Dossier : CST-2025-03

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 VISANT À AIDER À PROTÉGER DES INFRASTRUCTURES FÉDÉRALES EN VERTU DU PARAGRAPHE 27(1) 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 16 AVRIL 2025

Canada

TABLE DES MATIÈRES

I. APERÇU 1
II. CONTEXTE 2
III. NORME DE CONTRÔLE 4
IV. ANALYSE 5
A. Dossier mis à jour 6
B. Paragraphe 34(1) de la *Loi sur le CST* – déterminer si les activités sont raisonnables et proportionnelles 8
i. Examen des conclusions du ministre selon lesquelles les activités en cause sont raisonnables 8
ii. Examen des conclusions du ministre selon lesquelles les activités en cause sont proportionnelles 11
C. Paragraphe 34(3) de la *Loi sur le CST* – les conditions nécessaires à la délivrance d'une autorisation 13
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)) 13
ii. Le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu (alinéa 34(3)b)) 15
iii. L'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux (alinéa 34(3)c)) 16
iv. Les mesures pour protéger la vie privée permettront d'assurer que l'information acquise au titre de l'autorisation 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 informations électroniques ou aux infrastructures de l'information des institutions fédérales (alinéa 34(3)d)) 17
V. REMARQUES 19
A. Clarification de la remarque formulée dans la décision CST-2024-02 19
VI. CONCLUSIONS 21

I. APERÇU

1. Il s'agit d'une décision concernant l'examen des conclusions du ministre de la Défense nationale (le ministre) concernant une autorisation de cybersécurité pour des activités visant à protéger des infrastructures fédérales (autorisation) délivrée le 23 février 2025, en vertu de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*). L'autorisation vise le renouvellement des activités autorisées approuvées par le commissaire au renseignement dans la décision CST-2024-02, et aucune nouvelle autorisation opérationnelle n'est demandée.

2. Le Centre de la sécurité des télécommunications (CST) a pour mandat de mener des activités de cyberprotection afin de défendre les systèmes électroniques, les appareils et les réseaux du gouvernement fédéral ainsi que l'information qu'ils contiennent contre les cybercriminels et les cybermenaces parrainés par des États étrangers. Le CST fournit également des conseils et une orientation en vue de renforcer l'approche des institutions du Parlement et du gouvernement fédéral en matière de cybersécurité, par exemple, les ministères fédéraux, les organismes gouvernementaux et les sociétés d'État.

3. Pour mener efficacement ses activités de cyberprotection, le CST peut devoir contrevenir à certaines lois canadiennes. Il peut acquérir incidemment des communications ou de l'information qui portent atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens ou des personnes se trouvant au Canada. Avant d'entreprendre des activités pouvant avoir ces effets, le CST doit obtenir une autorisation délivrée par le ministre et approuvée par le commissaire au renseignement.

4. Le 24 février 2025, le Bureau du commissaire au renseignement a reçu l'autorisation que je dois examiner et approuver en vertu de la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*). Conformément à la *Loi sur le CR*, le commissaire au renseignement doit fournir une décision écrite dans les 30 jours suivant la date de réception de l'autorisation ou avant l'expiration de tout autre délai convenu avec le ministre (art 20(3)). Pour cette autorisation, le ministre et moi avons convenu que je ferai connaître ma décision au plus tard le 18 avril 2025. Nous avons convenu de cette date afin de mieux tenir compte de l'autorisation précédente, qui ne devait pas expirer avant le 13 mai 2025.

5. Pour les motifs ci-après, je suis convaincu que les conclusions du ministre relativement aux activités et aux catégories d'activités énumérées au paragraphe 50 de l'autorisation sont raisonnables.

6. Par conséquent, conformément à l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation.

II. CONTEXTE

7. Le CST est l'organisme national du renseignement électromagnétique en matière de renseignement étranger et l'expert technique de la cybersécurité et de l'assurance de l'information (art 15(1), *Loi sur le CST*). Le contexte législatif détaillé des activités de cybersécurité du CST est énoncé dans des décisions antérieures du commissaire au renseignement concernant la cybersécurité, accessibles sur le site Web du BCR.

8. Afin de comprendre les vulnérabilités et les atteintes à l'intégrité des systèmes fédéraux, le CST doit accéder à ces systèmes et acquérir de l'information provenant de ceux-ci. 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 ou des personnes se trouvant au Canada (art 22(4), 27, *Loi sur le CST*).

9. Pour délivrer l'autorisation, le ministre doit entre autres conclure que les activités envisagées sont raisonnables et proportionnelles, et que des mesures pour protéger la vie privée des Canadiens sont en place (art 24 et 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*).

10. Pour approuver les activités ou les catégories d'activités précisées dans l'autorisation, le commissaire au renseignement doit être convaincu que les conclusions du ministre – essentiellement les motifs justifiant la délivrance de l'autorisation – sont raisonnables (art 14, *Loi sur le CR*). Ce n'est qu'à ce moment que le CST peut exercer les activités autorisées.

11. Malgré une autorisation, la *Loi sur le CST* impose des limites quant aux activités de cybersécurité du CST. Le CST ne doit pas diriger ses activités vers un Canadien ou une personne se trouvant au Canada, ni porter atteinte à la *Charte canadienne des droits et libertés* (la *Charte*) (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 » signifie que l'information acquise n'a pas été délibérément recherchée (art 23(5), *Loi sur le CST*).

12. 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 datée du 23 février 2025;
    b) la demande de la chef du CST (la chef), datée du 20 février 2025, qui comprend les huit annexes suivantes :
        i) Liste des institutions fédérales recevant des services de cybersécurité du CST;
        ii) Arrêté ministériel – personnes désignées en application de l'article 45 de la *Loi sur le CST*, daté du 13 juin 2023;
        iii) Avis de surveillance du réseau du CST;
        iv) Rapport sur les résultats des activités de 2024;
        v) Évaluation de la compromission d'une institution fédérale;
        vi) Tableau de conservation et de suppression;
        vii) Ensemble des politiques sur la mission en matière de cybersécurité (EPM), approuvé le 14 février 2025;
        viii) Registre des modifications apportées à l'EPM;
        ix) [redacted];
    c) la note d'information de la chef à l'intention du ministre, datée du 20 février 2025;
    d) le document d'information – aperçu des activités;
    e) des documents supplémentaires pour le dossier, y compris des présentations au commissaire au renseignement et au personnel, datant de janvier 2025.

III. NORME DE CONTRÔLE

13. La *Loi sur le CR* exige que le commissaire au renseignement examine si les conclusions du ministre sont raisonnables. J'appliquerai donc la norme de la décision raisonnable, tel qu'elle est appliquée dans les contrôles judiciaires de mesures administratives.

14. 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 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.

15. Les contraintes factuelles et juridiques pertinentes peuvent comprendre le régime législatif applicable, l'incidence de la décision et les principes d'interprétation des lois. Le régime législatif établi par la *Loi sur le CR* et la *Loi sur le CST*, de même que les débats législatifs connexes, montre que le législateur a créé la fonction de commissaire au renseignement pour servir de mécanisme indépendant afin de garantir que les mesures gouvernementales en matière de sécurité nationale et de renseignement établiraient un équilibre entre la primauté du droit et les droits et libertés des Canadiens.

16. 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*). Si, au contraire, les conclusions sont jugées déraisonnables, il « n'approuve pas l'autorisation » (art 20(1)b), *Loi sur le CR*).

IV. ANALYSE

17. Le 20 février 2025, la chef a présenté une demande écrite en vue d'obtenir une autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales (demande) au ministre. La demande énonce les activités de cybersécurité que le CST souhaite mener pour accéder aux systèmes des institutions fédérales et acquérir de l'information qui provient ou passe par les infrastructures d'information afin de les protéger contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

18. La demande décrit les solutions de cybersécurité déployées dans les systèmes fédéraux – avec le consentement des institutions 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 : (1) solutions au niveau de l'hôte (SNH) – capteurs installés sur des dispositifs d'extrémité physiques ou virtuels (p. ex., postes de travail et serveurs); (2) solutions axées sur les réseaux (SAR) – capteurs installés au niveau du réseau qui copient le trafic sur le réseau; et (3) solutions infonuagiques (SI) – capacités semblables aux SNH et aux SAR dans un environnement infonuagique.

19. La demande décrit également comment la chef propose que le CST analyse, traite et conserve 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.

20. À la lumière des faits présentés dans la demande de la chef, le ministre a conclu qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions énoncées aux paragraphes 34(1) et (3) de la *Loi sur le CST* ont été remplies.

21. Par conséquent, le ministre a délivré une autorisation avec une période de validité d'un an au CST pour mener les activités énoncées au paragraphe 50 de l'autorisation :

    a) accéder à un système fédéral et déployer, à la demande d'un client fédéral, des SNH, des SAR et des SI;

b) acquérir de l'information, au moyen des SNH, SNR et SI, y compris de l'information qui est identifiée comme se rapportant à des Canadiens ou à des personnes se trouvant au Canada, qui provient ou passe par les systèmes fédéraux;
c) utiliser, analyser, conserver ou divulguer de l'information acquise en vertu de la présente autorisation pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux;
d) prendre des mesures d'atténuation, comme il est décrit dans la demande, pour contrer les cybermenaces.

22. Les activités de cybersécurité énumérées dans l'autorisation sont les mêmes que celles que j'ai approuvées l'année dernière. Néanmoins, selon la jurisprudence du commissaire au renseignement, le ministre doit avoir la meilleure information disponible pour décider s'il doit autoriser des activités. Cela signifie que, l'information contenue dans l'autorisation, ainsi que les documents à l'appui, doivent être mis à jour pour refléter les activités opérationnelles les plus récentes entreprises par le CST. La façon dont les activités ont été entreprises par le passé peut être un facteur qui permet d'établir si les conclusions du ministre sont raisonnables.

A. Dossier mis à jour

23. Je suis convaincu que le dossier actuel indique qu'il s'agit d'une autorisation nouvelle et distincte. Le dossier contient également de nouveaux renseignements qui tiennent compte des remarques que j'ai faites dans ma décision de 2024 (CST-2024-02).

24. En réponse à ma remarque concernant le libellé utilisé dans les avis aux utilisateurs pour les informer de l'utilisation potentielle de l'information communiquée dans les systèmes fédéraux, le CST a joint une copie de son propre avis de surveillance de réseau révisé. Conformément à ma remarque, l'avis révisé mentionne clairement l'acquisition et l'utilisation potentielles de l'information à des fins de cybersécurité, indiquant que des « [r]enseignements personnels recueillis au moyen de pratiques de surveillance […] pourraient également être recueillis, utilisés, analysés, conservés ou divulgués à des fins de cybersécurité. » Je comprends, d'après le dossier, que le même avis sera utilisé par le SCRS et que le CST recommande aux partenaires fédéraux de revoir leurs propres avis d'ouverture de session pour s'assurer qu'ils sont aussi clairs.

25. En réponse à ma remarque selon laquelle il serait utile d'inclure des renseignements plus détaillés sur la communication de rapports à l'extérieur du CST, le rapport sur les résultats indique maintenant avec précision le nombre de rapports de cyberdéfense communiqués à des partenaires internationaux et le nombre de ces rapports qui contenaient de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada (IRC). J'accueille également avec satisfaction l'ajout de renseignements sur les mises en garde et les autres mesures mises en place conformément à l'EPM afin de limiter davantage la divulgation d'IRC. La demande fournit également plus de précisions sur les contrôles internes « multicouches » utilisés par les employés du CST pour s'assurer que l'information conservée est conforme à l'autorisation.

26. En ce qui concerne ma remarque soulignant l'importance d'indiquer clairement toute communication protégée par le secret professionnel de l'avocat acquise incidemment, le rapport sur les résultats au dossier comprend maintenant une section indiquant clairement si des communications protégées par le secret professionnel de l'avocat reconnues ont été utilisées, analysées, conservées ou divulguées (aucune n'a été faite et je suis convaincu que, si de telles communications avaient été acquises incidemment et supprimées immédiatement, elles auraient également été indiquées). Une mise à jour correspondante de l'EPM confirme maintenant que la chef m'informera si elle décide d'utiliser, d'analyser, de conserver ou de communiquer des communications protégées par le secret professionnel de l'avocat.

27. En ce qui concerne l'EPM mis à jour, le dossier comprend un tableau indiquant les sections qui ont été modifiées. Ce tableau est utile et tient compte d'une remarque que j'ai faite dans la décision CST-2023-05, demandant que toute modification pertinente apportée à l'EPM soit portée à l'attention du ministre et à mon attention.

28. Enfin, je souligne que les autorisations précédentes et actuelles contiennent une condition selon laquelle le CST doit informer le ministre lorsqu'il accepte une demande pour mener des activités en vertu de l'autorisation d'une institution fédérale qui ne reçoit pas, à l'heure actuelle, des services de cybersécurité du CST, et que le CST doit m'en informer par la suite.

J'ai reçu cette information dans les rapports de fin d'autorisation exigés par la loi (art 52, *Loi sur le CST*).

29. Suivant l'article 14 de la *Loi sur le CR*, relativement à la délivrance d'une autorisation de cybersécurité, je dois examiner si les conclusions du ministre sur lesquelles repose l'autorisation délivrée sont raisonnables.

B. Paragraphe 34(1) de la *Loi sur le CST* – déterminer si les activités sont raisonnables et proportionnelles

i. Examen des conclusions du ministre selon lesquelles les activités en cause sont raisonnables

30. Pour délivrer une autorisation de cybersécurité, le ministre doit conclure « qu'il y a des motifs raisonnables de croire que l'activité en cause (*any activity* en anglais) est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités » (art 34(1), *Loi sur le CST*). Le ministre a conclu, au paragraphe 15 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités étaient raisonnables, compte tenu de l'objectif d'aider à protéger les systèmes fédéraux contre les méfaits, l'utilisation non autorisée ou la perturbation.

31. Le ministre explique que les activités de cybersécurité énumérées 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. Les systèmes fédéraux sont [...] et la grande majorité de l'information qui est stockée se rapporte à des Canadiens et à des personnes se trouvant au Canada. De plus, l'information contenue dans les systèmes ne se limite pas à des renseignements au sujet des employés des institutions fédérales qui reçoivent une assistance en matière de cybersécurité du CST, mais comprend également de l'information provenant de membres du public canadien qui, par exemple, communiquent avec les institutions par courriel. Il en ressort la nécessité de l'autorisation ainsi que la mise en œuvre efficace par le CST de mesures de contrôle pour protéger la vie privée. Je souligne que les activités énumérées dans

l'autorisation visent néanmoins les cybermenaces et ne visent ni les Canadiens ni les personnes se trouvant au Canada.

32. Le ministre justifie les activités autorisées en se fondant sur les deux mêmes raisons principales que l'année dernière : 1) l'efficacité des activités pour lesquelles l'autorisation est demandée; et 2) la nécessité que le CST participe à l'intervention en matière de cybersécurité compte tenu des menaces à l'égard des systèmes fédéraux.

33. Premièrement, les activités du CST consistent à déployer des outils avancés d'analyse des logiciels malveillants et des capacités automatisées de cybersécurité. L'information acquise dans le cadre de ces activités aide le CST à protéger les systèmes fédéraux. Le ministre explique que les connaissances et les cybersolutions du CST lui permettent de détecter des menaces inconnues des fournisseurs commerciaux de cybersécurité et d'intervenir face à ces menaces. Le renseignement spécialisé du CST sur les acteurs malveillants et le déploiement de ses outils et capacités uniques dès que possible appuient également la conclusion du ministre selon laquelle les activités sont efficaces et raisonnables.

34. Je suis d'accord avec le ministre que les activités exposées dans l'autorisation permettent au CST de conseiller les institutions fédérales et de mieux protéger leurs systèmes. Dans le cadre des activités, le CST pourrait recommander des mesures d'atténuation et les mener avec le consentement des institutions fédérales. Le rapport sur les résultats indique le nombre d'événements malveillants détectés sur les systèmes fédéraux de mai à octobre 2024 et confirme l'efficacité des solutions de cybersécurité du CST. Je souligne que le nombre d'événements malveillants détectés a presque triplé depuis l'autorisation de 2023 à 2024, et je remercie le CST d'avoir inclus une explication (en lien avec une remarque que j'ai formulée dans la décision de l'année dernière concernant la mise en contexte des changements dans le volume ou la nature des menaces détectées) selon laquelle les facteurs sont multiples, notamment une augmentation des activités de balayage et l'élaboration de nouvelles analyses pour découvrir les événements malveillants.

35. Je prends également note des exemples précis fournis dans la demande de la chef qui indiquent les façons dont les solutions de cybersécurité à déployer ont été utilisées pour

détecter les incidents de cybersécurité et intervenir. Comme le ministre l'a souligné, au cours des dernières années, les solutions de cybersécurité du CST ont joué un rôle déterminant pour détecter de plusieurs compromissions dans les systèmes fédéraux. Néanmoins, malgré l'efficacité des solutions de cybersécurité, les systèmes fédéraux peuvent toujours être compromis. En effet, le dossier contient de l'information sur la compromission du réseau [...] entre [...], même si les solutions de cybersécurité du CST avaient été déployées et ont finalement mené à la détection de l'intrusion.

36. Le deuxième motif qui appuie les conclusions du ministre selon lesquelles les activités sont raisonnables à l'égard du contexte actuel des cybermenaces. Comme l'a expliqué le ministre, les cybermenaces de criminels de haut calibre et d'acteurs parrainés par des États contre les systèmes fédéraux sont de plus en plus fréquentes et sophistiquées. Les auteurs de menaces utilisent des techniques efficaces et profitent d'une multitude de points d'entrée et de méthodes pour infiltrer les infrastructures d'information au niveau de l'hôte, du réseau ou du nuage.

37. De plus, les systèmes fédéraux sont vastes et complexes, et ils ont été créés et sont maintenus à des fins différentes et par diverses parties au fil des ans. Les pratiques en matière de sécurité de l'information diffèrent considérablement d'une institution fédérale à l'autre, ce qui augmente le risque de cybermenaces. En utilisant les grandes quantités d'information qu'il acquiert au moyen de ses solutions de cybersécurité et en analysant plus en profondeur les activités anormales, le CST est en mesure de détecter les menaces et de protéger de façon proactive les institutions fédérales qui ne pourraient pas découvrir les menaces par elles-mêmes. Comme l'a dit le ministre, cela donne lieu à un « renforcement global des systèmes fédéraux et des systèmes [désignés comme] d'importance. Les techniques de cybersécurité du CST font partie d'un écosystème de protection, dans le cadre duquel la découverte d'une menace se traduit par une protection pour tous. »

38. Je suis convaincu que le ministre a établi un fondement factuel suffisant en ce qui concerne la menace pour les systèmes fédéraux. Les conclusions démontrent qu'il existe un lien rationnel entre les activités précisées dans l'autorisation et l'objectif de protéger les systèmes fédéraux contre les méfaits, l'utilisation non autorisée ou la perturbation. Le dossier montre également

que les activités du CST sont non seulement nécessaires pour aider à protéger les systèmes fédéraux, mais elles servent aussi de mesure de protection de la vie privée, compte tenu de leur efficacité à prévenir et à atténuer les compromissions. Par conséquent, j'estime que les conclusions du ministre quant au caractère raisonnable des activités énoncées dans l'autorisation sont raisonnables.

ii. Examen des conclusions du ministre selon lesquelles les activités en cause sont proportionnelles

39. Le ministre a conclu, au paragraphe 20 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités autorisées au paragraphe 50 de l'autorisation sont « proportionnelles vu la manière dont elles sont menées ». Le ministre présente les mêmes mesures et contrôles énumérés dans l'autorisation de l'année dernière (CST-2024-02), maintenant divisés en exigences prévues par la loi et en mesures et contrôles internes supplémentaires. Il indique les raisons pour lesquelles les activités sont nécessaires et utiles, notamment pour acquérir de l'information permettant d'aider à protéger les systèmes fédéraux et de soutenir d'autres activités du CST. Il reconnaît que les activités autorisées peuvent mener à l'acquisition d'un grand volume d'information auprès de plusieurs plateformes afin de détecter les menaces. 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.

40. En ce qui a trait aux mesures et aux contrôles, je peux retracer la justification du ministre pour y recourir, et je suis convaincu qu'elle est raisonnable. Premièrement, le ministre reconnaît que le CST a un accès étendu aux systèmes fédéraux. Pour mener efficacement des activités de cybersécurité, le CST doit obtenir une grande quantité d'informations, notamment des fichiers, des courriels et des messages de clavardage à l'égard desquels les Canadiens et les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée. Les mesures à l'appui de ses conclusions relatives à la proportionnalité seront appliquées après l'acquisition de l'information, car le CST doit d'abord acquérir l'information pour que les solutions de cybersécurité soient efficaces.

41. Deuxièmement, le CST emploie plusieurs couches de contrôles internes pour protéger les renseignements qu'il acquiert. Par exemple, l'accès à l'information acquise est limité aux employés désignés du CST qui sont formés pour manipuler ce type d'information et qui l'utilisent selon le principe du besoin de savoir pour effectuer leur travail, et le programme de conformité interne du CST a établi un processus d'intervention en cas d'incident.

42. Lorsqu'il tient compte de l'objectif et de la nature des activités, le ministre a également procédé à un exercice de mise en balance de ce qu'il considère comme des intérêts d'importance, notamment l'acquisition de l'information et la protection de la vie privée des Canadiens et des personnes se trouvant au Canada. Il décrit comment les activités cherchent à atteindre un équilibre raisonnable entre les objectifs de cybersécurité et l'atteinte éventuelle aux droits en matière de vie privée. 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. Si de l'information à l'égard de laquelle les Canadiens ou les personnes se trouvent au Canada ont un droit en matière de vie privée est acquise et conservée, l'accès à cette information et son utilisation seraient limités.

43. Enfin, l'exercice de mise en balance du ministre est indéniable lorsqu'il expose les lois fédérales qui pourraient être enfreintes. Il explique qu'il y a une faible possibilité que des infractions au *Code criminel* soient commises au-delà de celles énumérées dans la demande et que d'autres lois fédérales puissent être enfreintes, selon les circonstances de l'activité menée. Il indique qu'il y en a peu, parce que les activités se dérouleraient uniquement sur les systèmes des institutions fédérales consentantes. De plus, les activités doivent entrer dans la portée de celles décrites dans la demande de la chef et se limiter à l'acquisition de l'information pour protéger les systèmes fédéraux et les systèmes désignés d'importance pour le gouvernement fédéral. En cas de contravention à une loi fédérale qui n'est pas mentionnée dans la demande – par exemple, le CST sait à l'avance que les activités entraîneront une contravention à une loi fédérale qui n'est pas mentionnée dans la demande ou le CST contrevient à une loi fédérale qui n'est pas mentionnée, sans le savoir à l'avance – la chef en informera le ministre et le commissaire au renseignement.

44. Pour ces motifs, je suis convaincu que les droits en matière de vie privée des Canadiens et des personnes se trouvant au Canada ont été pris en compte et que la mise en balance est raisonnable. De plus, je suis convaincu qu'en cas de contravention à une loi fédérale, les conséquences négatives de cette contravention seront limitées. Par conséquent, je suis convaincu que les conclusions du ministre concernant la proportionnalité des activités sont raisonnables.

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

45. Lorsque le ministre estime que les activités sont raisonnables et proportionnelles en vertu du paragraphe 34(1) de la *Loi sur le CST*, il peut délivrer une autorisation de cybersécurité s'il conclut qu'il a des motifs raisonnables de croire que les quatre conditions 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. le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu;
iii. l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information des institutions fédérales;
iv. les mesures visées à l'article 24 de la *Loi sur le CST* 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 informations électroniques ou aux infrastructures de l'information des institutions fédérales.

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))

46. Les conclusions du ministre établissent un lien entre les types d'information et leur période de conservation. Elles expliquent également pourquoi les différentes périodes de conservation sont nécessaires pour des motifs opérationnels. L'information est conservée conformément aux exigences énoncées dans l'EPM ainsi que dans 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, et est régie par un calendrier de conservation.

47. Le CST emploie plusieurs mesures internes pour assurer la protection de l'information qu'il acquiert et pour maintenir une protection rigoureuse de la vie privée. L'information acquise est initialement soumise à des processus automatisés pour déterminer si le CST devrait la conserver parce qu'elle est nécessaire ou essentielle à des fins de cybersécurité. Si l'information n'est pas initialement signalée comme étant nécessaire ou essentielle, elle est classée comme étant non évaluée. Le ministre explique que l'information non évaluée est conservée pendant un maximum de […] afin de permettre au CST de l'utiliser pour examiner les vulnérabilités nouvellement découvertes au fil du temps. Le ministre énumère les mesures de protection en place pour assurer le respect de cette période de conservation.

48. Conformément à l'EPM, cette information doit être strictement contrôlée et son accès doit être limité aux membres du personnel autorisés à mener ou à soutenir des activités de cybersécurité. De plus, la liste des membres du personnel fait l'objet d'un suivi aux fins de reddition de comptes, et l'information non évaluée ne peut pas être communiquée à l'extérieur du CST.

49. Le critère du caractère « nécessaire » s'applique à l'information qui ne se rapporte pas à des Canadiens ou à des personnes se trouvant au Canada; quant au critère du caractère « essentiel », il s'applique à l'information qui s'y rapporte. Essentiellement, l'information est jugée « nécessaire » pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux lorsqu'elle est requise pour comprendre la cyberactivité malveillante, […], dans le but d'aider à protéger les systèmes fédéraux. Cette information […]

50. L'IRC est considérée comme essentielle si, sans elle, le CST ne peut pas découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux. Elle peut inclure […] L'information acquise peut être très sensible pour les Canadiens et les personnes se trouvant au Canada, 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 fichiers.

51. L'information qui est jugée nécessaire ou essentielle peut être conservée jusqu'à ce qu'elle ne soit plus utile à ces fins, […]. Conformément à l'EPM, cette information doit faire l'objet d'un suivi. De plus, le programme de conformité interne du CST intervient en cas d'incident et fait circuler des rappels trimestriels aux analystes de la cybersécurité pour s'assurer que l'information qui n'a pas été jugée comme nécessaire ou essentielle est supprimée dans […] après l'acquisition. De plus, les gestionnaires des opérations « doivent examiner » l'IRC reconnue conservée tous les trimestres pour confirmer à nouveau si elle est toujours essentielle. L'information qui n'est plus essentielle doit être supprimée.

52. Je remarque qu'il y a toujours une divergence avec l'EPM mis à jour, qui comprend maintenant une mention de l'examen trimestriel indiquant qu'on rappelle aux gestionnaires des opérations d'examiner l'IRC reconnue pour confirmer à nouveau si elle est toujours essentielle. J'ai déjà soulevé que le dossier pourrait bénéficier d'une plus grande clarté en ce qui concerne les différents libellés utilisés dans le cadre de l'examen trimestriel dans une décision antérieure en matière de cybersécurité (CST-2025-01).

53. Je suis d'avis que la conservation de l'information pour la durée nécessaire permet au CST de mettre au point les cyberinterventions nécessaires pour suivre l'évolution du savoir-faire des auteurs de menaces utilisant des logiciels malveillants. Ainsi, les systèmes fédéraux ainsi que des systèmes désignés d'importance sont mieux protégés.

54. Compte tenu des mesures pour protéger l'IRC et limiter l'accès à l'information non évaluée, j'estime raisonnable la conclusion du ministre concernant la période d'évaluation de […]. 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 fédéraux peut être conservée jusqu'à ce qu'elle ne soit plus utile.

ii. Le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu (alinéa 34(3)b))

55. Avant de déployer ses solutions de cybersécurité, le CST obtient le consentement par écrit des propriétaires des systèmes fédéraux qui autorisent le CST à accéder à leurs systèmes. De

plus, conformément à la pratique courante du gouvernement fédéral, les propriétaires de systèmes fédéraux doivent informer leurs utilisateurs, notamment les employés, que leurs dispositifs de travail et leurs activités sur le réseau sont surveillés à des fins de cybersécurité et d'assurance de l'information.

56. Comme l'a expliqué le ministre, « [e]n reconnaissant cet avis, les utilisateurs démontrent leur consentement au propriétaire du système fédéral avec qui le CST a convenu de fournir ces services de cybersécurité ». Cependant, il arrive parfois qu'il soit impossible d'obtenir le consentement des personnes dont l'information peut être acquise par le CST dans le cadre d'activités de cybersécurité. Il peut s'agir, par exemple, du consentement des personnes qui communiquent avec des fonctionnaires fédéraux par courriel ou par clavardage. Pour remédier à cette situation qui a été soulevée dans ma décision précédente, CST-2024-02, le CST s'est efforcé d'évaluer la faisabilité de donner un avis aux utilisateurs externes, ce qui, à mon avis, serait utile.

57. J'estime que la conclusion du ministre à l'égard de cette condition est raisonnable.

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

58. Le CST ne peut pas prédire le trafic réseau, les fichiers ou les processus qui seront ou sont utilisés de façon malveillante. Afin de surveiller efficacement les systèmes fédéraux et d'atténuer les éventuelles cybermenaces, le CST doit acquérir une vaste gamme d'informations, y compris le trafic réseau, les fichiers, les courriels et les messages de clavardage. Bien que le contenu des fichiers et des communications puisse sembler légitime pour le destinataire, il peut comprendre des codes ou des liens malveillants qui permettent à l'auteur de menace d'installer un logiciel malveillant sur l'ordinateur d'une cible.

59. Le ministre explique comment les auteurs de menaces déguisent leurs activités et leurs comportements malveillants afin de réduire la probabilité d'être découverts, et donne des exemples. Le CST ne peut pas obtenir les mêmes résultats en utilisant différentes solutions de cybersécurité qui permettent d'obtenir moins d'information, y compris l'IRC. Par

conséquent, les solutions de cybersécurité sont efficaces uniquement en raison de l'acquisition de « n'importe quelle » information.

60. Les conclusions du ministre contiennent des exemples de la façon dont le CST peut 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. Cependant, avant de pouvoir utiliser l'IRC, elle doit avoir été jugée 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.

61. Le ministre a expliqué pourquoi il a des motifs raisonnables de croire que l'acquisition de l'information est nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux. Je suis donc convaincu que les conclusions du ministre dans ce sens sont raisonnables.

iv. Les mesures pour protéger la vie privée permettront d'assurer que l'information acquise au titre de l'autorisation 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 informations électroniques ou aux infrastructures de l'information des institutions fédérales (alinéa 34(3)d))

62. Étant donné que les systèmes fédéraux sont situés au Canada, le CST va certainement acquérir incidemment de l'IRC, y compris de l'information qui portera atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens et des personnes se trouvant au Canada. L'article 24 de la *Loi sur le CST* exige que le CST mette en place des mesures 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 du volet de son mandat touchant la cybersécurité. Au paragraphe 41 de l'autorisation, le ministre conclut qu'il a des motifs raisonnables de croire que les mesures requises à l'article 24 feront en sorte que l'IRC est utilisée, analysée ou conservée uniquement si elle est essentielle.

63. Comme l'a expliqué le ministre, l'EPM établit des politiques complexes visant à contrôler et à protéger l'IRC qui est acquise au titre d'une autorisation de cybersécurité. Avant de traiter ce type d'information, les employés du CST doivent suivre une formation couvrant les exigences légales et politiques applicables. Un accès approprié à l'information non évaluée est également accordé à un nombre limité de membres du personnel occupant des rôles de gouvernance et de reddition de comptes. L'IRC est également fournie uniquement aux employés du CST selon le principe du besoin de savoir dans le cadre de leur travail. L'IRC acquise au titre de l'autorisation doit être jugée « essentielle » avant d'être utilisée, analysée ou conservée, et la justification de la conservation doit être consignée. Le processus pour déterminer si l'information est essentielle peut être manuel ou automatisé.

64. L'EPM énonce également les mesures de protection de la vie privée qui sont en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada lorsque de l'information qui les concerne est communiquée à d'autres ministères ou à des partenaires. Par exemple, les renseignements personnels peuvent être supprimés afin d'éviter de dévoiler l'identité d'une personne. En outre, l'IRC ne peut être communiquée que si le destinataire ou la catégorie de destinataires a été désigné par arrêté ministériel (art 45, *Loi sur le CST*) et si le CST conclut que la communication est nécessaire pour protéger les institutions fédérales et les systèmes désignés comme étant d'importance (art 44, *Loi sur le CST*).

65. À mon avis, lorsqu'elles sont suivies, ces mesures permettent au CST de respecter efficacement ses obligations prévues par la loi et les politiques de protéger la vie privée des Canadiens et des personnes se trouvant au Canada et de veiller à ce que l'information qui se rapporte à eux soit utilisée uniquement lorsqu'il est essentiel de le faire. Par conséquent, je suis convaincu du caractère raisonnable de la conclusion du ministre selon laquelle il a des motifs raisonnables de croire que l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada ne sera utilisée, analysée ou conservée que si elle est essentielle pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes des institutions fédérales.

V. REMARQUES

66. J'aimerais faire les remarques suivantes pour faciliter l'examen et la rédaction des prochaines autorisations ministérielles. Elles visent à clarifier une remarque antérieure et ne changent rien à mes constatations actuelles ou antérieures concernant le caractère raisonnable des conclusions du ministre.

A. Clarification de la remarque formulée dans la décision CST-2024-02

67. Le CST a inclus dans le dossier [...] une remarque que j'ai formulée dans la décision de l'année dernière et que j'aimerais clarifier.

68. La remarque reconnaissait et résumait la justification du CST présentée en réponse à une remarque antérieure que j'ai formulée dans la décision CST-2023-01. Cette remarque antérieure a soulevé la question selon laquelle le CST ne cherchait plus à obtenir une autorisation ministérielle pour une activité donnée que le commissaire au renseignement précédent n'avait pas approuvée, mais que le CST menait quand même, apparemment. À mon avis, certains éléments de la justification du CST auraient pu être interprétés comme laissant croire que si le CST a déterminé qu'une activité n'impliquait pas l'acquisition par lui d'information provenant de l'infrastructure mondiale de l'information (IMI), il pourrait aller de l'avant non seulement sans autorisation ministérielle, mais aussi sans avoir à déterminer si l'acquisition de cette information porterait atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens ou des personnes se trouvant au Canada. J'ai donc souligné que lorsque le CST détermine que les activités ne nécessitent pas une autorisation ministérielle parce qu'elles ne comprennent pas l'acquisition par le CST d'information provenant de l'IMI et qu'elles ne sont donc pas assujetties à l'examen du commissaire au renseignement, le CST doit tout de même examiner si ces activités mèneront à l'acquisition d'informations qui porteraient atteinte à l'attente raisonnable de protection en matière de vie privée.

69. En expliquant ma remarque, au paragraphe 81 de la décision de l'année dernière (CST-2024-02), j'ai affirmé que « l'information accessible au public acquise pour l'application de l'article 17 de la *Loi sur le CST* ne peut contenir d'information liée au Canada acquise

incidemment. En effet, conformément au paragraphe 23(4), le pouvoir d'acquérir incidemment de l'information liée au Canada est limité aux activités menées au titre d'une autorisation » (soulignement ajouté). […], je reconnais que ce passage n'aurait pas dû mentionner l'« information liée au Canada », mais plutôt plus indiquer l'« information à laquelle les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée » (soulignement ajouté). Il est admis que la première catégorie d'information est plus large que la seconde. La seconde reflète ce que j'ai voulu communiquer. Par conséquent, le renvoi au paragraphe 23(4) aurait dû être un renvoi au paragraphe 22(4).

70. Je remercie le CST et le ministre d'avoir inclus […], mettant en lumière la nécessité d'apporter une clarification. Étant donné que des remarques sont formulées pour améliorer le contenu des prochaines autorisations ou pour mettre en évidence une question que le CST doit examiner, la clarification n'a pas d'incidence sur mon évaluation du caractère raisonnable des conclusions du ministre examinées dans cette décision.

71. L'idée principale de ma remarque ne change pas non plus : lorsqu'une activité n'exige pas une autorisation ministérielle, la question de savoir si elle mènera à l'acquisition d'informations qui portent atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens ou des personnes se trouvant au Canada doit néanmoins demeurer au cœur de la décision du CST de mener ou non l'activité. En effet, cette analyse est nécessaire pour déterminer si les droits prévus à l'article 8 de la *Charte*, qui offre des protections contre les fouilles, les perquisitions et les saisies abusives, pourraient être violés. […], il y a une reconnaissance explicite selon laquelle des mesures appropriées doivent être mises en place pour empêcher que l'information acquise incidemment porte atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens au moment de mener des activités hors du cadre d'une autorisation ministérielle.

72. […] donne également des exemples de certaines activités et de mesures correspondantes pour empêcher l'acquisition incidente d'information. Sans vouloir laisser entendre, en aucune manière, que telle était intention du CST, je tiens à préciser que le fait que de tels exemples sont présents au dossier qui m'a été présenté ne signifie pas qu'ils ont un sceau d'approbation

du commissaire au renseignement. Je termine en réitérant un commentaire que j'ai formulé dans la remarque de l'année dernière, c'est-à-dire que dans les situations où la nécessité d'une autorisation est incertaine, il est raisonnable de faire preuve de prudence.

VI. CONCLUSIONS

73. D'après mon examen du dossier, 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 et des catégories d'activités énumérées au paragraphe 50 de l'autorisation sont raisonnables.

74. J'approuve donc, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, l'autorisation de cybersécurité pour des activités visant à protéger des infrastructures fédérales, délivrée par le ministre le 23 février 2025.

75. 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.

76. 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 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 16 avril 2025

(Original signé)

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