant participé au breffage classifié du 17 février 2021 auquel participaient également des représentants du CCC et du SCRS. Lors de ce breffage, M. Touati a été informé que les agences gouvernementales soupçonnaient qu'un groupe d'acteurs informatiques malveillant soupçonné d'être affilié à la République populaire de Chine, surnommé APT31, serait responsable des activités détectées en janvier 2021 ciblant les comptes courriels de parlementaires. Il a également été informé des tactiques et des cibles historiques de cet acteur malveillant. M. Touati a expliqué qu'il était familier avec l'acteur malveillant identifié lors du breffage. Il s'agissait d'un acteur bien connu dans le monde de la cybersécurité, sous d'autres acronymes aussi.

[14] De son côté, M. Touati a partagé avec les représentants du CCC et du SCRS des informations techniques sur les systèmes d'informations de la Chambre des communes. Il a expliqué qu'aucune information ne démontrait que le système de protection de la Chambre des communes n'avait pas fonctionné adéquatement et qu'il n'avait pas bloqué les activités ciblant les parlementaires. De surcroît, ces activités visaient les adresses électroniques publiques des députés, lesquelles ne sont pas usuellement utilisées sur les appareils personnels de ces derniers et sont traditionnellement gérées

[1] [CAN.SUM.000027.001]

par leur personnel. Ainsi, même dans l'éventualité où la cyberattaque avait réussi, aucune information sensible sur les parlementaires n'aurait pu été recueillie.

[15] M. Touati a expliqué que son évaluation du risque représenté par la cyberattaque n'a pas été affectée par le breffage classifié du 17 février 2021. L'information obtenue ne démontrait pas en quoi l'évaluation des Services numériques, selon laquelle la cyberattaque avait échoué, était erronée. Dans ces circonstances, M. Touati n'était pas alarmé par le breffage classifié qu'il venait de recevoir. Selon lui, cette attaque n'avait rien d'extraordinaire. La Chambre des communes est fréquemment ciblée par des cyber acteurs malveillants.

[16] M. Touati a tout de même demandé à son équipe de mener des vérifications additionnelles pour s'assurer de ne rien manquer, notamment en remontant dans le temps et en élargissant la portée des vérifications déjà effectuées. M. Touati a qualifié cet exercice de diligence raisonnable. À la suite de ces démarches, le diagnostic initial à l'égard de cette cyberattaque est demeuré inchangé. M. Touati a indiqué qu'à ce jour, il ne disposait d'aucun renseignement qui permettrait de conclure que la cyberattaque avait compromis les informations de parlementaires.

[17] Les rencontres subséquentes énumérées dans la chronologie ont permis de poursuivre cet échange d'information entre l'équipe de M. Touati et le CCC. M. Touati a indiqué que la chronologie semblait généralement refléter la fréquence des rencontres auxquelles il a participé.

4. Changements en cybersécurité

[18] M. Dicaire a souligné deux changements en cours au sujet de la cybersécurité. Premièrement, dans le cadre du renouvellement de l'entente avec le CCC présentement en négociations, on cherche à améliorer les processus de collaboration pour contrer les cybermenaces qui revêtent un degré de gravité supérieur. Ce nouveau protocole visera à améliorer la réactivité de la Chambre des communes de même que

la collaboration et les interactions entre les deux entités dans les cas qui exigent une réponse rapide.

[19] Deuxièmement, M. Dicaire a exprimé le souhait que le CCC améliore le contenu de ses bulletins d'information aux Services numériques en ce a trait aux recommandations. Selon lui, les recommandations partagées dans les bulletins sont très techniques. Plus de contexte l'aiderait dans l'exécution de son mandat concernant la continuité des opérations parlementaires.

[20] Depuis environ le milieu de l'année 2023, M. Dicaire remarque une volonté croissante des agences gouvernementales de partager plus d'information. À titre d'exemples, M. Dicaire a fait allusion aux Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et aux parlementaires et à l'information transmise par Affaires Mondiales Canada relativement à la campagne de *Spamouflage* qui a ciblé les parlementaires à la fin de l'été 2023.