Dossier : CST-2025-09

Bureau du commissaire au renseignement
Office of the Intelligence Commissioner

C.P./P.O. Box 1474, Succursale/Station B
Ottawa, Ontario K1P 5P6
613-992-3044 • télécopieur 613-992-4096

[TRADUCTION FRANÇAISE]

COMMISSAIRE AU RENSEIGNEMENT

DÉCISION ET MOTIFS

AFFAIRE INTÉRESSANT UNE AUTORISATION DE CYBERSÉCURITÉ
POUR DES ACTIVITÉS MENÉES DANS DES INFRASTRUCTURES NON FÉDÉRALES
EN VERTU DU PARAGRAPHE 27(2) DE LA
LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS ET
DE L'ARTICLE 14 DE LA *LOI SUR LE COMMISSAIRE AU RENSEIGNEMENT*

[...]

Canada

TABLE DES MATIÈRES

I. APERÇU

1. Il s'agit d'une décision concernant l'examen des conclusions du ministre de la Défense nationale (ministre) autorisant le Centre de la sécurité des télécommunications (CST) à aider à protéger l'information électronique et les infrastructures (c.-à-d. les systèmes, les dispositifs et les réseaux informatiques) appartenant à une entité non fédérale – [...] (autorisation).

2. L'autorisation prévoit des activités identiques à celles que j'ai approuvées relativement à la même entité non fédérale le [...] (décision CST-2025-01).

3. Le [...], en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*), le ministre a délivré l'autorisation. Le [...], le Bureau du commissaire au renseignement l'a reçue pour que je l'examine et l'approuve, conformément à la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*).

4. Pour les motifs ci-après, je suis convaincu que les conclusions tirées par le ministre en vertu des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités ou aux catégories d'activités énumérées au paragraphe 81 de l'autorisation sont raisonnables. Par conséquent, conformément à l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation.

II. CONTEXTE

5. Dans le cadre du volet de son mandat touchant la cybersécurité, le CST mène des activités de cyberprotection afin d'aider à protéger certains systèmes, dispositifs et réseaux électroniques ainsi que l'information qu'ils contiennent contre les cybermenaces criminelles et parrainées par des États. De plus, le CST fournit des avis et des conseils pour renforcer la posture de cybersécurité de ces systèmes (art 17, *Loi sur le CST*).

6. Sous le régime de la *Loi sur le CST*, le CST est tenu d'obtenir une autorisation ministérielle pour toute activité relevant du volet de son mandat touchant la cybersécurité qui contreviendrait à toute autre loi fédérale ou qui entraînerait l'acquisition par celui-ci d'information qui porterait atteinte à une attente raisonnable de protection en matière de vie privée des Canadiens (citoyens canadiens, résidents permanents ou personnes morales formées sous le régime d'une loi fédérale

ou provinciale) et des personnes se trouvant au Canada (art 22(4) et 27, *Loi sur le CST*). Afin de mener efficacement des activités de cybersécurité, le CST acquiert de telles informations.

7. La *Loi sur le CST* établit deux types distincts d'autorisations ministérielles pour les activités de cybersécurité : celles délivrées pour les systèmes fédéraux (art 27(1)) et celles délivrées pour les systèmes non fédéraux désignés comme étant d'importance pour le gouvernement fédéral – systèmes non fédéraux – (art 27(2)), par exemple ceux liés aux secteurs de la santé, de l'énergie et des télécommunications.

8. Les autorisations qui se rapportent à des systèmes non fédéraux doivent satisfaire à deux exigences. Premièrement, les systèmes doivent avoir été désignés, par arrêté ministériel, comme étant importants pour le gouvernement fédéral (art 21, *Loi sur le CST*). L'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada* (Arrêté sur les SDI), émis le 25 août 2020, définit de vastes catégories de systèmes désignés, dont l'une englobe l'entité non fédérale. Deuxièmement, le processus d'autorisation doit être lancé par le propriétaire ou l'exploitant du système non fédéral qui présente une demande écrite au CST pour mener les activités en cause (art 33(3), *Loi sur le CST*). Le dossier comprend la demande écrite de l'entité non fédérale pour le soutien du CST afin de mener des activités de cybersécurité.

9. L'autorisation énonce les conclusions du ministre – les motifs, en fait – à l'appui des activités ou des catégories d'activités que le CST peut mener. L'autorisation est valide jusqu'à un an si le commissaire au renseignement l'approuve (art 36, *Loi sur le CST*).

10. Malgré une autorisation, la *Loi sur le CST* impose des limites quant aux activités de cybersécurité du CST. Les activités de cybersécurité du CST ne doivent pas viser des Canadiens ou des personnes se trouvant au Canada et ne peuvent pas porter atteinte à la *Charte canadienne des droits et libertés* (art 22(1), *Loi sur le CST*). Toutefois, le CST peut acquérir incidemment de l'information qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada (art 23(4), *Loi sur le CST*). Le terme « incidemment » signifie que l'information acquise n'a pas été délibérément recherchée (art 23(5), *Loi sur le CST*). Pour utiliser, analyser, conserver ou communiquer l'information, le CST est tenu par la loi de veiller à ce que des mesures soient en

place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada (art 24, *Loi sur le CST*).

11. Conformément à l'article 23 de la *Loi sur le CR*, le ministre a confirmé dans sa lettre de présentation m'avoir fourni toute l'information dont il disposait pour délivrer l'autorisation en cause. Le dossier est donc composé de ce qui suit :

    a) l'autorisation;
    b) la demande de la chef du CST (la chef) au ministre (demande), datée du […], qui comprend les annexes suivantes :
        i. lettre de demande de l'entité non fédérale;
        ii. quatre arrêtés ministériels;
        iii. Rapport sur les résultats de 2025;
        iv. six évaluations de la menace et survols du Centre canadien de la cybersécurité;
        v. Ensemble des politiques sur la mission en matière de cybersécurité (EPM) approuvé en novembre 2025;
        vi. Registre des changements apportés à l'EPM;
    c) les réponses aux remarques du commissaire au renseignement;
    d) la note d'information de la chef au ministre;
    e) le document d'information – aperçu des activités.

III. NORME DE CONTRÔLE

12. Conformément à la *Loi sur le CR*, le commissaire au renseignement est tenu d'examiner si les conclusions du ministre sont raisonnables. J'appliquerai donc la norme de la décision raisonnable, telle qu'elle est appliquée dans les contrôles judiciaires de mesures administratives.

13. Comme la Cour suprême du Canada l'a indiqué, lorsqu'elle procède au contrôle d'une décision selon la norme de la décision raisonnable, la cour de révision doit commencer son analyse à partir des motifs du décideur administratif. Au paragraphe 99 de l'arrêt *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65 [*Vavilov*], la Cour suprême du Canada a décrit de manière succincte ce qui constitue une décision raisonnable :

> La cour de révision doit s'assurer de bien comprendre le raisonnement suivi par le décideur afin de déterminer si la décision dans son ensemble est raisonnable. Elle doit donc se demander si la décision possède les caractéristiques d'une décision raisonnable, soit la justification, la transparence et l'intelligibilité, et si la décision est justifiée au regard des contraintes factuelles et juridiques pertinentes qui ont une incidence sur celle-ci.

14. Les contraintes factuelles et juridiques pertinentes peuvent comprendre le régime législatif applicable et l'incidence de la décision. Le régime législatif applicable institué par la *Loi sur le CR* et la *Loi sur le CST* met en évidence la fonction de commissaire au renseignement en tant que mécanisme indépendant qui permet d'assurer un juste équilibre entre les mesures prises par le gouvernement à des fins de sécurité nationale et de renseignement et le respect de la primauté du droit ainsi que des droits et intérêts des Canadiens.

15. Lorsque le commissaire au renseignement est convaincu (*satisfied* en anglais) que les conclusions en cause du ministre sont raisonnables, il « approuve » l'autorisation (art 20(1)a), *Loi sur le CR*). À l'inverse, lorsqu'il n'est pas convaincu qu'elles sont raisonnables, il « n'approuve pas » l'autorisation (art 20(1)b), *Loi sur le CR*). Dans les deux cas, le commissaire au renseignement doit motiver sa décision.

IV. ANALYSE

16. Le ministre a délivré l'autorisation valide pour une période d'un an, sous réserve de mon approbation. Une description de l'entité non fédérale et des activités de cybersécurité visées par l'autorisation figure à l'annexe classifiée de la présente décision (annexe A). L'annexe facilite la lecture de la version de la présente décision qui sera tôt ou tard rendue publique, et permet de veiller à ce que la décision présente la nature des faits dont j'ai été saisi, lesquels ne seraient autrement accessibles que dans le dossier.

A. Dossier mis à jour

17. Le dossier comprend les réponses aux remarques que j'ai formulées dans la décision CST-2025-01 concernant la même entité non fédérale, ainsi que celles trouvées dans les décisions subséquentes relatives à d'autres autorisations de cybersécurité. Je suis satisfait des réponses rapides et exhaustives fournies par le CST pour régler les questions soulevées dans

mes remarques et je suis d'avis que le processus de surveillance continu mis en place fonctionne efficacement.

i. Lettres de demande

18. La première de ces remarques a abordé un thème que j'ai repris dans plusieurs décisions en matière de cybersécurité rendues en 2025, à savoir le contenu de la lettre de demande du propriétaire du système. Les principaux aspects de mes remarques ont été résolus par l'inclusion de la confirmation expresse que l'entité non fédérale possède une autorisation légale d'obtenir des informations et de les transmettre au CST à des fins de cybersécurité. La lettre montre également qu'il s'agit d'un renouvellement des activités de cybersécurité existantes par la demande de leur poursuite.

19. En outre, à la suite de ma remarque à savoir qu'il serait utile que la demande donne un aperçu des mesures prises par l'entité non fédérale pour aviser les utilisateurs de son système, et obtenir leur consentement à cet effet, le dossier indique que l'entité non fédérale a fourni au CST un aperçu de sa politique d'utilisation acceptable et qu'elle informe les employés que l'entité non fédérale effectue une surveillance de la cybersécurité. Comme il est indiqué dans la décision CST-2025-08 (para 23), le CST s'engage à continuer de fournir à ses clients non fédéraux le libellé recommandé à utiliser dans les avis d'ouverture de session.

20. Une autre remarque liée aux lettres de demande formulée dans la décision de l'an dernier se rapporte au libellé utilisé concernant le brouillage de renseignements personnels et exclusifs avant la communication. J'étais d'avis qu'il manquait de clarté dans la lettre quant à savoir si l'entité non fédérale comprend bien les mesures de protection de la vie privée du CST énoncées dans l'EPM. La lettre de demande actuelle précise quand il est nécessaire de brouiller l'information : lorsqu'on transmet des rapports de cybersécurité à l'extérieur du CST à des destinataires autres que le propriétaire du système ou de l'information, le CST ne transmet que des informations sur la menace, comme […] des activités suspectes observées. Les informations telles que le nom de la victime, le nom du ministère ou de l'entité sont brouillées.

ii. Mise à jour de l'EPM – novembre 2025

21. L'EPM mis à jour inclus dans le dossier corrige une incohérence entre des dispositions des autorisations stipulant que les gestionnaires opérationnels « doivent examiner » les informations conservées reconnues se rapportant à un Canadien tous les trimestres et les versions antérieures de l'EPM indiquant qu'on leur « rappelle d'examiner » tout simplement. Un autre ajout important à l'EPM qui ne s'applique pas à la présente autorisation, mais à d'autres autorisations liées aux entités non fédérales que j'ai approuvées, est que le CST avisera le ministre et, par la suite, moi-même lorsqu'il accepte une nouvelle demande de la part d'une entité non fédérale pour étendre ses activités de cybersécurité à d'autres sous-entités qui utilisent ses infrastructures d'information, à condition que ces sous-entités soient énumérées dans l'autorisation initiale.

22. Un des principaux points non résolus concerne mon encouragement du CST à envisager de développer son approche pour déterminer le niveau de sensibilité de l'information se rapportant à un Canadien afin de faire référence explicitement à la sensibilité des informations liées aux institutions fondamentales canadiennes. Je comprends que le CST effectue d'autres analyses et consultations sur ce point soulevé dans ma décision la plus récente (CST-2025-08).

iii. Autres mises à jour

23. Dans la décision CST-2025-08, mes motifs ont souligné que la *Loi sur le CST* énonce différentes exigences particulières pour les autorisations de cybersécurité pour les systèmes fédéraux et non fédéraux. Plus précisément, l'objectif principal d'une autorisation ne devrait pas combiner la protection des deux types de systèmes, et l'évaluation pour déterminer si l'information est « nécessaire » et « essentielle » devrait refléter le type d'autorisation que le ministre a délivrée. La demande et l'autorisation actuelles reflètent correctement cette définition.

24. Le dossier fournit également une mise à jour concernant l'interception des communications entre avocat et client. Je note que le nouveau libellé de la condition régissant la conservation des communications entre avocat et client a réduit sa portée. Seules les communications entre avocat et client jugées essentielles pour découvrir, isoler, prévenir ou atténuer les dommages aux informations électroniques et aux infrastructures de l'information de l'entité non fédérale

mentionnées dans l'autorisation peuvent être conservées par la chef et renvoyées au ministre aux fins de décision. Contrairement aux autorisations antérieures, on ne fait plus référence à tous les autres systèmes fédéraux et systèmes d'importance. J'accueille cette restriction supplémentaire pour donner suite aux préoccupations que j'avais soulevées dans des remarques antérieures au sujet du secret professionnel de l'avocat. Par souci de clarté, je précise n'avoir reçu à ce jour aucun signalement indiquant que la chef a décidé de conserver des communications entre avocat et client. J'ajoute également que j'attends toujours le résultat du travail du CST visant à déterminer si le ministre devrait être celui qui décide si les communications protégées par le secret de l'avocat devraient être conservées.

25. Ma remarque concernant l'inclusion d'arrêtés ministériels désignant des systèmes d'importance a été abordée en incluant deux arrêtés supplémentaires de 2022 désignant respectivement les informations électroniques ou les infrastructures d'information du gouvernement de l'Ukraine et du gouvernement de la Lettonie comme systèmes d'importance. Fait important, cela donne au ministre un portrait complet de la façon dont l'information se rapportant à un Canadien pourrait être transmise. Par souci de clarté, je note qu'il est indiqué qu'aucune information se rapportant à un Canadien n'a été transmise à l'un ou l'autre des gouvernements au cours de l'autorisation existante.

26. Enfin, en plus d'être mis à jour pour traiter des remarques ou des questions précises que j'ai soulevées, il demeure essentiel que le dossier présente toujours au ministre et à moi-même les informations les plus exactes. Voici des exemples où une mise à jour aurait été requise :

    a) La demande indique que l'entité non fédérale a acheté un produit commercial de cybersécurité pour effectuer une analyse des vulnérabilités, mais la note d'information continue d'indiquer que l'entité non fédérale n'a pas la capacité requise. La note d'information fait toujours référence à des événements à venir [...] qui se sont déjà produits.

    b) La demande fait référence à [...] du premier trimestre de 2024 et à une tendance prévue pour la fin de 2024. Une mise à jour aurait pu être fournie pour refléter les

dernières données disponibles ou pour indiquer si la tendance prévue s'est concrétisée.

c) Le Rapport sur les résultats contient moins d'information que ce qui est habituellement inclus. À savoir, aucune information n'est fournie sur la ou les dates de déploiement des solutions de cybersécurité du CST. Puisque l'autorisation initiale a été délivrée et approuvée de façon accélérée compte tenu des circonstances, je suggère d'inclure ces informations dans le rapport de fin d'autorisation préparé conformément à l'article 52 de la *Loi sur le CST* afin de mettre en évidence l'état du déploiement depuis le début de l'autorisation jusqu'à la fin.

d) Le libellé de l'autorisation initiale utilisé pour décrire la portée des informations acquises au moyen d'une solution de cybersécurité particulière – […] – a été modifié. Alors que l'original indiquait que la solution accédait […] (c.-à-d., l'entité non fédérale), la demande actuelle indique que « le CST accédera seulement aux […] qui contiennent des mesures prédéfinies de sécurité et de télémétrie d'utilisation accessibles par le client » (soulignement ajouté). Cela semble avoir réduit […] accessibles par le CST, mais la description restante de la solution de cybersécurité demeure la même et indique que le CST va acquérir […]. Par conséquent, je voudrais que les futures demandes précisent davantage la portée des informations accessibles au moyen de la […] solution de cybersécurité. Il serait également utile pour le ministre et moi-même que le dossier indique si l'entité non fédérale a choisi de déployer une capacité approuvée donnée […]. Je remarque que cette capacité a le potentiel d'élargir la portée des types d'informations que le CST acquerrait

B. Les conclusions du ministre sont-elles raisonnables (art 34(1), *Loi sur le CST*)

27. Une fois de plus, le ministre a délivré l'autorisation de façon proactive; il n'y a pas de compromission ou de menace particulière pour l'entité non fédérale. Néanmoins, le ministre établit un fondement factuel pour le soutien du CST. Effectivement, le dossier décrit en détail les auteurs de cybermenace existants et fournit de l'information sur la probabilité que les systèmes de l'entité non fédérale soient la cible de cyberactivités malveillantes – informations

que j'ai incluses à l'annexe A. Le ministre s'appuie sur les compromissions subies par d'autres entités et sur la preuve continue de vulnérabilités et d'activités malveillantes vécues par ces entités. [. . .].

28. Le ministre se base également sur la sensibilité et l'importance des infrastructures d'information de l'entité non fédérale ainsi que sur les informations importantes qu'elles contiennent, qui [liste des informations détenues par l'entité non fédérale]. Les conclusions expliquent que le CST doit obtenir de grandes quantités d'informations pour détecter et analyser les cybercompromissions. Le ministre conclut également que l'acquisition des informations est nécessaire pour prendre des mesures d'atténuation en temps réel, afin de prévenir les cybercompromissions.

29. En somme, le ministre fonde ses conclusions sur l'importance stratégique de l'entité non fédérale, sa posture en matière de cybersécurité, ainsi que sur les cybermenaces auxquelles des entités semblables à l'entité non fédérale continueront de faire face. De plus, le ministre sait que les activités de cybersécurité énoncées dans l'autorisation entraîneront l'acquisition d'informations à l'égard desquelles les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée. Je suis convaincu que les activités décrites respectent l'exigence prévue par la loi selon laquelle les activités du CST ne doivent pas viser des Canadiens ou des personnes se trouvant au Canada.

30. Compte tenu de ce qui précède, j'estime que les conclusions du ministre quant au caractère raisonnable des activités énoncées dans l'autorisation sont raisonnables.

C. Les conclusions du ministre sont-elles proportionnelles (art 34(1), *Loi sur le CST*)

31. Le ministre conclut également qu'il avait des motifs raisonnables de croire que les activités autorisées sont proportionnelles. Le ministre tient compte de la manière dont elles sont menées, du fait qu'elles ont un lien rationnel avec l'objectif à atteindre et qu'elles ne porteront qu'une atteinte minimale aux droits et libertés de tiers, ainsi que de la capacité de tiers d'accéder à de l'équipement ou à des infrastructures ou de les utiliser.

32. Tout comme l'an dernier, le ministre arrive à cette conclusion en se fondant sur sept mesures et contrôles internes qu'applique le CST après l'acquisition des informations. Je peux suivre le raisonnement du ministre lorsqu'il s'est appuyé sur ces mesures. L'accès aux informations acquises se limite aux employés désignés du CST qui sont formés pour manipuler ce type d'information et qui les utilisent selon le principe du besoin de savoir pour effectuer leur travail. Comme l'explique le dossier, bien que les analystes aient accès à l'éventail des informations acquises, ils s'intéressent au comportement anormal et non au contenu des fichiers, des courriels ou des messages de clavardage eux-mêmes. Le ministre était conscient des droits en matière de vie privée en jeu et il a énoncé les mesures mises en place pour les protéger.

33. En ce qui concerne les lois fédérales auxquelles le CST pourrait contrevenir, je suis convaincu que le ministre conclut raisonnablement qu'elles seront proportionnelles parce que les activités doivent respecter la portée de celles décrites dans la demande. À titre de mesure de protection supplémentaire, en cas de contravention à une loi fédérale qui ne figure pas dans la demande, la chef en informera le ministre et le commissaire au renseignement.

34. J'estime que les conclusions du ministre concernant la proportionnalité des activités sont justifiées et intelligibles et qu'elles sont raisonnables.

D. Paragraphe 34(3) de la *Loi sur le CST* – les conditions nécessaires à la délivrance d'une autorisation

35. Après avoir établi que les activités sont raisonnables et proportionnelles, le ministre peut délivrer une autorisation s'il conclut qu'il existe également des motifs raisonnables de croire que les trois conditions suivantes, énoncées au paragraphe 34(3) de la *Loi sur le CST*, sont remplies :

    i. l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire;

    ii. l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux;

    iii. les mesures en place permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement

si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux.

i. L'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire (alinéa 34(3)a))

36. Puisqu'il n'est pas possible de déterminer à l'avance quelles informations sont nécessaires pour aider à découvrir et à prévenir les cyberactivités malveillantes, le ministre juge raisonnable que le CST conserve les informations non évaluées pendant une période maximale de 12 mois. L'efficacité des activités du CST dépend de la capacité à recouper et à analyser de multiples sources d'informations déjà acquises, y compris les indicateurs de compromission découverts.

37. Une condition de l'autorisation veut que toutes les informations acquises soient traitées conformément aux politiques opérationnelles pertinentes du CST. Les informations sont conservées conformément à l'EPM, qui contient un calendrier de conservation pour les différentes catégories d'informations qui peuvent être acquises. En outre, les périodes de conservation tiennent compte de la période minimale obligatoire de deux ans prévue dans la *Loi sur la protection des renseignements personnels,* LRC (1985), c P-21, pour les renseignements personnels utilisés à des fins administratives (*Règlement sur la protection des renseignements personnels*, DORS/83-508, art 4), et du pouvoir de gestion de l'information et d'aliénation ou d'élimination des documents conféré au CST par la *Loi sur la Bibliothèque et* les Archives du Canada, LC 2004, c 11.

38. Avant la fin de la période de 12 mois, toutes les informations non évaluées seront automatiquement supprimées, à moins qu'elles ne soient jugées « nécessaires » ou « essentielles » pour aider à protéger les systèmes non fédéraux. Les informations jugées « nécessaires » ou « essentielles » peuvent être conservées jusqu'à ce qu'elles « ne soient plus utiles dans le cadre du volet du mandat du CST touchant la cybersécurité et l'assurance de l'information ». Le critère du caractère « nécessaire » s'applique à l'information qui, de par sa nature, ne contient aucun élément se rapportant à un Canadien ou à une personne se trouvant au Canada. Le critère du caractère « essentiel » s'applique à l'information identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada.

39. L'information conservée parce qu'elle est essentielle doit être examinée par un gestionnaire des opérations tous les trimestres afin de vérifier si elle est toujours essentielle; l'information qui n'est plus essentielle doit être supprimée.

40. J'estime que la conclusion du ministre concernant la période d'évaluation de 12 mois est raisonnable. En effet, le fait de conserver l'information pendant la durée nécessaire permet au CST de mener efficacement ses activités de cybersécurité et d'élaborer les cyberinterventions requises afin de suivre le rythme de l'évolution rapide des techniques utilisées par les auteurs de menaces liées à des logiciels malveillants. Cela permet une meilleure protection des systèmes non fédéraux, et par conséquent, des systèmes fédéraux. Je souscris également à la conclusion du ministre selon laquelle l'information « nécessaire » ou « essentielle » pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux peut être conservée jusqu'à ce qu'elle ne soit plus utile, pourvu qu'elle soit toujours « nécessaire » ou « essentielle » à cette fin à la suite des examens trimestriels requis.

ii. L'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux (alinéa 34(3)c))

41. Les conclusions du ministre réaffirment que les activités de cybersécurité du CST ne sont efficaces que si le CST est en mesure d'acquérir une vaste gamme d'informations et de dégager des tendances qui indiquent des activités anormales. La demande indique que les mesures commerciales utilisées par l'entité non fédérale sont insuffisantes pour détecter et contrer les méthodes et les capacités sophistiquées déployées par des auteurs de menace avancés et tenaces.

42. Le ministre donne des exemples de la façon dont le CST peut aussi utiliser l'information acquise au titre de l'autorisation pour appuyer des activités au titre d'autres autorisations de cybersécurité et d'autres volets de son mandat, y compris les activités autorisées concernant d'autres systèmes non fédéraux. Avant de pouvoir être utilisée, l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada doit avoir été évaluée comme étant essentielle à des fins de cybersécurité. L'utilisation, l'analyse, la conservation et la communication ultérieures de toute information acquise au titre de l'autorisation sont assujetties

aux restrictions et aux conditions énoncées dans l'EPM, y compris les conditions imposées par les clients du CST ou les entités qui font la divulgation.

43. Compte tenu de ce qui précède, je suis convaincu que les conclusions du ministre sont raisonnables.

> *iii. Les mesures visant à protéger la vie privée permettront de faire en sorte que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux (alinéa 34(3)d))*

44. L'article 24 de la *Loi sur le CST* exige que le CST ait des mesures en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la communication de l'information qui se rapporte à eux et qui a été acquise dans le cadre des volets de son mandat touchant la cybersécurité et l'assurance de l'information. Comme l'établit la jurisprudence du commissaire au renseignement, de telles mesures revêtent une importance encore plus grande lorsque le rôle (ou la portée du réseau) d'une entité non fédérale est directement et intrinsèquement lié à de l'information sensible à l'égard de laquelle il existe une attente raisonnable de protection en matière de vie privée.

45. En ce qui concerne la conservation de l'information se rapportant à un Canadien, le ministre réitère que l'information ne peut être utilisée ou conservée que si elle est essentielle pour découvrir, isoler ou prévenir des dommages aux systèmes non fédéraux. Le ministre énonce des conditions et des restrictions supplémentaires pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada. Mentionnons plus particulièrement la nécessité que l'information soit traitée conformément à l'article 8 de l'EPM, qui prévoit que les justifications relatives au caractère essentiel doivent être consignées (art 8.2.2, EPM).

46. D'autres mesures raisonnables mises en place par le CST consistent à limiter l'accès à l'information et à effectuer des analyses au moyen de processus automatisés – dans la mesure du possible – qui limitent le contact des employés à l'information non évaluée. Les personnes ayant accès à l'information acquise au titre de cette autorisation doivent non seulement soutenir le CST et ses exigences sur le plan opérationnel, mais elles doivent également comprendre les

exigences légales et politiques relatives aux activités liées à leurs responsabilités. Le CST effectue également des évaluations régulières de la conformité pour aider à déceler et à résoudre les incidents en matière de vie privée qui pourraient survenir au cours d'activités opérationnelles.

47. Pour que le CST communique de l'information se rapportant à un Canadien, il faut que la communication soit nécessaire pour aider à protéger les systèmes non fédéraux, ainsi que les systèmes fédéraux ou d'autres systèmes d'importance. Les conclusions du ministre et le dossier reflètent la condition prévue à l'article 44 de la *Loi sur le CST*. Comme l'a indiqué la décision de l'année dernière, l'information n'est communiquée qu'aux personnes ou aux catégories de personnes désignées en vertu de l'*Arrêté ministériel désignant les destinataires de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui a été acquise, utilisée ou analysée dans le cadre des volets du mandat du CST touchant la cybersécurité et l'assurance de l'information*, émis le 13 juin 2023 en application de l'article 45. Ces personnes ou catégories de personnes comprennent les propriétaires ou les administrateurs de systèmes ou de réseaux informatiques utilisés par le gouvernement fédéral ou une entité non fédérale, ainsi que les personnes et les catégories de personnes autorisées au sein d'entités étrangères avec lesquelles le CST a conclu des ententes.

48. Avant de communiquer de l'information se rapportant à un Canadien, le CST met également en place des mesures qui doivent être suivies (art 24, EPM), dont le brouillage de l'information nominative. L'EPM définit les niveaux d'approbation requis pour la communication de l'information se rapportant à un Canadien, dont les approbations doivent être consignées.

49. L'EPM établit des politiques détaillées visant à contrôler et à protéger l'information se rapportant à un Canadien qui est acquise au titre d'une autorisation de cybersécurité. À mon avis, ces mesures contribuent à faire en sorte que le CST respecte son obligation prévue par la loi à l'article 24 et appuient les conclusions du ministre. Je suis donc convaincu que les conclusions du ministre sont raisonnables.

V. REMARQUES

50. Je souhaite formuler la remarque suivante, qui ne change rien à mes conclusions concernant le caractère raisonnable des conclusions du ministre.

A. Prévoir des exceptions aux périodes de conservation dans les autorisations

51. Dans les décisions CST-2024-06 et CST-2025-08, j'ai soulevé un incident de conformité lié à l'obligation de préservation de la preuve. À savoir, conformément à une demande du ministère de la Justice, le CST a conservé, aux fins de litige, des informations recueillies au titre de l'autorisation en question qui auraient autrement été supprimées dans un délai précis. J'avais indiqué que les exceptions potentielles au traitement habituel des données brutes sur les clients qui sont conservées au titre d'une autorisation, comme celles liées à l'obligation de préservation de la preuve, devraient être énoncées dans l'autorisation.

52. Compte tenu des informations additionnelles fournies dans cette autorisation, je demeure d'avis qu'il est judicieux que les conditions ou restrictions des futures autorisations tiennent compte des exceptions potentielles aux périodes de conservation à appliquer, notamment celles qui sont prévues par l'obligation de préservation de la preuve. Cela s'applique particulièrement dans la présente situation, car il est prévu qu'au moins une obligation de préservation de la preuve continuera d'être en vigueur pendant la présente autorisation. L'avantage de cette condition serait que, dans le cours normal, le CST n'ait pas nécessairement à considérer toute conservation excessive qui en résulterait comme un incident de conformité.

53. Toutefois, je tiens à souligner que les exceptions au fonctionnement ordinaire des calendriers de conservation établis dans l'EPM devraient être, effectivement, exceptionnelles et aussi limitées que possible en nombre et en portée. Comme l'a expliqué le CST, la conservation excessive concerne les données brutes des clients qui ont été traitées dans [certains systèmes périphériques]. Bien que je ne connaisse pas les détails des deux cas de préservation de la preuve, il n'est pas évident de savoir comment les données brutes recueillies sur les clients en vertu des autorisations ministérielles seraient normalement pertinentes à un litige ou plus généralement à un litige contre le gouvernement du Canada.

VI. CONCLUSIONS

54. D'après mon examen du dossier, je suis convaincu que les conclusions tirées par le ministre en vertu des paragraphes 34(1) et (3) de la *Loi sur le CST* à l'égard des activités énumérées au paragraphe 81 de l'autorisation sont raisonnables.

55. J'approuve donc, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, l'autorisation de cybersécurité pour des activités menées dans des infrastructures non fédérales délivrée par le ministre le […].

56. Comme le ministre l'a indiqué, et en vertu du paragraphe 36(1) de la *Loi sur le CST*, cette autorisation expire un an après la date de mon approbation.

57. Conformément à l'article 21 de la *Loi sur le CR*, une copie de la présente décision sera remise à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement afin de l'aider à réaliser les éléments de son mandat au titre des alinéas 8(1)a) à c) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, LC 2019, c 13, art 2.

[…]

(Original signé)

L'honorable Simon Noël, c.r.
Commissaire au renseignement