Dossier : CST-2025-06

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*

LE 2 JUILLET 2025

Canada

TABLE DES MATIÈRES

I. APERÇU

1. Il s'agit d'une décision concernant les 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 trois entités non fédérales (autorisation).

2. L'autorisation vise les activités approuvées par le commissaire au renseignement au cours des quatre années précédentes (décisions CST-2024-06, 2023-05, 2022-05, 2021-05) relativement à [entité A]. Elle vise également de nouvelles activités pour [entité A] ainsi que des activités de cybersécurité liées à deux autres entités non fédérales : [entités B et C].

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, laquelle a été reçue par le Bureau du commissaire au renseignement pour que je procède à l'examen et à l'approbation aux termes de 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 87 de l'autorisation sont raisonnables.

5. Par conséquent, en application de l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation.

II. CONTEXTE

6. Le contexte législatif détaillé des activités de cybersécurité du CST est énoncé dans des décisions antérieures du commissaire au renseignement. Dans le cadre de son mandat, le CST mène des activités de cyberprotection pour défendre certains systèmes, dispositifs et réseaux électroniques ainsi que l'information qu'ils contiennent contre les cybermenaces que posent des criminels et des acteurs parrainés 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*).

7. Les systèmes peuvent appartenir à une institution fédérale – des systèmes fédéraux (art 27(1), *Loi sur le CST*) – ou à une entité non fédérale désignée comme étant d'importance pour le gouvernement fédéral – des systèmes non fédéraux (art 27(2), *Loi sur le CST*), notamment des entités des secteurs de la santé, de l'énergie et des télécommunications, comme il est précisé dans l'Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada daté du 25 août 2020. Si l'autorisation vise un système non fédéral, le propriétaire ou l'opérateur du système doit amorcer le processus en demandant par écrit au CST de mener des activités de cybersécurité pour protéger le système et l'information électronique qu'il contient (art 33(3), *Loi sur le CST*).

8. Afin de comprendre les vulnérabilités et les atteintes à l'intégrité des systèmes non fédéraux, le CST doit accéder à ces systèmes et acquérir de l'information provenant de ceux-ci. Pour ce faire, le CST pourrait devoir contrevenir à certaines lois fédérales. Une autorisation ministérielle confère au CST le pouvoir légal de mener des activités de cybersécurité qui contreviennent à une loi fédérale ou qui l'amènent à acquérir incidemment de l'information qui porte atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens (citoyens canadiens, résidents permanents ou sociétés constituées en vertu d'une loi canadienne ou provinciale) et des personnes se trouvant au Canada (art 22(4) et 27, *Loi sur le CST*).

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 exécuter. Le ministre doit, entre autres conditions, conclure que les activités proposées sont nécessaires (art 33(2), *Loi sur le CST*), raisonnables et proportionnelles (art 34, *Loi sur le CST*). L'autorisation est valide pendant une période maximale d'un an après l'approbation du commissaire au renseignement (art 36, *Loi sur le CST*). Ce n'est qu'à ce moment que le CST peut exercer les activités autorisées.

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 un Canadien ou à une personne se trouvant au Canada (art 23(4), *Loi sur le CST*). Le terme « incidemment » s'entend de la manière dont l'information est

acquise dans le cas où elle n'était pas délibérément recherchée (art 23(5), *Loi sur le CST*). Pour utiliser, analyser, conserver ou divulguer l'information, le CST est tenu par la loi de veiller à ce que des mesures pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada soient en place (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 tous les renseignements dont il disposait pour accorder l'autorisation en cause. Le dossier est donc composé de ce qui suit :

    a) l'autorisation;
    b) la note d'information de la chef du CST à l'intention du ministre;
    c) la demande de la chef, qui comprend 17 annexes, notamment les suivantes :
        i. lettres de demande des trois entités non fédérales;
        ii. deux arrêtés ministériels;
        iii. Tableau de conservation et de suppression;
        iv. liste des recommandations du CST à l'intention de [entité A];
        v. Rapport sur les résultats des activités pour 2024-2025;
        vi. Ensemble des politiques sur la mission en matière de cybersécurité (EPM) approuvé le 14 février 2025;
    d) le document d'information – aperçu des activités;
    e) les réponses aux remarques du commissaire au renseignement.

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, la Cour suprême du Canada décrit brièvement en quoi consiste 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 […], la chef du CST a présenté au ministre une demande d'autorisation (demande). La demande énonce les activités de cybersécurité que le CST souhaite mener et décrit comment le CST analysera, traitera et conservera l'information acquise ainsi que les mesures en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada, dans les cas où le CST acquiert incidemment de l'information sur eux.

17. La demande définit également les solutions de cybersécurité à déployer dans les systèmes non fédéraux – avec le consentement des entités non fédérales – pour permettre au CST d'acquérir des données de façon sécuritaire et de prendre des mesures d'atténuation, manuellement ou automatiquement. Les solutions sont les suivantes : […]

18. Une description des entités non fédérales, des activités de cybersécurité et des solutions figure dans l'annexe classifiée de la présente décision (annexe A). L'annexe facilitera 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.

19. Le ministre a conclu qu'il existe des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions des paragraphes 34(1) et (3) de la *Loi sur le CST* ont été remplies. Par conséquent, le ministre a délivré l'autorisation assortie d'une période de validité d'un an, sous réserve de l'approbation du commissaire au renseignement.

A. Dossier mis à jour

20. Les activités de cybersécurité qui ont été approuvées au cours des quatre dernières années relativement à [entité A] sont de nouveau incluses dans l'autorisation de cette année, qui autorise en outre le CST à […]. L'autorisation a été élargie de façon à inclure également des activités de cybersécurité permettant au CST d'accéder aux infrastructures électroniques et de l'information de deux autres entités non fédérales ainsi que de les protéger de façon proactive contre les cybermenaces connues et potentielles.

21. En plus de l'autorisation visant deux nouvelles entités non fédérales, le dossier comprend un certain nombre de mises à jour. Plus particulièrement, le CST a inclus une annexe décrivant en détail ses réponses à certaines remarques formulées dans des décisions antérieures concernant la cybersécurité et le renseignement étranger. Je constate que le CST prend au sérieux mes remarques et que les efforts qu'il déploie pour y donner suite en temps opportun renforcent le régime des autorisations ministérielles. L'autorisation traite des trois questions suivantes soulevées dans des remarques antérieures : (i) le pouvoir légal des entités non fédérales de recueillir et de communiquer de l'information; (ii) le consentement des utilisateurs des systèmes non fédéraux; (iii) la communication de rapports fondés sur des activités malveillantes ou des vulnérabilités.

22. Dans la décision CST-2024-05 relative à une autorisation de cybersécurité, j'ai fait remarquer que même si le ministre n'est pas tenu par la loi de confirmer que l'entité non fédérale a le pouvoir légal de recueillir de l'information personnelle sur des Canadiens et des personnes se trouvant au Canada à partir de son réseau à des fins de cybersécurité et de les communiquer par la suite au CST, le fait de recevoir une telle confirmation serait utile au ministre et à moi-même. Dans le même ordre d'idées, dans la décision CST-2024-06 de l'an dernier concernant [entité A], j'ai indiqué que le ministre devrait être en mesure de comprendre facilement, à partir de la lettre de demande adressée au CST par l'entité non fédérale, que celle-ci a compétence pour recueillir l'information et qu'il existe un fondement juridique pour la communication efficace de cette information au CST. De plus, dans la décision CST-2024-07, j'ai recommandé que le lien entre le pouvoir légal de l'entité de recueillir l'information et l'utilisation de celle-ci à des fins de cybersécurité soit énoncé plus clairement dans le dossier pour le ministre.

23. Dans le dossier relatif à la décision CST-2025-01, la chef a indiqué que le CST avait reçu une confirmation verbale que l'entité non fédérale avait le pouvoir légal de recueillir et d'utiliser l'information personnelle à des fins de cybersécurité, mais qu'il avait entrepris d'obtenir une confirmation par écrit en vue des prochaines autorisations. Je suis heureux de constater que les lettres de demande liées à la présente autorisation confirment maintenant que chaque entité non fédérale a le pouvoir légal d'acquérir de l'information à des fins de cybersécurité et de la communiquer au CST, en plus de donner au CST l'accès à ses systèmes, lesquels contiennent de l'information personnelle et des communications privées qui peuvent être acquises incidemment, utilisées, analysées, conservées ou divulguées par le CST à des fins de cybersécurité.

24. J'ai soulevé des préoccupations concernant le consentement des personnes dont l'information peut être acquise dans plusieurs décisions en matière de cybersécurité (CST-2023-02; 2024-02; 2024-05; 2024-06; 2024-07; et CST-2025-01). Bien que le CST obtienne le consentement du propriétaire ou de l'opérateur des systèmes non fédéraux à l'égard desquels il entreprend des activités de cybersécurité, contrairement aux autorisations de cybersécurité visant les systèmes fédéraux, la loi ne prévoit aucune obligation pour ce qui est de tenir compte du consentement des personnes dont l'information peut être acquise (art 34(3)b), *Loi sur le CST*).

25. Dans la décision CST-2024-06, j'ai expliqué que l'information pour laquelle il existe une attente raisonnable de protection en matière de vie privée et qui est partagée dans le système d'une entité non fédérale pourrait finir par être conservée par le CST à des fins de cybersécurité. Par conséquent, les enjeux relatifs au consentement des personnes dont l'information peut être acquise doivent demeurer des enjeux centraux et être abordés dans les autorisations de cybersécurité. Dans la décision CST-2024-07, j'ai ajouté que la confirmation des entités non fédérales concernant leur pouvoir légal de recueillir l'information et de l'utiliser à des fins de cybersécurité peut comprendre des éléments liés au consentement des utilisateurs des systèmes qui appartiennent aux entités non fédérales. De plus, dans la décision CST-2025-01, j'ai indiqué qu'il serait utile que la confirmation comprenne un aperçu des mesures prises par l'entité non fédérale pour aviser les utilisateurs de ses systèmes que leur information peut être recueillie et utilisée à des fins de cybersécurité, et pour obtenir leur consentement à cet égard.

26. En ce qui concerne la présente autorisation, le CST a entrepris de recommander aux entités non fédérales de s'assurer que leurs avis d'ouverture de session indiquent aux utilisateurs que l'information contenue ou partagée sur les appareils et les réseaux des entités peut être utilisée à des fins de cybersécurité. Cela comprend l'information personnelle et les communications privées qui peuvent être acquises incidemment et qui pourraient être utilisées, analysées, conservées ou divulguées. Je m'attends à ce que le CST informe le ministre et moi-même des éléments nouveaux liés à cette recommandation.

27. En ce qui a trait au contenu des lettres de demande, j'avais aussi fait remarquer dans la décision CST-2025-01 qu'il serait utile de donner au ministre un aperçu général des raisons pour lesquelles l'entité non fédérale sollicite le soutien du CST. Le fait d'inclure des détails supplémentaires dans la lettre de demande a l'avantage d'expliquer plus clairement l'objectif à atteindre par le CST et de s'assurer que le consentement de la partie requérante est pleinement éclairé. Je constate que des détails supplémentaires sont maintenant fournis dans les lettres de demande.

28. En ce qui concerne la communication des rapports sur la cyberdéfense aux entités non fédérales qui reçoivent des services de cybersécurité du CST, j'ai fait remarquer dans des décisions antérieures (CST-2024-02 et CST-2024-06) que le CST devrait indiquer le lien entre les

vulnérabilités incluses dans ses rapports à l'intention de l'entité et l'incidence de ces vulnérabilités sur les systèmes. Je suis satisfait de constater que la demande de cette année fournit un contexte supplémentaire relativement au contenu des rapports du CST, y compris l'incidence que les enjeux signalés par le CST pourraient avoir sur les systèmes non fédéraux.

29. Suivant l'article 14 de la *Loi sur le CR*, je dois examiner si les conclusions du ministre, qui ont été formulées au titre des paragraphes 34(1) et (3) de la *Loi sur le CST* et sur lesquelles repose l'autorisation délivrée au titre du paragraphe 27(2) de cette loi, sont raisonnables.

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

30. Le ministre a conclu qu'il avait des motifs raisonnables de croire que les activités sont raisonnables compte tenu de l'objectif qui consiste à aider à protéger l'information électronique et les infrastructures des entités non fédérales, ainsi qu'à protéger potentiellement les systèmes fédéraux et d'autres systèmes d'importance contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

31. Le ministre explique que les activités de cybersécurité énoncées dans l'autorisation présentent un risque que le CST acquière de l'information à l'égard de laquelle les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable en matière de protection de la vie privée. Étant donné que les solutions de cybersécurité acquièrent [...]. Je suis d'avis que le CST recueillera presque certainement de telles informations, ce qui fait ressortir la nécessité de cette autorisation. Je souligne, toutefois, que je suis convaincu que les activités de cybersécurité énoncées dans l'autorisation 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.

32. Pour justifier le caractère raisonnable des activités des trois entités non fédérales, le ministre se fonde sur trois motifs : 1) l'efficacité des activités pour lesquelles l'autorisation est demandée; 2) le besoin du soutien du CST compte tenu des rôles importants des entités non fédérales; et 3) la menace que représentent les auteurs de cybermenaces pour les systèmes des entités non fédérales.

33. Premièrement, les activités énoncées dans l'autorisation sont efficaces et complètent les autres activités de cybersécurité des entités non fédérales. Le ministre explique que les connaissances et les cybersolutions du CST permettent de détecter des menaces inconnues des fournisseurs commerciaux de solutions de cybersécurité et d'intervenir face à ces menaces. Le ministre explique aussi que les entités non fédérales détiennent de grandes quantités de données et, compte tenu de leur nature, sont des cibles attrayantes pour les auteurs de menaces. Ces entités détiennent également des informations […] ce qui offre aux auteurs de menaces des occasions d'exploiter les faiblesses et rend les efforts de cyberdéfense plus difficiles.

34. Les solutions de cybersécurité permettent au CST de repérer et de mieux comprendre les cyberactivités malveillantes et d'autres indicateurs de compromission afin de conseiller les entités non fédérales sur la façon de protéger leurs systèmes et sur les mesures d'atténuation à prendre. L'information que le CST recueille peut aussi l'aider à protéger les systèmes fédéraux et d'autres systèmes d'importance.

35. Le deuxième motif sur lequel se fonde le ministre est le rôle essentiel joué par les entités non fédérales. L'autorisation renouvelle les activités de cybersécurité visant à protéger […]. Je constate que […], ce qui signifie qu'il est dans l'intérêt public d'en assurer la protection, mais aussi que l'information peut être particulièrement attrayante pour les auteurs de rançongiciels. L'autorisation définit également de nouveaux pouvoirs en ce qui concerne les activités visant à repérer et à contrer les menaces hautement sophistiquées et persistantes à l'encontre de […].

36. Pour sa part, [entité C] fournit des services essentiels pour soutenir […]. Une cybercompromission pourrait causer […]. Je constate que l'autorisation actuelle à l'égard de [entité A] n'expire qu'en octobre 2025, mais je conviens avec le ministre que l'élargissement de la portée du soutien du CST pour inclure [entité C] est pressant compte tenu […].

37. Le troisième motif à l'appui de la conclusion du ministre est le contexte actuel des cybermenaces. Tel qu'il est indiqué dans la décision CST-2025-01, l'autorisation de cybersécurité a pour but d'aider à protéger les systèmes et l'information de l'entité non fédérale. La protection des systèmes ne nécessite pas de réagir à une cybercompromission. Dans les contextes où les activités de cybersécurité sont menées à des fins préventives ou proactives –

lorsqu'il n'y a pas de compromission connue ou de menace particulière pour l'entité non fédérale – le ministre doit néanmoins établir un fondement factuel pour l'aide du CST.

38. Dans l'autorisation, le ministre n'indique pas avec certitude que les entités non fédérales seront ciblées par des auteurs de cybermenaces. Cependant, le dossier décrit en détail les auteurs de cybermenaces existants et fournit de l'information sur la probabilité que les systèmes des entités non fédérales soient la cible de cyberactivités malveillantes – information que j'ai incluse à l'annexe A. La justification du ministre repose sur le fait que les cybermenaces à l'encontre des entités non fédérales sont directement liées au rôle essentiel que les entités jouent. En effet, les données relatives aux incidents liés à des rançongiciels montrent […].

39. Le CST évalue que l'entité C […].

40. Je constate que dans la décision de l'an dernier concernant [entité A], j'ai soulevé des préoccupations au sujet de certains éléments des conclusions du ministre, notamment en ce qui concerne le recours à la présence de menaces permanentes et à la mise en œuvre en suspens de recommandations du CST pour justifier la présence continue du CST dans le système. Plus précisément, j'ai fait remarquer que lors du renouvellement des autorisations de cybersécurité pour une période prolongée, le CST devrait justifier sa présence continue dans les systèmes de l'entité non fédérale et que, par conséquent, les conclusions du ministre pourraient devoir évoluer pour satisfaire à la norme de la décision raisonnable que je dois appliquer.

41. L'autorisation fournit des éclaircissements sur la justification de la présence continue du CST dans les systèmes de [entité A]. Elle fournit de l'information contextuelle supplémentaire sur la nature et le type de menaces auxquelles [entité A] fait actuellement face ainsi que sur des menaces futures […]. De plus, on sait désormais clairement quelles recommandations clés restent à mettre en œuvre et quelles en sont les répercussions sur la posture de cybersécurité de l'entité. Je suis satisfait de constater que l'information supplémentaire contenue dans le dossier répond à mes préoccupations antérieures.

42. Comme le ministre l'a expliqué, […] le contexte des cybermenaces de [entité A] et nécessite donc le déploiement par le CST de […]. Bien que les mesures prises par [entité A] aient amélioré sa posture de cybersécurité, des activités malveillantes et des vulnérabilités sont encore

détectées. L'aide continue du CST est sollicitée afin de protéger les systèmes de [entité A] contre les menaces actuelles et continues. [...] assure une posture de cybersécurité solide.

43. Je trouve convaincante la justification du ministre selon laquelle la nature des entités non fédérales en fait des cibles probables pour les auteurs de cybermenaces. Il existe un lien rationnel entre les activités de cybersécurité et l'efficacité de la protection des systèmes des entités non fédérales. Je suis également convaincu que le ministre a établi un fondement factuel suffisant en ce qui concerne la menace pour les systèmes des entités non fédérales. Par conséquent, 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*)

44. Le ministre a également conclu qu'il avait des motifs raisonnables de croire que les activités de cybersécurité autorisées du CST sont proportionnelles compte tenu de la manière dont elles sont menées, et parce qu'elles ont un lien rationnel avec l'objectif à atteindre et ne porteront qu'une atteinte minimale aux droits et libertés de « tiers », ainsi qu'à leur capacité d'accéder à de l'équipement ou à des infrastructures ou de les utiliser.

45. Le ministre indique les raisons pour lesquelles les activités sont nécessaires et utiles, notamment pour l'acquisition d'informations permettant d'aider à protéger les systèmes non fédéraux et de soutenir d'autres activités du CST. Il reconnaît que les activités autorisées peuvent mener à l'acquisition de grandes quantités d'informations afin de repérer des cybermenaces. Toutefois, le ministre fait remarquer que le CST ne conserve qu'un très faible pourcentage de la quantité totale de données acquises initialement. Je suis convaincu que les conclusions du ministre à cet égard sont raisonnables en ce qui concerne les activités autorisées.

46. Pour démontrer que les activités sont proportionnelles, le ministre énonce les mêmes mesures et contrôles internes que le CST a appliqués dans des autorisations antérieures pour assurer la protection de l'information qu'il acquiert. Je peux retracer la justification du ministre pour le recours à ces mesures et contrôles, et je suis convaincu qu'elle est raisonnable. Le ministre explique comment les activités visent à atteindre un équilibre raisonnable entre l'obtention de

l'information nécessaire et les intérêts en matière de protection de la vie privée. Le CST se penche sur tout comportement anormal lié à l'information, plutôt que sur son contenu.

47. Quant aux lois fédérales qui sont susceptibles d'être enfreintes, l'exercice de mise en balance du ministre est également évident. En effet, l'autorisation indique que les activités sont limitées en nombre, car elles ne se dérouleraient que dans des systèmes pour lesquels le CST a reçu le consentement exprès du propriétaire pour les mener. De plus, les activités doivent entrer dans la portée de celles décrites dans la demande de la chef et se limiter à l'acquisition d'informations aux fins de la protection de systèmes non fédéraux et de systèmes fédéraux. À titre de mesure de protection supplémentaire, en cas d'infraction à une loi fédérale qui ne figure pas dans la demande, la chef en informera le ministre et le commissaire au renseignement.

48. Il appert des conclusions du ministre qu'il comprend les intérêts en matière de vie privée qui sont en jeu et les mesures en place pour les protéger, ainsi que les incidences possibles sur la primauté du droit. Il a conclu, en tenant compte de ces éléments, que les activités étaient proportionnelles. J'estime que ses conclusions sont justifiées et intelligibles. En conséquence, je suis convaincu que les conclusions du ministre concernant le caractère proportionnel des activités sont raisonnables.

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

49. Lorsque le ministre estime que les activités sont raisonnables et proportionnelles au titre du paragraphe 34(1) de la *Loi sur le CST*, il peut délivrer une autorisation de cybersécurité pour aider à protéger les systèmes non fédéraux s'il conclut qu'il existe des motifs raisonnables de croire que les trois conditions énoncées au paragraphe 34(3) de la *Loi sur le CST* sont remplies, à savoir :

a) l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire;
b) l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux;
c) 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))

50. L'information est conservée conformément aux exigences définies dans les politiques du CST et est régie par un calendrier de conservation. Le ministre explique que le calendrier de conservation intègre les périodes de conservation minimales prévues par la *Loi sur la protection des renseignements personnels,* LRC (1985), c P-21, et la *Loi sur la Bibliothèque et les Archives du Canada*, LC 2004, c 11.

51. Le CST est incapable de déterminer à l'avance quelles informations seront utiles pour repérer les activités malveillantes. Par conséquent, il acquiert une grande quantité d'informations qui sont générées par les systèmes des entités non fédérales ou qui s'y trouvent. Le ministre explique que le CST traite ces informations, principalement par des méthodes automatisées. Ce processus permet de déterminer que certaines informations sont « nécessaires » ou « essentielles ». Toute autre information est considérée comme étant non évaluée, même si elle a fait l'objet du processus automatisé. La période maximale de conservation de l'information non évaluée est de 12 mois.

52. Il s'écoule souvent un certain temps entre le moment où la compromission débute et celui où elle est découverte. Comme le ministre l'a expliqué, l'efficacité des activités du CST dépend de la capacité à recouper et à analyser de multiples sources d'information déjà acquise, y compris les indicateurs de compromission découverts. De nouvelles vulnérabilités sont découvertes de façon continue, et une période de conservation de 12 mois permet au CST de remonter aux origines d'un événement ou d'examiner son évolution au fil du temps. Le fait de comparer une compromission avec des données non évaluées ou des activités malveillantes non détectées aide le CST à élaborer de meilleures mesures d'atténuation et cyberinterventions qui peuvent être utilisées non seulement pour les systèmes non fédéraux dans le cas présent, mais aussi pour les autres systèmes désignés comme étant d'importance et les systèmes fédéraux.

53. Avant la période de 12 mois, l'information non évaluée sera automatiquement supprimée, à moins qu'elle soit jugée « nécessaire » ou « essentielle » pour aider à protéger les systèmes non fédéraux, ou les systèmes fédéraux et les autres systèmes désignés comme étant d'importance. La chef indique dans la demande que les entités non fédérales sont au courant de cette utilisation de l'information et l'acceptent.

54. L'accès à l'information non évaluée est strictement contrôlé et est limité aux personnes autorisées à mener ou à soutenir des activités de cybersécurité (art 10.2, EPM). Chaque interrogation effectuée à l'égard de l'information acquise non évaluée est enregistrée à des fins d'audit et de responsabilisation. L'information non évaluée ne peut pas être transmise à d'autres organismes que le CST.

55. Le ministre souligne également que le programme interne de conformité du CST a établi un processus d'intervention en cas d'incidents. Tant que les processus fonctionnent comme prévu, l'approche à plusieurs niveaux permet au CST de maintenir des mesures strictes de protection de la vie privée.

56. Comme il est expliqué dans le dossier, 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. L'information est jugée « nécessaire » lorsqu'elle est requise pour comprendre une cyberactivité malveillante, y compris [...], dans le but d'aider à protéger les systèmes non fédéraux. Le but est d'aider à réaliser des analyses de détection et de prévention et à renforcer davantage l'écosystème de cyberdéfense.

57. En revanche, le critère du caractère « essentiel » s'applique à l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada. Sans cette information, le CST ne serait pas en mesure de découvrir, d'isoler, de prévenir ou d'atténuer des dommages au système non fédéral. Cela peut inclure [...]. L'information acquise peut être très sensible pour les Canadiens, et la plupart des analyses sont effectuées au moyen de processus automatisés, qui signalent des comportements anormaux et limitent l'exposition des employés au contenu des dossiers.

58. L'information qui est jugée nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer des dommages peut être conservée « indéfiniment ou jusqu'à ce qu'elle ne soit plus utile à ces

fins ». Cette information fait l'objet d'un suivi et, tous les trimestres, les gestionnaires de l'exploitation « doivent examiner » l'information reconnue conservée qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada afin de valider de nouveau si elle est toujours essentielle.

59. Compte tenu des multiples niveaux de contrôles internes et de limites visant l'accès à l'information non évaluée, 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 ainsi que 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.

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

60. Les activités de cybersécurité du CST ne sont efficaces que si elles permettent d'acquérir une vaste gamme d'informations qui sont ensuite évaluées pour repérer des activités malveillantes. Le CST ne peut pas prédire [...] et doit donc acquérir une quantité importante d'informations. Étant donné que les systèmes non fédéraux sont situés au Canada, le CST acquerra incidemment de l'information qui portera atteinte à l'attente raisonnable en matière de protection de la vie privée des Canadiens et des personnes se trouvant au Canada.

61. Le ministre explique que, bien que des plateformes de cybersécurité commerciales soient actuellement utilisées par les entités non fédérales, elles « ne sont pas suffisantes pour repérer et contrer les cybermenaces persistantes et de plus en plus complexes ». Comme on l'a fait remarquer dans la décision de l'an dernier concernant les activités de cybersécurité du CST (CST-2024-06), il n'est pas clair si les mesures de sécurité disponibles sur le marché seront suffisantes un jour pour protéger pleinement les systèmes des entités non fédérales et les

systèmes fédéraux. Il ne faut pas être alarmiste, mais l'expertise du CST est devenue de plus en plus importante pour répondre aux cybermenaces de plus en plus complexes et sophistiquées.

62. Enfin, le ministre donne des exemples de la façon dont l'information acquise au titre de cette autorisation peut aussi être utilisée par le CST pour soutenir des activités au titre d'autres autorisations de cybersécurité et dans le cadre d'autres volets de son mandat. 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 divulgation ultérieures de toute information acquise au titre de l'autorisation sont assujetties aux restrictions et aux conditions énoncées dans l'EPM.

63. Pour ces motifs, je suis convaincu que les conclusions du ministre sont raisonnables.

iii. Les mesures visant à protéger la vie privée 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 (alinéa 34(3)d))

64. 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 divulgation de l'information qui se rapporte à eux et qui a été acquise dans la réalisation des volets de son mandat touchant la cybersécurité et l'assurance de l'information. Je souligne que ces mesures revêtent une importance encore plus grande lorsque le rôle 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 en matière de protection de la vie privée – ce qui est le cas de [entité A et de l'information qu'elle acquiert].

65. En ce qui concerne la conservation de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada (IRC), le ministre réitère que l'information ne peut être conservée que si elle est jugée essentielle, ce qui signifie que sans cette information, le CST ne serait pas en mesure de découvrir, d'isoler ou de prévenir des dommages au système de l'entité non fédérale. Les justifications relatives au caractère essentiel doivent être consignées par les

employés (art 8.2.2, EPM). À mon avis, ces mesures contribuent à faire en sorte que le CST respecte son obligation législative prévue à l'article 24 et appuient les conclusions du ministre.

66. Pour que le CST divulgue de l'IRC, il faut que la divulgation soit nécessaire pour aider à protéger les systèmes non fédéraux, les systèmes fédéraux ou d'autres systèmes d'importance. Les conclusions du ministre et le dossier reflètent l'obligation législative prévue à l'article 44 de la *Loi sur le CST*. L'information n'est divulguée 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*, pris le 13 juin 2023 en application de l'article 45 de la *Loi sur le CST*. Ces destinataires comprennent les propriétaires ou les administrateurs d'un système ou d'un réseau informatique utilisé 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.

67. Avant de divulguer de l'IRC, le CST met également en place des mesures qui doivent être suivies (art 24, EPM). Une des méthodes utilisées par le CST consiste à supprimer l'information permettant d'identifier une personne. En cas de divulgation d'IRC, l'EPM définit les niveaux d'approbation requis pour la divulgation, lesquels doivent être documentés.

68. Je constate que dans les lettres de demande adressées au CST, chaque entité non fédérale a demandé que tous ses renseignements exclusifs et tous les renseignements personnels qui pourraient être recueillis et conservés soient masqués avant d'être communiqués au-delà de l'entité et du CST.

69. L'EPM établit des politiques complexes visant à contrôler et à protéger l'IRC qui est acquise au titre d'une autorisation de cybersécurité. À mon avis, lorsqu'elles sont suivies, ces mesures permettent au CST de respecter efficacement l'obligation législative de protéger suffisamment cette information. Par conséquent, je suis convaincu que la conclusion du ministre est raisonnable.

V. REMARQUES

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

A. Portée de l'autorisation

71. Dans la lettre de demande de [entité B], le [représentant autorisé de l'entité] demande au CST « d'aider à protéger l'information électronique et les infrastructures de l'information sous le contrôle et la supervision » de son bureau. Selon le dossier, [description des infrastructures de l'information].

72. Cependant, le dossier indique également […] autres [entités] qui « font partie du réseau de [entité B] ». [Entité C] est l'une des [entités] supplémentaires énumérées qui […]. La nature de certaines de ces [entités] laisse entendre qu'elles peuvent détenir des informations particulièrement sensibles […]. [Entité C] est la seule entité parmi celles énumérées pour laquelle une lettre de demande est jointe au dossier, et pour laquelle […].

73. L'autorisation indique que le CST peut déterminer quand et pour quelle [entité] le CST accepte les demandes de mener des activités touchant la cybersécurité et l'assurance de l'information, à condition que [entité B] soit le propriétaire des infrastructures en question. Le CST doit informer le ministre lorsqu'il accepte une telle demande et en informer par la suite le commissaire au renseignement.

74. Bien que l'autorisation indique clairement que le CST ne peut mener des activités que pour des infrastructures qui appartiennent à [entité B] compte tenu du fait que des [entités] supplémentaires énumérées sont répertoriées comme étant « au sein du système d'[entité B] », je tiens à préciser qu'aucune activité liée à l'infrastructure utilisée par ces [entités] qui n'appartiennent pas à [entité B] n'est autorisée.

VI. CONCLUSIONS

75. D'après mon examen du dossier transmis, je suis convaincu que les conclusions tirées par le ministre en application des paragraphes 34(1) et (3) de la *Loi sur le CST* à l'égard des activités énumérées au paragraphe 87 de l'autorisation sont raisonnables.

76. 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 [...].

77. 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.

78. 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 accomplir 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.

Le 2 juillet 2025

(Original signé)

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