NON CLASSIFIÉ

Centre de la sécurité des télécommunications

Partie C
Rapport institutionnel à l'Enquête publique sur l'ingérence étrangère

Juin 2024

Le CST et l'ingérence étrangère en un coup d'œil

Le Centre de la sécurité des télécommunications (CST) est l'organisme de renseignement électromagnétique étranger ainsi que l'autorité technique en matière de cybersécurité et d'assurance de l'information au Canada. Le CST intercepte et analyse des communications électroniques étrangères pour fournir des informations uniques au gouvernement du Canada au sujet des menaces étrangères contre la sécurité et la prospérité du Canada, ainsi que des connaissances importantes à l'appui de l'exécution des politiques étrangères et des prises de décisions connexes.

Les auteures et auteurs étatiques hostiles tentent par différents moyens, dont l'espionnage, les cyberactivités malveillantes et la désinformation en ligne, d'influencer et de perturber la société et la démocratie du Canada. Pour les contrer, il faut adopter une approche pangouvernementale à laquelle le CST participe activement en :

- prenant tous les moyens dont il dispose en vertu des volets de son mandat (renseignement étranger, cybersécurité, cyberopérations étrangères et assistance technique et opérationnelle) pour contrer les activités hostiles d'auteures et auteurs étatiques;
- offrant du renseignement étranger aux décisionnaires du gouvernement du Canada sur les intentions, les moyens et les activités des auteures et auteurs de menace étrangers;
- participant au Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GT MSRE);
- protégeant les infrastructures électorales fédérales du Canada contre les cyberactivités malveillantes;
- aidant, à titre préventif, les institutions démocratiques à renforcer leur cybersécurité;
- transmettant des évaluations des menaces non classifiées au public;
- communiquant de l'information aux Canadiennes et Canadiens pour les aider à :
    - repérer la désinformation,
    - protéger leur confidentialité et sécurité en ligne.

Depuis les élections fédérales de 2015, le CST s'assure que des mesures de cyberdéfense robustes et efficaces sont en place pour protéger les systèmes d'Élections Canada et d'autres organisations qui appuient les processus démocratiques du pays. En raison de son expérience liée à la surveillance des activités d'ingérence, l'organisme a produit de nombreux rapports sur les risques que représente l'ingérence étrangère contre le processus démocratique du Canada et sur les moyens de le protéger de ces menaces.

Pour en savoir plus, veuillez consulter les rapports institutionnels du CST datant de septembre 2023 et de janvier 2024.

1. Liste et description de toutes les principales occurrences d'ingérence étrangère soupçonnée ciblant les processus démocratiques du Canada, dont un résumé, les dates, la cible, le pays concerné, les joueurs clés, le flux d'information et toute mesure prise.

La réponse sera fournie séparément.

2. Liste et description de tous les moyens dont dispose chaque ministère et organisme fédéral afin de détecter, de décourager et de contrer les activités d'ingérence étrangère, y compris tout changement à ces moyens ou leur évolution.

2.1 Aperçu du mandat

Avant août 2019, le mandat du CST était régi en trois volets par la *Loi sur la défense nationale*, soit :

A. acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
B. fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
C. fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.

Après l'adoption de la *Loi sur le CST* le 1er août 2019, les trois volets se sont transformés en cinq volets. Les articles 15 à 20 de la *Loi sur le CST* définissent le mandat du CST :

- renseignement étranger (article 16);
- cybersécurité et assurance de l'information (article 17);
- cyberopérations défensives (article 18);
- cyberopérations actives (article 19);
- assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, aux Forces armées canadiennes et au ministère de la Défense nationale (article 20).

Le CST reconnaît que l'ingérence étrangère représente une menace constante à laquelle est confronté le Canada, et ce, en dehors des périodes électorales également. Tous les volets du mandat du CST contribuent à l'approche pangouvernementale visant à détecter, à décourager et à contrer les activités telles que l'ingérence étrangère, l'espionnage et les cyberactivités malveillantes.

2.1.1 Renseignement étranger (article 16)

Le volet du mandat touchant le renseignement étranger permet au CST de mener des activités de renseignement électromagnétique (SIGINT pour *signals intelligence*). Le SIGINT consiste à intercepter, à décoder et à analyser des communications et d'autres signaux électroniques dans le but de recueillir du renseignement concernant des entités étrangères. Les activités de SIGINT reposent sur les priorités en matière de renseignement du gouvernement du Canada, établies par le Cabinet, et sur la Directive ministérielle sur les priorités en matière de renseignement, ces priorités portant notamment à l'ingérence étrangère. Le renseignement étranger recueilli par le CST et sur lequel il fait rapport fournit de l'information aux décisionnaires sur les activités, les intentions et les intérêts de diverses entités étrangères.

Le CST tire actuellement parti de trois autorisations ministérielles (AM) pour appuyer ses activités de renseignement étranger. Ces autorisations se distinguent les unes des autres par le type de technique d'acquisition qu'elles autorisent, et non par le type de

renseignement étranger recherché. Toutes trois appuient la capacité du CST à acquérir une grande variété de renseignement étranger, y compris, mais sans s'y limiter, le renseignement étranger en lien avec l'ingérence étrangère. Les détails de ces AM sont fournis dans l'annexe classifiée de la question 5.

2.1.2 Cybersécurité et assurance de l'information (article 17)

Le volet du mandat touchant la cybersécurité et l'assurance de l'information permet au CST de fournir des avis, des conseils et des services liés à la cybersécurité afin d'aider à défendre les systèmes fédéraux et les systèmes non fédéraux désignés par la ou le ministre de la Défense nationale comme étant d'importance pour le gouvernement du Canada (systèmes d'importance). Par exemple, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) du CST déploie des capteurs sur les points terminaux (comme des serveurs, des portables ou des ordinateurs de bureau), qui peuvent détecter automatiquement des activités malveillantes, comme des maliciels, et offrir une protection contre les cybermenaces.

Il y a actuellement trois AM utilisées par le CST pour répondre au volet de son mandat touchant la cybersécurité et l'assurance de l'information. Une d'entre elles permet de protéger les systèmes fédéraux, tandis que les deux autres permettent de protéger les systèmes d'importance. Toutes trois autorisent la prestation de certains services de cybersécurité sur les systèmes fédéraux ou sur les systèmes d'importance afin de les protéger contre les menaces à la cybersécurité de toutes les origines. Les détails de ces AM sont fournis dans l'annexe classifiée de la question 5.

C'est en vertu du volet du mandat touchant la cybersécurité que le CST fournit des avis et des conseils aux partis politiques, à la population canadienne et à l'électorat durant les périodes électorales. Tout particulièrement, le CST a fourni des avis et de l'aide à Élections Canada durant les élections de 2019 et de 2021 (plus de détails à la question 4). Le CST a également fourni des avis et des conseils aux partis politiques, en plus d'offrir une ligne d'assistance, pendant les élections. Plus d'information se trouve à la section 2.3.3 du rapport institutionnel du CST datant de janvier 2024, ainsi qu'à la question 7 du présent rapport institutionnel.

2.1.3 Cyberopérations défensives (article 18)

Les cyberopérations défensives (COD) permettent au CST de prendre des mesures en ligne afin de protéger les infrastructures canadiennes contre les cybermenaces étrangères en perturbant ces activités. Pendant les élections de 2019 et de 2021, le CST était prêt à entreprendre des cyberopérations défensives afin de protéger les systèmes d'Élections Canada, au besoin.

Le CST tire actuellement parti d'une AM autorisant des activités de COD. Les détails de cette AM sont fournis dans l'annexe classifiée de la question 5.

2.1.4 Cyberopérations actives (article 19)

Les cyberopérations actives (COA) permettent au CST de prendre des mesures en ligne afin de perturber les capacités de menaces étrangères contre le Canada.

Le CST tire actuellement de trois AM pour appuyer ses activités de COA. Les détails de ces AM sont fournis dans l'annexe classifiée de la question 5.

2.1.5 Assistance technique et opérationnelle (article 20)

En ce qui a trait au volet de son mandat touchant l'assistance technique et opérationnelle, le CST fournit une assistance aux organismes fédéraux chargés de l'application de la loi et de la sécurité, aux Forces canadiennes et au ministère de la Défense nationale. Lorsqu'il mène des activités dans le cadre d'une demande d'assistance, le CST doit respecter les restrictions et les autorisations légales de l'organisme demandeur, comme un

mandat délivré par un tribunal. En vertu de ce volet de son mandat, le CST peut aider ses partenaires nationaux à contrer ou à repérer l'ingérence étrangère.

3. Liste et description de toutes les propositions de politiques, de tous les plans législatifs et de toutes les demandes de ressources en lien avec l'ingérence étrangère, y compris, mais sans s'y limiter, les notes de service à la ou au sous-ministre (ou l'équivalent) ou à la ou au sous-ministre adjoint (ou l'équivalent). Au minimum, il faut fournir la date de la demande, la date de la décision (le cas échéant), le résumé des changements proposés et le résultat de la demande.

De septembre 2018 jusqu'à maintenant, le CST a participé à l'élaboration de mémoires au Cabinet, de présentations au Conseil du Trésor et de propositions budgétaires officielles ayant un lien avec l'ingérence étrangère, ou a dirigé de telles initiatives, dans le contexte de la protection des institutions et des processus démocratiques du Canada. Toutefois, il n'est pas possible de fournir le contenu et les détails connexes, étant donné que ces informations divulgueraient des documents confidentiels du Cabinet.

Les récents budgets fédéraux ont affecté des ressources au CST à l'appui de son vaste mandat, qui comprend des activités qui appuient directement ou indirectement l'atténuation, la perturbation ou la prévention de l'ingérence étrangère et/ou la protection de la démocratie. Par exemple :

Dans le budget de 2018 était annoncé un investissement de 507,7 millions de dollars sur 5 ans et de 108,8 millions de dollars par année suivante, afin de financer la Stratégie nationale de cybersécurité axée sur trois objectifs :

1. Assurer la sécurité et la résilience des cybersystèmes canadiens en renforçant la capacité du gouvernement du Canada d'enquêter sur les cybercrimes, d'élaborer des évaluations de la menace, d'assurer la sécurité des infrastructures essentielles et de collaborer avec les secteurs des finances et de l'énergie en vue de renforcer leur cybersécurité;
2. Permettre d'investir dans un écosystème cybernétique novateur et adapté en soutenant les placements en apprentissage cybernétique intégrés au travail pour les étudiantes et étudiants et en aidant les entreprises à améliorer leur posture de cybersécurité par la création d'un programme volontaire de cyberattestation;
3. Renforcer le leadership, la gouvernance et la collaboration en prenant l'initiative, au pays comme à l'étranger, pour faire avancer la cybersécurité au Canada, en collaborant étroitement avec les partenaires provinciaux, territoriaux et du secteur privé et des partenaires internationaux de confiance.

- Cet investissement **comprenait 155,2 millions de dollars sur 5 ans, et 44,5 millions de dollars par année suivante, pour que le CST crée un nouveau Centre canadien pour la cybersécurité (Centre pour la cybersécurité)**, une source unifiée de conseils de spécialistes, d'avis, de services et de soutien sur des questions opérationnelles de cybersécurité. Ainsi, les Canadiennes et Canadiens ainsi que les entreprises peuvent compter sur une source bien établie et fiable de conseils sur la cybersécurité.
- Ces investissements ont un lien avec l'ingérence étrangère, car les États étrangers cherchent à utiliser l'infrastructure mondiale de l'information afin de servir leurs objectifs stratégiques au détriment des intérêts nationaux et de la sécurité du Canada. Les adversaires étrangers utilisent de plus en plus des cyberoutils dans le but de cibler les processus démocratiques partout dans le monde. La désinformation est devenue omniprésente durant les élections nationales, et les adversaires utilisent dorénavant l'intelligence artificielle (IA) générative pour créer et propager du faux contenu, ce qui représente une menace pour les processus démocratiques.
- C'est pourquoi une connectivité sécurisée et fiable est essentielle, car elle est à la base de la prestation des services et systèmes critiques, comme les soins de santé, les transactions

financières, le transport sécuritaire, les communications d'urgence et la démocratie. Le Centre pour la cybersécurité du CST favorise la cyberrésilience du Canada, qui renforce la capacité de résister à l'ingérence étrangère et de la contrer.

- Le Centre pour la cybersécurité a par la suite été créé le 1er octobre 2018, et est aujourd'hui une source d'expertise pour toutes les questions de cybersécurité, y compris d'ingérence étrangère. Notamment, le Centre pour la cybersécurité dirige la publication aux deux ans de l'évaluation des cybermenaces contre le processus démocratique du Canada, qui informe les Canadiennes et Canadiens et renforce la résilience afin de contrer de telles activités malveillantes.

Le budget de 2018 a également annoncé 225 millions de dollars sur 4 ans, et 62,1 millions de dollars par la suite, afin de préserver la capacité canadienne de renseignement électromagnétique étranger.

- Le pouvoir du CST de recueillir du renseignement électromagnétique étranger aide à éclairer le gouvernement du Canada sur les questions de sécurité, de défense nationale et d'affaires internationales, en fonction des priorités établies par le gouvernement.
- Combattre l'ingérence étrangère et protéger la démocratie du Canada comptent parmi ces priorités.
- Le renseignement électromagnétique étranger offre au gouvernement du Canada un aperçu des plans, des intentions et des capacités des auteures et auteurs étatiques (ou leurs mandataires) visant à mener des activités d'ingérence ou d'influence contre les intérêts canadiens.

Dans le budget de 2019 était annoncé un investissement de 4,2 millions de dollars sur trois ans à compter de l'année financière 2019-2020 en vue d'offrir des conseils et des avis en cybersécurité aux partis politiques canadiens et aux responsables de l'administration électorale, dans le cadre de mesures plus vastes visant à renforcer et à protéger davantage les institutions démocratiques du Canada.

- Advenant la compromission des cybersystèmes utilisés par les partis politiques ou des cybersystèmes appuyant le travail des responsables de l'administration électorale, la confiance du public envers les processus électoraux courrait le risque d'être perturbée ou ébranlée.
- Afin de renforcer la sécurité des cybersystèmes utilisés par les partis politiques canadiens et par les responsables de l'administration électorale, le CST offre des conseils, des avis et des services techniques. Ceux-ci peuvent comprendre :
    - l'examen de l'architecture réseau et la prestation d'avis;
    - l'examen de sécurité des demandes de propositions en matière de TI;
    - l'évaluation des fournisseurs de services tiers en cybersécurité qui respectent une liste de normes clés en matière de sécurité des TI, ainsi que la prestation de conseils connexes.
- Le CST travaille également étroitement avec Élections Canada afin de protéger son infrastructure, ainsi qu'avec les principaux partis politiques pour améliorer leurs connaissances en matière de cybersécurité. Pour ce faire, il offre notamment des séances d'information, des ressources de formation, des consultations et des conseils personnalisés.

Dans le budget de 2022 était annoncé un investissement de 875,2 millions de dollars sur 5 ans, à compter de 2022-2023, et 238,2 millions de dollars par année suivante pour des mesures supplémentaires visant à gérer l'évolution rapide des cybermenaces. Ces mesures comprennent notamment :

- 263,9 millions de dollars sur 5 ans, à compter de 2022-2023, et 96,5 millions de dollars par année suivante pour renforcer la capacité du CST à lancer des cyberopérations pour prévenir et contrer les cyberattaques;

- 180,3 millions de dollars sur 5 ans, à compter de 2022-2023, et 40,6 millions de dollars par année suivante pour améliorer la capacité du CST à prévenir les cyberattaques contre les infrastructures essentielles et à y réagir;
- 178,7 millions de dollars sur 5 ans, à compter de 2022-2023, et 39,5 millions de dollars par année suivante afin d'élargir la protection de la cybersécurité pour les petits ministères, les organismes et les sociétés d'État;
- 252,3 millions de dollars sur 5 ans, à compter de 2022-2023, et 61,7 millions de dollars par année suivante pour permettre au CST de rendre les systèmes gouvernementaux essentiels plus résilients aux cyberincidents.

Le milieu universitaire compte certaines des chercheuses et certains des chercheurs les plus éminents dans les technologies émergentes et perturbatrices, y compris l'informatique quantique et l'intelligence artificielle. Il est possible de tirer parti de cette expertise afin de s'assurer que la collectivité de la sécurité et du renseignement du Canada garde une longueur d'avance sur ses adversaires.

- Le budget de 2022 annonçait également un investissement de 17,7 millions de dollars sur 5 ans, à compter de 2022-2023, et 5,5 millions de dollars par année suivante jusqu'en 2031-2032 pour que le CST établisse un programme unique de chaires de recherche en vue de financer des universitaires pour qu'ils mènent des recherches sur des technologies de pointe pertinentes aux activités du CST. Les chercheuses et chercheurs qui recevront ces subventions répartiront leur temps entre la recherche publiée examinée par les pairs et la recherche classifiée au CST.

Dans le budget de 2024 était annoncé un investissement de 917,4 millions de dollars sur 5 ans, et 145,8 millions de dollars par année suivante pour que le CST et Affaires mondiales Canada (AMC) améliorent leurs programmes de renseignement et de cyberopérations afin de protéger la sécurité économique du Canada et de réagir aux menaces à la sécurité nationale en constante évolution.

4. Liste et description de tous les arrangements et engagements (y compris les protocoles d'entente) avec les ministères et les organismes fédéraux et avec les partenaires internationaux, qui ont pour objectif de détecter, d'empêcher et de contrer les activités d'ingérence étrangère, en indiquant les dates auxquelles les arrangements sont en vigueur.

Les arrangements les plus étroits du CST en matière de renseignement sont avec d'autres organismes de renseignement des pays constituant la collectivité des cinq, c'est-à-dire les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. Bien qu'il n'ait pas indiqué d'ententes précises avec ses partenaires de la collectivité des cinq concernant l'ingérence étrangère, le CST continue de collaborer avec ses partenaires pour détecter les menaces courantes et s'en protéger, notamment l'ingérence étrangère contre les institutions et les processus démocratiques.

Les protocoles d'entente (PE) internationaux du CST avec d'autres pays ne font pas référence à la détection, à l'empêchement ou à la prévention des activités d'ingérence étrangère, car ils sont plutôt axés sur l'échange d'informations, de savoir-faire et de technologies de manière plus générale. Par conséquent, il n'existe pas d'arrangements ou d'engagements officiels entre le CST et ses partenaires internationaux portant précisément sur l'ingérence étrangère; toutefois, le CST et ses partenaires peuvent retirer des avantages à collaborer sur cette priorité commune.

Le CST continue de participer au Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GT MSRE) afin de détecter les menaces étrangères qui cherchent à s'ingérer dans les institutions et les processus démocratiques du Canada. Plus d'information sur la participation du CST au GT MSRE a été fournie à la section 2.3.1 du rapport institutionnel du CST de janvier 2024.

Le Centre pour la cybersécurité a relevé un arrangement ou engagement entre le CST et Élections Canada qui est concerné par la présente demande.

4.1 Arrangements ou engagements avec Élections Canada

À l'appui des 43e et 44e élections générales, le CST a mis sur pied des activités afin de coordonner et fournir les ressources du Centre pour la cybersécurité pour offrir des avis, des conseils et des outils de cyberdéfense à Élections Canada. Plus d'information sur ces activités a été fournie à la section 2.3.3 du rapport institutionnel du CST de janvier 2024.

Le groupe de travail sur les opérations de cyberdéfense (GT OCD) est un partenariat entre le Centre pour la cybersécurité et Élections Canada. L'objectif du GT OCD est d'offrir un cadre opérationnel pour l'échange d'information quant à la cybersécurité et pour la gestion des événements de cybersécurité (y compris les cybermenaces, les vulnérabilités ou les incidents de sécurité) qui ont une influence sur les élections générales ou qui les menacent.

Après les 44e élections générales, Élections Canada et le Centre pour la cybersécurité ont entamé une série de rencontres du GT OCD tous les deux mois afin d'appuyer la posture opérationnelle entre les élections générales d'Élections Canada, de mettre en œuvre les leçons tirées des 44e élections générales et de fournir des avis et des conseils sur les initiatives et enjeux émergents, d'envergure et à long terme d'Élections Canada en matière de cybersécurité.

Comparativement aux réunions du GT OCD organisées durant les élections générales, qui sont nécessairement de nature plus opérationnelle et tactique, le forum actuel du GT OCD permet à Élections Canada et au Centre pour la cybersécurité de collaborer sur le plan stratégique bien en avance sur les prochaines élections générales.

4.2 Autres activités

Le Centre pour la cybersécurité appuie les efforts continus en vue de créer de la cyberrésilience dans les activités économiques, de recherche et d'investissement au Canada. Bien qu'elles ne soient pas conçues précisément pour détecter, décourager ou contrer l'ingérence étrangère, ces activités, tout comme l'ensemble des autres activités de cybersécurité du Centre pour la cybersécurité, appuient indirectement cet objectif en améliorant la posture de cybersécurité globale des systèmes d'importance.

5. Liste et description de toutes les demandes de mandat liées à l'ingérence étrangère soumises au ministre de la Sécurité publique et des autorisations ministérielles soumises à la ou au ministre de la Défense nationale, en indiquant la date de soumission à la ou au ministre, la date d'approbation, la date de décision par la Cour fédérale et, le cas échéant, les raisons de cette décision.

5.1 Évolution des autorisations ministérielles entre la *Loi sur la défense nationale* et la *Loi sur le CST*

Le régime des autorisations ministérielles (AM) existe depuis 2001 à la suite de l'adoption de la partie V.1 de la *Loi sur la défense nationale* (LDN), et il a été transféré à la *Loi sur le Centre de la sécurité des télécommunications* (*Loi sur le CST*) en 2019. Le régime de la LDN prévoyait l'émission d'autorisations par la ou le ministre de la Défense nationale lorsque des activités de renseignement étranger et de cybersécurité du CST risquaient d'intercepter des communications privées.

La *Loi sur le CST* a modernisé le régime d'autorisations. Bien que le régime précédent était axé sur l'interception de communications privées, le régime de la *Loi sur le CST* exige que le CST obtienne une autorisation pour les activités de renseignement étranger et de cybersécurité si ces activités risquent de contrevenir à une loi fédérale ou de concerner l'acquisition d'information dans ou par l'entremise de l'infrastructure mondiale de l'information qui entre en conflit avec l'attente raisonnable de protection en matière de vie privée d'une Canadienne, d'un Canadien ou d'une personne au Canada. De plus, il a établi la norme à respecter afin d'obtenir une

autorisation auprès de la ou du ministre, c'est-à-dire des motifs raisonnables de croire qu'il est raisonnable et proportionnel d'accorder l'autorisation considérant la nature des activités et de ses objectifs. La *Loi sur le CST* a également ajouté un autre élément important au régime, soit que les autorisations de renseignement étranger et de cybersécurité accordées par la ou le ministre ne sont valides qu'une fois que la ou le commissaire au renseignement (CR), une partie indépendante et quasi judiciaire, les approuve.

5.2 Processus d'approbation des autorisations ministérielles

Les AM sont des instruments accordés par la ou le ministre de la Défense nationale (MDN), qui donnent au CST les pouvoirs de mener des activités à l'appui de son mandat qui risqueraient de contrevenir à une loi fédérale ou qui pourraient entrer en conflit avec l'attente raisonnable en matière de protection de la vie privée d'une Canadienne, d'un Canadien ou d'une personne au Canada.

Les AM sont valides pour une durée maximale d'un an. Les AM doivent démontrer ce qui suit :

- l'objectif des activités est raisonnable et proportionnel;
- l'information ne peut pas raisonnablement être obtenue d'une autre manière (c.-à-d. que l'activité est nécessaire);
- l'information ne sera pas conservée plus longtemps que ce qui est nécessaire;
- des mesures sont en place pour protéger la vie privée des Canadiennes, des Canadiens et des personnes se trouvant au Canada.

Les AM accordées en vertu des articles 16 (renseignement étranger) et 17 (cybersécurité) du mandat du CST doivent être examinées par la ou le CR. Une fois qu'une trousse d'AM est approuvée par la ou le ministre de la Défense nationale, les documents connexes sont envoyés à la ou au CR aux fins d'examen. La ou le CR examine les conclusions de la ou du MDN pour déterminer si elles sont raisonnables et remet sa décision d'approuver, de ne pas approuver ou d'approuver partiellement les activités décrites dans l'AM.

Toute cyberopération étrangère nécessite une AM. Les AM accordées en vertu de l'article 18 (cyberopérations défensives) du mandat du CST doivent faire l'objet d'une consultation auprès de la ou du ministre des Affaires étrangères. Les AM accordées en vertu de l'article 19 (cyberopérations actives) du mandat du CST doivent être approuvées par la ou le ministre des Affaires étrangères.

Plus d'information sur le processus d'AM a été fournie à la section 1.3.1 du rapport institutionnel du CST de janvier 2024.

La liste détaillée des AM se trouve à l'annexe classifiée de la question 5 (A5).

6. Liste et description des dates, des personnes participantes et du contenu résumé des discussions pour toutes les rencontres des cadres supérieures et supérieurs (au niveau des sous-ministres adjointes et sous-ministres adjoints ou plus élevé, y compris les ministres) avec des représentantes et représentants de gouvernements étrangers (en particulier la Chine, la Russie et l'Inde), lors desquelles la question de l'ingérence étrangère a été soulevée.

Les relations les plus étroites en matière d'échange de renseignement qu'entretient le CST sont avec les pays qui forment la collectivité des cinq, c'est-à-dire les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. Le CST tire parti de l'expertise collective de ce groupe pour répondre aux exigences en matière de renseignement étranger du Canada afin de protéger ses intérêts nationaux et sa population.

De plus amples renseignements sont disponibles à l'annexe classifiée de la question 6 (A6).

7. Liste et description de toutes les campagnes d'éducation à l'intention des parlementaires et des membres de leur personnel, des partis politiques, du personnel des gouvernements fédéral et provinciaux et des administrations municipales, des diasporas ou du grand public en lien avec l'ingérence étrangère.

En tant qu'autorité technique du Canada en matière de cybersécurité, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) est la source unifiée de conseils spécialisés, d'avis, de services et de soutien à l'intention des Canadiennes, des Canadiens et des organisations canadiennes. Les ressources éducatives suivantes peuvent aider à atténuer les risques associés aux cybermenaces visant les élections et contribuer à la protection des institutions et des processus démocratiques du Canada.

Pour en savoir plus, veuillez consulter la page Web sur les cybermenaces contre les élections[1].

7.1 Rapports sur les cybermenaces contre le processus démocratique du Canada

Le Centre pour la cybersécurité fait rapport des cybermenaces visant les processus démocratiques du Canada dans le but d'informer les Canadiennes et les Canadiens des tendances mondiales quant aux activités de cybermenace visant les élections nationales et les potentielles répercussions sur le Canada.

Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023

> **Description :** La plus récente version du rapport sur les *Cybermenaces contre le processus démocratique du Canada*, qui actualise les rapports de 2021 et de 2019. Plus précisément, ce rapport aborde les activités de cybermenace visant les élections, ainsi que la menace croissante que représente l'IA générative pour les processus démocratiques mondiaux et canadiens.
>
> **Public cible :** Grand public
>
> **URL :** https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023

Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021

> **Description :** Il s'agit de la troisième version de la publication du CST, intitulée *Cybermenaces contre le processus démocratique du Canada.* Le document se penche sur les tendances mondiales entourant les cybermenaces contre les processus démocratiques (qui comprennent l'électorat, les partis politiques et les élections) et examine la menace qui pèse sur le Canada, particulièrement les répercussions de la pandémie de COVID-19.
>
> **Public cible :** Grand public
>
> **URL :** https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

Le point sur les cybermenaces contre le processus démocratique du Canada en 2019

> **Description :** Il s'agit de la deuxième version de la publication du CST, intitulée *Cybermenaces contre le processus démocratique du Canada.* Cette mise à jour porte principalement sur les activités de cybermenace entreprises par des adversaires étrangers dans le but de s'ingérer dans le processus démocratique.
>
> **Public cible :** Grand public
>
> **URL :** https://www.cyber.gc.ca/fr/orientation/le-point-sur-les-cybermenaces-contre-le-processus-democratique-du-canada-en-2019

[1] https://www.cyber.gc.ca/fr/orientation/cybermenaces-elections

7.2 Publication d'orientation et de formation — Cybermenaces contre les élections

Le Centre pour la cybersécurité est déterminé à sensibiliser aux cybermenaces ciblant le Canada et à protéger l'intégrité des élections canadiennes. La liste suivante est composée de documents de formation et d'orientation conçus pour atténuer les répercussions des cybermenaces contre les élections, notamment en ce qui a trait aux membres des partis politiques, à l'électorat et aux organismes électoraux.

7.2.1 Orientation et formation publiées pour les partis politiques

Guide de cybersécurité à l'intention des équipes chargées des campagnes électorales

Description : Ce guide présente en profondeur des conseils pratiques et de l'orientation sur la cybersécurité qui s'applique à toutes les campagnes électorales.

Public cible : Partis politiques

URL : https://www.cyber.gc.ca/fr/orientation/guide-de-cybersecurite-lintention-des-equipes-chargees-des-campagnes-electorales

Facteurs à considérer lors de l'utilisation des médias sociaux dans votre organisation

Description : Ce document montre comment l'environnement de médias sociaux qui change rapidement révèle de nouveaux risques et défis. Il mentionne que toutes les parties prenantes devraient être informées du contexte de la menace en évolution et des mesures de sécurité nécessaires à la protection de leurs activités dans les médias sociaux.

Public cible : Partis politiques

URL : https://www.cyber.gc.ca/fr/orientation/facteurs-considerer-lors-de-lutilisation-des-medias-sociaux-dans-votre-organisation

7.2.2 Orientation et formation publiées à l'intention de l'électorat

Repérer les cas de mésinformation, désinformation et malinformation

Description : Ce document explique comment repérer les cas de mésinformation, de désinformation et de malinformation (MDM) et énumère les mesures de sécurité que les consommatrices, les consommateurs et les organisations peuvent prendre pour les contrer. Plus précisément, on souligne la manière dont l'IA peut être utilisée lors d'élections afin de propager de la MDM dont le but est de fragiliser la confiance du public envers les institutions et de discréditer les figures publiques.

Public cible : Grand public — Électorat

URL : https://www.cyber.gc.ca/fr/orientation/reperer-les-cas-de-mesinformation-desinformation-et-malinformation-itsap00300

Piratage psychologique

Description : Ce document explique le fonctionnement des attaques par piratage psychologique, aussi appelées « piratage humain » puisque les auteures et auteurs de menace mettent à profit les renseignements qu'ils trouvent sur Internet et les plateformes de médias sociaux pour cibler des individus et des organisations. Ils peuvent tenter d'influencer les internautes pour les contraindre de faire quelque chose qui leur permettra d'accéder à leur environnement, comme changer le mot de passe d'un compte.

Public cible : Grand public — Électorat

URL : https://www.cyber.gc.ca/fr/orientation/piratage-psychologique-itsap00166

7.2.3 Orientation et formation publiées à l'intention des organismes électoraux

Conseils en matière de cybersécurité à l'intention des organismes électoraux

Description : Le document présente les menaces courantes qui pèsent sur les processus électoraux du Canada et des conseils sur la façon de protéger les personnes et les systèmes associés à ces processus.

Public cible : Grand public – Organismes électoraux

URL : https://www.cyber.gc.ca/fr/orientation/conseils-en-matiere-de-cybersecurite-lintention-des-organismes-electoraux-itsm10020

Guide de cybersécurité à l'intention des organismes électoraux

Description : Ce guide de cybersécurité a pour objet de fournir des orientations aux organismes électoraux afin de les aider à prévoir et à atténuer les menaces propres aux processus démocratiques du Canada, et à y réagir. Il décrit les mesures de cybersécurité de base et les pratiques exemplaires qu'il convient de mettre en œuvre afin d'améliorer le profil de sécurité des organismes. Il établit également une série de normes auxquelles les organismes électoraux peuvent se référer pour continuer de renforcer les systèmes actuels et en mettre en place de nouveaux.

Public cible : Grand public — Organismes électoraux

URL : https://www.cyber.gc.ca/fr/orientation/guide-de-cybersecurite-lintention-des-organismes-electoraux-itsm10021

Prévenir les attaques par déni de service distribué et s'y préparer

Description : Les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) sont des cyberattaques au cours desquelles les auteures et auteurs de menace cherchent à perturber l'accès à un système, à un service, à un site Web ou à une application en réseau et à empêcher les utilisatrices et utilisateurs légitimes d'y accéder. Cette publication donne des conseils sur les mesures qu'il est possible de prendre lorsque survient une attaque par DDoS et ce qu'il faut faire pour en atténuer les répercussions.

Public cible : Grand public — Organismes électoraux

URL : https://www.cyber.gc.ca/fr/orientation/prevenir-attaques-deni-service-distribue-sy-preparer-itsap80110

Facteurs à considérer en matière de cybersécurité pour votre site Web;

Description : Ce document présente des pratiques exemplaires en matière de cybersécurité que les organisations devraient intégrer à la conception et à l'entretien de leur site Web.

Public cible : Grand public — Organismes électoraux

URL : https://www.cyber.gc.ca/fr/orientation/facteurs-considerer-en-matiere-de-cybersecurite-pour-votre-site-web-itsm60005

Reconnaître les courriels malveillants

Description : C'est en se familiarisant avec les courriels malveillants et les attaques par hameçonnage que l'on peut aider à protéger l'information de son organisation.

Public cible : Grand public – Organismes électoraux

URL : https://www.cyber.gc.ca/fr/orientation/reconnaitre-les-courriels-malveillants-itsap00100

Guide sur les rançongiciels

Description : Les renseignements contenus dans ce document visent à informer les organisations et à les aider à dresser le portrait des risques liés aux attaques par rançongiciel, à réduire les conséquences de ces attaques et à prendre des mesures préventives pour les contrer. Ce document est divisé en deux parties : (1) comment se protéger contre les rançongiciels et (2) comment se remettre d'un rançongiciel.

Public cible : Grand public — Organismes électoraux

URL : https://www.cyber.gc.ca/fr/orientation/guide-sur-les-rancongiciels-itsm00099

Rançongiciels : comment les prévenir et s'en remettre

Description : Un rançongiciel est un type de maliciel qui bloque l'accès aux fichiers ou aux systèmes jusqu'à ce que l'utilisatrice ou utilisateur verse une somme d'argent. Cette publication donne des conseils pour aider les organisations à se préparer à faire face à une attaque par rançongiciel et à se rétablir après coup.

Public cible : Grand public – Organismes électoraux

URL : https://www.cyber.gc.ca/fr/orientation/rancongiciels-comment-les-prevenir-et-sen-remettre-itsap00099

7.2.4 Orientation et formation publiées à l'intention des fonctionnaires

Lutter contre la désinformation : guide à l'intention des fonctionnaires

Description : Ce guide, créé par l'École de la fonction publique du Canada avec le soutien du CST et d'autres ministères fédéraux, vise à présenter un aperçu de la désinformation, de la façon dont la menace croissante affecte les institutions démocratiques et de la façon de repérer la désinformation touchant les programmes, les politiques et les services fédéraux, et d'y réagir.

Public cible : Personnel du gouvernement du Canada — Fonctionnaires

URL : https://www.canada.ca/fr/institutions-democratiques/services/proteger-institutions-democratiques/lutter-contre-desinformation-guide-intention-fonctionnaires.html

Cybermenaces contre le processus démocratique du Canada : Présentation pour le Comité consultatif des partis politiques

Description : Cette présentation a été offerte conjointement avec le Service canadien du renseignement de sécurité (SCRS) lors de la réunion annuelle du Comité consultatif des partis politiques (CCPP), organisée par Élections Canada le 8 septembre 2023, au Palais des congrès de Gatineau, au Québec.

Public cible : Personnel du gouvernement du Canada — Élections Canada, partis politiques membres du CCPP

Noms des fichiers :

- (U) « Foreign Interference: Briefing to Parliamentarians » — [PBH_CAN043117]
- (U) « Foreign Interference: A threat to Canada's National Security » — [TS_CAN014638]

- (U) « Cyber Threats to Canada's Democratic Process: Presentation to the Advisory Committee for Political Parties (ACPP) » — [PBH_CAN015062]
- (U) « Cybermenaces contre le processus démocratique du Canada : Présentation pour le Comité consultatif des partis politiques » — [PBH_CAN015006]

Hypertrucages et IA générative : Changer le contexte des menaces pour la cybersécurité

Description : Le Centre pour la cybersécurité offre des séances d'information éducatives sur l'IA générative et les hypertrucages aux membres du personnel d'AMC dans le cadre de la Semaine de la sensibilisation à la cybersécurité 2024. L'objectif de la présentation est d'informer les employées et employés d'AMC sur les cybermenaces liées l'IA générative, comme les modèles de langage de grande taille (LLM pour *large language models*) et les technologies d'hypertrucage.

Public cible : Personnel du gouvernement du Canada — Fonctionnaires

Nom du fichier : « Deepfakes and Generative AI: Shifting the Cyber Security Threat Landscape » — [Deepfakes and Generative AI_GAC Presentation_2024.pptx – PBH_CAN046669]

7.2.5 Orientation et formation publiées à l'intention du grand public

Désinformation en ligne

Description : Le CST a publié des vidéos et de l'orientation écrite qui présentent des trucs et des outils pour décerner et contrer la désinformation.

Public cible : Grand public

URL : https://www.canada.ca/fr/campagne/desinformation-enligne.html

De plus amples renseignements sont disponibles à l'annexe classifiée de la question 7 (A7).

7.3 Cours offerts par le Carrefour de l'apprentissage du Centre pour la cybersécurité

Les services du Carrefour de l'apprentissage du Centre pour la cybersécurité sont offerts aux employées et employés du gouvernement du Canada, des autres ordres de gouvernement et des organismes des infrastructures essentielles.

Cours ITLC 612 — Considérations liées à la cybersécurité à l'intention des organismes et des administrateurs électoraux

Description : Ce cours virtuel offre aux institutions démocratiques canadiennes les outils et les connaissances nécessaires pour qu'elles puissent prendre des décisions éclairées concernant la protection de leur infrastructure de TI.

Public cible : Gouvernement du Canada — Fonctionnaires

URL : https://lh-ca.cyber.gc.ca/course/view.php?id=172

Cours ITLC 616 — La cybersécurité à l'intention des décideurs et du personnel des TI travaillant pour un parti politique

Description : Ce cours virtuel examine les menaces précises qui pèsent sur les partis politiques afin de fournir aux décideuses et décideurs des renseignements sur le point de départ de l'intégration de la cybersécurité dans leur vie professionnelle quotidienne.

Public cible : Gouvernement du Canada — Fonctionnaires

URL : https://lh-ca.cyber.gc.ca/course/view.php?id=188

Cours ITLC 618 — Considérations liées à la cybersécurité pour la gestion des comptes de médias sociaux

Description : Ce cours virtuel informe les apprenantes et apprenants quant aux menaces liées à la cybersécurité dans les médias sociaux et aux meilleures façons de protéger leur organisation contre ces menaces.

Public cible : Gouvernement du Canada — Fonctionnaires

URL : https://lh-ca.cyber.gc.ca/course/view.php?id=191

7.4 Évaluation des cybermenaces nationales

L'Évaluation des cybermenaces nationales (ECMN) est un des rapports emblématiques sur la cybersécurité publiés par le Centre pour la cybersécurité. Son objectif est d'aider à renforcer la résilience du Canada face aux cybermenaces. L'ECMN fait la lumière sur les cybermenaces qui ciblent le Canada, indique la probabilité que surviennent de telles cybermenaces et explique comment elles pourraient évoluer au cours des années à venir.

Pour plus de ressources du Centre pour la cybersécurité afin d'aider les personnes et les organisations à mieux comprendre les cybermenaces qui ciblent le Canada et pour en savoir plus sur la façon de se protéger, visitez la page Web de l'Évaluation des cybermenaces nationales[2].

Évaluation cybermenaces nationales 2023-2024

Description : Au cours des deux dernières années, le CST a observé l'évolution de l'utilisation par les auteures et auteurs de cybermenace de la mésinformation, de la désinformation et de la malinformation (MDM). Les technologies faisant appel à l'apprentissage machine rendent les faux contenus plus faciles à fabriquer et plus difficiles à détecter. Par ailleurs, les États-nations démontrent de plus en plus de capacité et de volonté envers l'utilisation de MDM pour défendre leurs intérêts géopolitiques. Le CST considère que l'exposition de la population canadienne aux campagnes de MDM devrait presque assurément augmenter au cours des deux prochaines années.

Public cible : Grand public

URL : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

Évaluation cybermenaces nationales 2020

Description : Faisant le point à la suite de l'Évaluation des cybermenaces nationales 2018, ce document mentionne que les campagnes d'influence étrangère en ligne sont pratique courante et ne se limitent pas à des événements politiques importants, comme des élections.

Public cible : Grand public

URL : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020

Évaluation cybermenaces nationales 2018

Description : Dans cette évaluation, le CST mentionne qu'il est fort probable que les Canadiennes et Canadiens fassent l'objet d'activités malveillantes d'influence en ligne en 2019. Par exemple, le CST s'attendait à ce que les auteures et auteurs de cybermenaces parrainés par des États tentent de mener à bien leurs objectifs stratégiques nationaux en

[2] https://www.cyber.gc.ca/fr/orientation/evaluations-des-cybermenaces-nationales

ciblant les opinions des Canadiennes et Canadiens dans le cadre d'activités malveillantes d'influence en ligne.

Public cible : Grand public

URL : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2018

7.5 Entrevues avec les médias et sensibilisation continue

Dans le cadre de ses efforts continus d'éducation publique, le CST répond régulièrement à des entrevues avec les médias et organise des activités de sensibilisation concernant l'ingérence étrangère.

« AI-powered disinformation is spreading – is Canada ready for the political impact? »

Description : Le 17 janvier 2024, l'émission *The National* de la CBC a présenté un reportage sur l'IA et la désinformation et leurs répercussions potentielles sur les élections. La chef du CST, Caroline Xavier, a été interviewée dans le cadre de ce reportage.

Public cible : Grand public

URL : https://www.cbc.ca/news/politics/ai-deepfake-election-canada-1.7084398 (en anglais seulement)

« All it takes is one click: Chief cyberspy warns Canadians to protect themselves from online crime »

Description : Le 24 juin 2023, la chef du CST, Caroline Xavier, a été interviewée dans le cadre de l'émission *The House* à CBC Radio.

Public cible : Grand public

URL : https://www.cbc.ca/news/politics/canada-cse-cybersecurity-caroline-xavier-1.6886253 (en anglais seulement)

« Critical cyberattacks are an 'hourly' event. How can Canadians protect themselves? »

Description : Le 25 juin 2023, le dirigeant principal du Centre canadien pour la cybersécurité, Sami Khoury, a été interviewé à l'émission *The West Block* de Global News.

Public cible : Grand public

URL : https://globalnews.ca/news/9790617/cybersecurity-canada-attacks-russia-energy-infrastructure/ (en anglais seulement)

Conférence de presse

Description : Le 6 décembre 2023, des conférences de presse ont eu lieu afin de lancer le rapport sur les menaces contre le processus démocratique du Canada, et cinq entrevues de suivi ont été réalisées, principalement avec de petits médias régionaux.

Public cible : Grand public

URL : https://www.canada.ca/fr/securite-telecommunications/nouvelles/2023/12/le-centre-de-la-securite-des-telecommunications-publie-une-mise-a-jour-2023-sur-les-cybermenaces-contre-le-processus-democratique-du-canada.html

« I Am Now More Concerned About the Formidable Threat from China »

Description : Le 11 septembre 2021, Foreign Policy a interviewé Sami Khoury et Jen Easterly.

Public cible : Grand public

URL : https://foreignpolicy.com/2023/09/11/easterly-khoury-cybersecurity-russia-ukraine-war-china-threat/ (en anglais seulement)

7.6 Autre matériel éducatif

Conseils sur les appareils mobiles à l'intention des voyageurs connus du public

Description : Les personnes qui occupent un poste très en vue, notamment à titre de politicienne ou politicien ou comme membre de la haute direction doivent protéger leurs appareils mobiles lorsqu'elles voyagent. Les appareils mobiles contiennent des informations sensibles, ce qui en fait une cible alléchante pour les auteures et auteurs de cybermenace. S'ils réussissent à compromettre un appareil ou l'information qui s'y trouve, ces auteures et auteurs de menace pourraient s'en servir contre la personne ou l'organisation qu'elle représente.

Public cible : Grand public — Voyageuses et voyageurs connus du public

URL : https://www.cyber.gc.ca/fr/orientation/conseils-sur-les-appareils-mobiles-lintention-des-voyageurs-connus-du-public-itsap-00088

La menace posée par les générateurs de texte basés sur des modèles de langage de grande taille

Description : En 2023, le Centre pour la cybersécurité a publié un bulletin sur les cybermenaces portant précisément sur la menace posée par les générateurs de texte basés sur des modèles de langage de grande taille (LLM pour *large language model*). Le document d'information décrit comment les LLM représentent une menace grandissante pour l'écosystème d'information du Canada, les secteurs canadiens des médias et des télécommunications, et les structures dans lesquelles l'information est créée, partagée et transformée.

Public cible : Grand public

URL : https://www.cyber.gc.ca/fr/orientation/menace-posee-generateurs-texte-bases-modeles-langage-grande-taille

« Si du contenu en ligne vous fait sourciller, vous devez vous questionner »

Description : Cette campagne d'éducation sur la désinformation en ligne a été diffusée sur diverses plateformes numériques entre janvier et mars 2024.

Public cible : Grand public

URL : https://www.youtube.com/watch?v=3ZOy8UtBlYk

Le Canada se joint à la collectivité internationale de la sécurité pour la publication de conseils sur la menace croissante qui pèse sur la sécurité des collectivités à haut risque

Description : Ce communiqué de presse de 2024 mentionne la publication d'un bulletin rédigé par le Canada, les États-Unis, l'Estonie, le Japon, la Finlande et le Royaume-Uni dans le but d'informer le public à propos de la menace croissante à la cybersécurité qui pèse sur les personnes et les sociétés civiles.

Public cible : Grand public

URL : https://www.canada.ca/fr/securite-telecommunications/nouvelles/2024/05/le-canada-se-joint-a-la-collectivite-internationale-de-la-securite-pour-la-publication-de-conseils-sur-la-menace-croissante-qui-pese-sur-la-securit.html

8. Pour chacun des comités interministériels ayant un lien avec l'ingérence étrangère, liste de la fréquence des réunions (ou dates des réunions si elles sont ponctuelles) et description des documents qui sont produits de façon routinière (p. ex. ordres du jour, liste des participantes et participants, ordres du jour explicatifs à l'intention de la présidente ou du président, résumés des réunions, procès-verbaux).

On n'a pas demandé au CST de répondre à cette question.

9. Liste de toutes les rencontres des directrices et directeurs de division (ou l'équivalent) ou de postes supérieurs avec des représentantes et représentants de diasporas lors desquelles les discussions portaient sur l'ingérence étrangère. La liste devrait comprendre les dates, les noms des représentantes et représentants des ministères et des diasporas et le résumé des discussions.

Le CST n'a participé à aucune rencontre avec des diasporas au niveau de direction ou d'un niveau supérieur dans le but de discuter de l'ingérence étrangère.

10. Toute mise à jour de l'information fournie dans la première étape du rapport institutionnel.

10.1 Mise à jour de la section 2.3.1 (description des programmes, des politiques et des procédures mises en place pour réagir à l'ingérence étrangère)

Le GT MSRE a offert une surveillance et une évaluation améliorées des menaces en matière d'ingérence étrangère lors de quatre élections partielles fédérales en juin et en juillet 2023 et l'a offert à nouveau lors des élections partielles qui ont eu lieu à Toronto en juin 2024 pour donner suite aux recommandations du rapporteur spécial indépendant. Cette surveillance améliorée comprend également la production de rapports classifiés et non classifiés sur l'évaluation du groupe de travail visant à déterminer s'il y a eu de l'ingérence étrangère lors des élections partielles. Les rapports sont ensuite transmis au premier ministre, aux ministres concernées et concernés, au Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) et aux représentantes ou représentants désignés des partis qui détiennent la bonne habilitation de sécurité. Les rapports produits dans le cadre des élections partielles de juin et de juillet 2023 concluaient qu'aucune tentative d'ingérence étrangère n'a été observée pendant ces votes.

10.2 Mise à jour de la section 8 (structure de gouvernance de la sécurité et du renseignement)

Outre les comités énumérés dans le rapport institutionnel de janvier 2024, le CST a participé aux comités suivants :

- Comité des sous-ministres sur l'Indo-Pacifique, présidé par AMC;
- Comité des sous-ministres sur l'ingérence étrangère, organisé et présidé par le Bureau du Conseil privé (BCP);
- Comité de coordination des sous-ministres adjoints sur l'Arctique, présidé par Relations Couronne-Autochtones et l'Agence canadienne de développement économique du Nord.

10.3 Mise à jour de la section 9 (produits de renseignement portant sur l'ingérence étrangère)

Le CST fournit une liste actualisée des produits de renseignement portant sur l'ingérence étrangère depuis la création de la liste dans le cadre de la première étape du rapport institutionnel.

Le CST est au courant que des élections partielles ont eu lieu dans la période séparant la demande originale et cette nouvelle demande, et il appuyait activement les activités du GT MSRE pendant cette période. Étant donné qu'il n'est plus responsable de la présidence du GT MSRE, le CST ne détient pas les dossiers officiels quant aux élections partielles qui ont eu lieu

depuis la première étape du rapport institutionnel. C'est pourquoi les plus récents rapports de situation (RAPSIT) du GT MSRE n'ont pas été ajoutés à cette liste.

Une liste à jour des produits de renseignement est disponible à l'annexe classifiée de la question 10 (A10).