# Résumé du gouvernement du Canada pour la Commission sur l'ingérence étrangère

## Opérations par courriel de la RPC contre les parlementaires

*Le présent document a été préparé par le gouvernement du Canada pour l'Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux. Il est présenté en réponse à une demande expresse de la Commission d'enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux, qui souhaite obtenir le résumé non classifié de l'information portant sur ce sujet particulier. Il ne faut pas se fonder sur ce résumé pour comprendre toute autre question. Il repose sur le renseignement recueilli et évalué au cours d'une période donnée et ne reflète pas nécessairement l'entière connaissance que le gouvernement du Canada avait de cette question à quelque moment que ce soit. Le renseignement sous-jacent a été communiqué à la Commission. Le présent document contient des résumés et des passages caviardés qui retranchent du renseignement les éléments qui risqueraient de porter préjudice à la sécurité nationale et aux relations internationales. Sont également retranchées les activités, techniques, méthodes et sources de renseignement sensibles qui pourraient causer des préjudices, et le document respecte les lois canadiennes pertinentes. Par ailleurs, il n'énonce pas toutes les mises en garde ni toutes les limites qui figurent dans les documents classifiés originaux et ne précise pas le degré de fiabilité et de crédibilité du renseignement, puisque cela risquerait de divulguer de l'information préjudiciable.*

**RÉSUMÉ**

1. La cybermenace en provenance de la République populaire de Chine (RPC) est importante, tant en matière de volume que de complexité. Les agents de la RPC recourent à des techniques de cyberespionnage pour recueillir des informations qui leur procureront des avantages sur le plan économique et diplomatique, et ils cherchent fréquemment à obtenir de grands ensembles de données contenant de l'information personnelle, vraisemblablement dans le but de procéder à une analyse des données de masse et de profilage de cible. Bien que les systèmes du gouvernement du Canada aient été compromis par les auteurs de la cybermenace de la RPC à de nombreuses reprises ces dernières années, toutes les compromissions connues ont été traitées.

2. À titre d'autorité technique du gouvernement du Canada en matière de cybersécurité et d'assurance de l'information, le Centre de la sécurité des télécommunications (CST) offre des avis, des lignes directrices et des services pour aider à la protection des systèmes des ministères et organismes fédéraux, ainsi que d'autres systèmes désignés comme importants par le gouvernement du Canada.

3. Afin de protéger l'infrastructure du gouvernement du Canada, y compris la Chambre des communes, contre les menaces à la cybersécurité, et de réagir à celles-ci, les directions générales du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) et du SIGINT du CST travaillent de concert pour s'acquitter des mandats du CST en matière de cybersécurité et d'assurance de l'information[1]. Dans le cadre de son mandat en matière

[1] Il convient de souligner que, dans le présent résumé, on fait référence à la Chambre des communes, et non aux députés.

de renseignement étranger, le CST peut recueillir des renseignements conformes aux priorités du Canada en matière d'information afin de découvrir des incidents de cybersécurité commis par un acteur étranger et mettant en cause une victime canadienne. Un processus officiel de nettoyage existe par lequel un résumé NON CLASSIFIÉ ou SECRET de ces renseignements peut être produit pour fournir aux victimes potentielles de cyberincidents les renseignements techniques nécessaires pour évaluer et atténuer les menaces.

4. L'équipe de gestion des incidents du Centre pour la cybersécurité reçoit des rapports d'incidents provenant de diverses sources, y compris du SIGINT et de la Direction générale de la cyberdéfense du Centre pour la cybersécurité. L'équipe de Gestion des incidents et coordination opérationnelle (GICO) du Centre pour la cybersécurité envoie ensuite de l'information non classifiée tirée de ces rapports aux équipes de sécurité des TI des éventuelles entités victimes. En tant que responsable des systèmes, le destinataire peut ensuite utiliser ces renseignements pour effectuer sa propre évaluation de la situation, puis faire un suivi auprès du Centre pour la cybersécurité s'il a besoin de soutien supplémentaire. Les organisations ne sont pas tenues de fournir de la rétroaction, mais elles peuvent participer à un échange d'information avec le Centre pour mieux comprendre la menace et les mesures d'atténuation possibles.

5. Les services offerts par le CST comprennent le déploiement, sur demande (et avec l'autorisation ministérielle), de capteurs au niveau du réseau, de capteurs au niveau du nuage et de capteurs au niveau de l'hôte afin de détecter les cyberactivités malveillantes sur les systèmes qu'ils protègent. Ces mesures de défense bloquent en moyenne 6,6 milliards de tentatives malveillantes par jour dirigées contre les réseaux du gouvernement du Canada, et offrent au CST du renseignement sur la cybermenace qu'il transmet à ses clients pour contribuer à contrer les cybermenaces, y compris en assurant le suivi des campagnes de courriels de pistage.

6. Les auteurs de cybermenaces utilisent des liens de pistage pour tenter de faire ouvrir par le destinataire un courriel contenant une image ou un autre lien (soit un lien de traçage) qui permet une connexion à un serveur contrôlé par un auteur de menace. Celui-ci peut alors confirmer la validité des adresses de courriel ciblées et recueillir des données préliminaires à propos des utilisateurs, notamment l'appareil utilisé et l'information de réseau local. Ces courriels peuvent être annonciateurs d'activités de traçage de la part de l'auteur de menace.

**Renseignements additionnels sur les activités malveillantes ciblant les systèmes parlementaires**

7. En janvier 2021, le CST a informé les employés de la sécurité des TI de la Chambre des communes d'activités malveillantes ciblant les systèmes parlementaires; on a plus tard déterminé qu'il s'agissait d'une campagne de courriels de pistage ciblant les comptes de courriel des parlementaires.

8. Entre janvier et avril 2021, le CST et le Service canadien du renseignement de sécurité (SCRS) ont rencontré des employés de la sécurité des TI de la Chambre des communes, et le CST a transmis au moins 12 rapports contenant des indicateurs techniques de compromissions touchant les systèmes de TI de la Chambre des communes.

9. Le 17 février 2021, le CST a présenté un exposé de niveau SECRET aux responsables de la sécurité des TI de la Chambre des communes, y compris au directeur de la Sécurité des TI. L'exposé du CST a été présenté par des experts en la matière du CST en présence de représentants du SCRS. L'exposé portait principalement sur l'auteur de menaces désigné sous le nom d'APT31[2]. Les pays, les tactiques et les catégories de cibles qui ont toujours intéressé les auteurs de menaces, comme les politiciens américains et canadiens, ont été explicitement communiqués. À la fin de l'exposé, la Chambre des communes a été invitée à communiquer au Centre pour la cybersécurité du CST tout renseignement sur les menaces provenant de ses réseaux qui permettrait à ce dernier de fournir de l'aide pour repérer les activités malveillantes et les atténuer.

10. Les rapports d'information fournis par le Centre pour la cybersécurité à la Chambre des communes au sujet de ces événements ont fait l'objet d'instructions de traitement indiquant que les renseignements communiqués dans les rapports ne peuvent être transmis qu'aux responsables de la défense des réseaux ou de l'analyse des cybermenaces au sein du ministère visé ou de l'organisation concernée, et qu'ils doivent être accompagnés d'un énoncé concernant ces restrictions. Les destinataires peuvent demander l'autorisation du CST s'ils souhaitent transmettre des informations provenant d'un rapport rédigé par le CST, mais aucune demande de ce genre n'a été reçue. Le Centre pour la cybersécurité et la Chambre des communes ont travaillé ensemble pour contrecarrer la tentative de compromission des auteurs de cybermenaces de la RPC.

**Actions menées après l'exposé du 17 février 2021**

11. L'événement de cybersécurité mené par le groupe APT31 en 2021 a permis au CST de tirer trois « leçons » en ce qui concerne la réponse à la menace en cours, lesquelles ont directement déterminé la manière dont le CST et la Chambre des communes répondent désormais aux questions de cyberdéfense.
    i. Immédiatement après la réunion du 17 février avec la Chambre des communes, les représentants du CST à l'interne se sont dit préoccupés par le fait que la

[2] Une menace persistante avancée (MPA, ou APT en anglais) est un auteur ou un groupe sophistiqué possédant la capacité de mener une cyberactivité malveillante avancée et soutenue, souvent dans le but de conserver un accès constant au réseau de la victime. L'organisation APT31 est un regroupement d'agents du renseignement, de pirates informatiques contractuels et de membres du personnel de soutien qui réalisent des cyberopérations malveillantes pour le compte de la RPC.

Chambre des communes n'avait pas reçu suffisamment d'information pour saisir l'importance de la menace. Ces préoccupations ont été transmises aux principaux membres de la direction du CST. Bien que le directeur de la Sécurité des TI de la Chambre des communes ait reçu une copie de la plupart des communications échangées entre le Centre pour la cybersécurité et l'équipe de la Sécurité des TI de la Chambre des communes, des moyens de communication plus officiels ont depuis été mis en place pour améliorer les procédures. En fin de compte, cette situation a abouti à une renégociation du protocole d'entente existant entre le CST et la Chambre des communes, ainsi qu'à la tenue régulière de réunions pour discuter d'incidents et de services potentiels.

ii. On a également déterminé que la coordination interne et globale pouvait être renforcée afin d'assurer une communication efficace entre les équipes travaillant à la résolution d'incidents tels que l'activité du groupe APT31 ciblant la Chambre des communes. Par exemple, une réunion quotidienne de coordination sur place concernant la lutte contre les menaces du groupe APT31 a été mise en œuvre à la fin de février 2021. Depuis, celle-ci a été remplacée par la création, en novembre 2021, d'une Unité de cyberincident nationale plus large, qui comprend notamment des représentants de la GRC, du SCRS et du MDN.

iii. Les représentants du CST ont également collaboré avec les équipes de la Chambre des communes pour s'assurer que cette dernière adopte la gamme complète des mesures offertes par le programme de cybersécurité du CST afin de mieux se défendre contre les cybermenaces et de réagir à celles-ci. En outre, afin de mieux gérer les événements liés à la cybersécurité, on procède actuellement à la mise à jour d'un protocole d'entente liant le CST et la Chambre des communes.

12. En novembre 2021, le SCRS a également transmis un exposé analytique classifié à 35 clients du gouvernement du Canada à propos des campagnes de courriels de traçage ciblant des membres de l'Alliance interparlementaire sur la Chine par des auteurs de la cybermenace de la RPC, APT31.

13. Une chronologie détaillée des événements liés à cette campagne et à la réponse opérationnelle figure à **l'onglet A.**