~~TRÈS SECRET//SI//RAC~~

Dossier : 2200-B-2024-07

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 SUR 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 15 novembre 2024

Canada

TABLE DES MATIÈRES

I. APERÇU

1. Il s'agit d'une décision qui examine 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 des entités non fédérales.

2. Le 22 octobre 2024, en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des communications*, LC 2019, c 13, art 76 (*Loi sur le CST*), le ministre a délivré une autorisation de cybersécurité concernant des activités menées dans des infrastructures non fédérales relativement aux gouvernements des Territoires du Nord-Ouest (GTNO), du Yukon (GY) et du Nunavut (GNT) (autorisation). Il s'agit de la deuxième année où le ministre délivre une autorisation de cybersécurité concernant ces trois entités non fédérales, que j'ai approuvée dans la décision 2200-B-2023-06, et la troisième année qu'une autorisation de cybersécurité est accordée à l'égard du GTNO (décision 2200-B-2022-06).

3. Le 23 octobre 2024, le Bureau du commissaire au renseignement a reçu l'autorisation pour que je procède à l'examen et à l'approbation selon la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*).

4. Pour les motifs qui suivent, 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 79 de l'autorisation sont raisonnables.

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

II. CONTEXTE

6. Dans le cadre de son mandat à titre d'organisme national du renseignement électromagnétique (art 15(1), *Loi sur le CST*), le CST exerce des activités de cyberprotection pour protéger les systèmes, les dispositifs et les réseaux électroniques ainsi que l'information qu'ils contiennent contre les cybermenaces que posent des criminels et des acteurs parrainés par l'État. 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*). Les systèmes peuvent appartenir à une institution fédérale — des systèmes fédéraux (para 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 appert de l'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada* pris le 25 août 2020.

7. Afin de mener ses activités de cyberprotection à l'égard des systèmes fédéraux et non fédéraux de manière efficace, le CST peut devoir contrevenir à certaines lois canadiennes. De même, le CST peut incidemment acquérir des communications et de l'information qui nuisent à l'attente raisonnable de protection en matière de vie privée de Canadiens ou de personnes se trouvant au Canada. La *Loi sur le CST* oblige le CST à obtenir une autorisation ministérielle avant de mener des activités de cybersécurité qui peuvent dépasser les limites de la loi et qui empiètent sur les intérêts des Canadiens en matière de protection de la vie privée.

8. 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 ses informations électroniques (art 33(3), *Loi sur le CST*).

9. La chef du CST doit ensuite présenter au ministre une demande écrite énonçant les faits qui lui permettraient de conclure qu'il existe des motifs raisonnables de croire que l'autorisation est nécessaire (art 33(2), *Loi sur le CST*). En outre, le ministre doit conclure que les conditions prévues aux paragraphes 34(1) et (3) de la *Loi sur le CST* ont été remplies. Le ministre énonce ses conclusions dans l'autorisation, qui est soumise à l'examen du commissaire au renseignement. Celui-ci approuve les activités ou les catégories d'activités précisées dans l'autorisation ministérielle s'il est convaincu que les conclusions du ministre sont raisonnables.

10. L'autorisation ministérielle n'est valide que lorsqu'elle est approuvée par le commissaire au renseignement (art 28, *Loi sur le CST*). Ce n'est qu'à ce moment-là que le CST peut exercer les activités énoncées dans l'autorisation, soit des activités qui constitueraient par ailleurs des

infractions et qui porteraient atteinte aux intérêts en matière de vie privée des Canadiens ou des personnes se trouvant au Canada.

11. Conformément au paragraphe 27(2) de la *Loi sur le CST*, le ministre peut autoriser le CST à acquérir de l'information qui provient d'un système non fédéral, passe par ce système, y est destinée ou y est stockée afin d'aider à protéger, dans les cas visés à l'alinéa 184(2)e) du *Code criminel*, LRC 1985, c C-46, ce système contre tout méfait, toute utilisation non autorisée ou toute perturbation de son fonctionnement. L'alinéa 184(2)e) s'applique généralement aux personnes qui gèrent la qualité du service d'un système informatique ou sa protection.

12. Malgré toute autorisation de cybersécurité, la *Loi sur le CST* impose des limites aux activités du CST. Ce dernier doit s'abstenir de mener quelque activité que ce soit visant un Canadien ou une personne se trouvant au Canada ou de contrevenir à la *Charte canadienne des droits et libertés* (*Charte*) (art 22(1), *Loi sur le CST*). Toutefois, lorsqu'il mène des activités au titre d'une autorisation, le CST est autorisé à acquérir incidemment de l'information concernant un Canadien ou une personne se trouvant au Canada (art 23(4), *Loi sur le CST*). Le mot « incidemment » signifie que l'information acquise n'a pas été délibérément recherchée (art 23(5), *Loi sur le CST*).

13. Lorsque le CST acquiert des renseignements personnels concernant des Canadiens ou des personnes se trouvant au Canada, il doit suivre des mesures législatives et politiques strictes pour utiliser, analyser et conserver ces renseignements. En effet, le CST est tenu de mettre en place des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada dans l'utilisation, l'analyse, la conservation et la divulgation de l'information qui se rapporte à eux (art 24, *Loi sur le CST*).

14. 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 comprend donc ce qui suit :

    a) La lettre du ministre adressée au commissaire au renseignement;
    b) L'autorisation;

c) La note d'information de la chef adressée au ministre;

d) La demande de la chef, qui comprend les 15 annexes suivantes :

i. Lettres de demande des trois entités non fédérales;

ii. Deux arrêtés ministériels;

iii. Tableau de conservation et suppression;

iv. Rapport sur les résultats des activités de 2023;

v. Ensemble des politiques sur la mission en matière de cybersécurité (EPM), approuvé le 28 février 2022;

e) Le document d'information – aperçu des activités.

III. NORME DE CONTRÔLE

15. Selon l'article 12 de la *Loi sur le CR*, le commissaire au renseignement procède à un examen quasi judiciaire des conclusions sur lesquelles une autorisation ministérielle est accordée afin de déterminer si ces conclusions sont raisonnables.

16. La jurisprudence du commissaire au renseignement établit que la norme de la décision raisonnable, qui s'applique aux contrôles judiciaires des mesures administratives, est la même qui s'applique à mon examen.

17. Comme l'indique la Cour suprême du Canada, 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 (*Mason c Canada (Citoyenneté et Immigration*), 2023 CSC 21 au para 79). Au paragraphe 99 de l'arrêt *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65, la Cour 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.

18. Les contraintes factuelles et juridiques pertinentes peuvent inclure le régime législatif applicable, l'incidence de la décision et les principes d'interprétation des lois. En effet, pour comprendre ce qui est raisonnable, il est nécessaire de tenir compte du contexte dans lequel la décision faisant l'objet du contrôle a été prise, tout comme de celui dans lequel elle est contrôlée. Il est donc nécessaire de comprendre le rôle du commissaire au renseignement, qui est un élément essentiel du régime législatif instauré par la *Loi sur le CR* et la *Loi sur le CST*.

19. Un examen de la *Loi sur le CR* et de la *Loi sur le CST*, ainsi que des débats législatifs, montre que le législateur a créé le rôle du commissaire au renseignement afin qu'il serve de mécanisme indépendant permettant d'assurer un juste équilibre entre les mesures prises par le gouvernement à des fin de sécurité nationale, et le respect de la primauté du droit ainsi que des droits et libertés des Canadiens. J'estime que le législateur m'a attribué un rôle de gardien afin de maintenir cet équilibre. Dans mon examen des conclusions du ministre, je dois soigneusement déterminer si les intérêts importants des Canadiens et des personnes se trouvant au Canada, notamment en matière de vie privée, ont été dûment pris en compte et pondérés, et je dois m'assurer que la primauté du droit est pleinement respectée.

20. 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, lorsque ces conclusions sont déraisonnables, il « n'approuve pas » l'autorisation (art 20(1)b), *Loi sur le CR*).

IV. ANALYSE

21. La chef a adressé au ministre une demande écrite pour une autorisation concernant des activités de cybersécurité menées dans des infrastructures non fédérales (demande) afin d'obtenir l'autorisation de mener des activités pour aider à protéger les systèmes de trois entités non fédérales d'importance pour le gouvernement fédéral. La demande constitue une demande de renouvellement de l'autorisation ministérielle que j'ai approuvée dans la décision 2200-B-2023-06. L'autorisation ne contient pas de nouvelles activités par rapport à l'autorisation accordée l'année dernière.

22. Conformément à des autorisations ministérielles antérieures, des capteurs, soit des logiciels dont l'objet consiste à détecter les cyberactivités malveillantes, ont été déployés sur les systèmes appartenant au GTNO […], et sur les systèmes appartenant au GY […] et au GNT […]. Les capteurs permettent au CST d'acquérir en toute sécurité de l'information des systèmes pour découvrir des cyberactivités malveillantes. Plus précisément, les capteurs comportent […]. La demande énonce les raisons pour lesquelles le CST souhaite mener ces activités de cybersécurité dans les systèmes qui appartiennent aux trois gouvernements territoriaux.

23. Une description du contexte factuel qui a mené aux autorisations antérieures ainsi que d'autres renseignements sur les activités dont il est question dans l'autorisation se trouvent dans l'annexe classifiée de la présente décision (annexe A). J'ai décidé de placer ces informations dans une annexe pour deux raisons. Premièrement, cela empêchera qu'une partie importante du texte de la présente décision soit caviardé, ce qui facilitera la lecture de sa version publique. Deuxièmement, cela permettra de s'assurer que la nature des faits dont j'ai été saisi, qui autrement ne seraient accessibles que dans le dossier, est incluse dans la décision.

24. Les annexes XIII, XIV et XV du dossier énumèrent les ministères et les organismes des gouvernements territoriaux qui utilisent les systèmes des entités non fédérales et qui seraient donc admissibles à recevoir les services de cybersécurité du CST au titre de l'autorisation.

25. Compte tenu des faits exposés dans la demande que la chef a présentée le 7 octobre 2024, le ministre a conclu qu'il avait des motifs raisonnables de croire que l'autorisation était nécessaire et que les conditions énoncées aux paragraphes 34(1) et (3) de la *Loi sur le CST* étaient remplies. Conformément à l'article 14 de la *Loi sur le CR*, je dois me pencher sur la question de savoir si les conclusions du ministre sur le fondement desquelles l'autorisation a été accordée sont raisonnables.

A. Paragraphe 34(1) de la *Loi sur le CST* — Déterminer si les activités sont raisonnables et proportionnelles

i. Signification du caractère raisonnable et proportionnel

26. 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 » (para 34(1), *Loi sur le CST*).

27. Le ministre doit appliquer sa compréhension de ces seuils (caractère raisonnable et proportionnel) pour en arriver à sa conclusion. La question de savoir si une activité est raisonnable et proportionnelle dépend du contexte et le ministre peut tenir compte d'un certain nombre de facteurs. Le commissaire au renseignement doit établir si les conclusions du ministre, qui comprennent sa compréhension des seuils, sont « raisonnables » en procédant à un examen selon la norme de décision raisonnable, expliquée précédemment.

ii. Examen de la conclusion du ministre selon laquelle les activités en cause sont raisonnables

28. Le ministre a conclu au paragraphe 49 de l'autorisation qu'il avait des motifs raisonnables de croire que les activités autorisées dans l'autorisation sont raisonnables compte tenu de l'objectif d'aider à protéger les systèmes des entités non fédérales ainsi que de potentiellement protéger les systèmes fédéraux et d'autres systèmes d'importance contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

29. Il appert du dossier que le CST, pour mener ses activités de cybersécurité, « doit » acquérir […]. Étant donné que les systèmes se trouvent au Canada, au moins une partie de l'information se rapportera à des Canadiens ou à des personnes se trouvant au Canada. Je suis toutefois convaincu que le but des activités de cybersécurité dont il est question dans l'autorisation est de découvrir des cybermenaces et d'y donner suite; elles ne visent pas des Canadiens ou des personnes se trouvant au Canada. Ces activités sont conformes aux dispositions législatives qui interdisent d'acquérir délibérément de l'information qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada et de mener des activités

visant des Canadiens ou des personnes se trouvant au Canada (para 22(1) et 23(3), *Loi sur le CST*).

30. Tout comme dans la décision rendue l'année dernière concernant ces entités non fédérales, le ministre fournit deux raisons principales pour justifier le caractère raisonnable des activités de cybersécurité : 1) les activités visées par l'autorisation demandée sont efficaces; et 2) la participation du CST à l'intervention en matière de cybersécurité est nécessaire compte tenu du rôle clé joué par les entités non fédérales dans la gouvernance de l'Arctique, une région stratégique pour le Canada.

31. D'abord, les activités énoncées dans l'autorisation sont efficaces et complètent les autres activités de cybersécurité des entités non fédérales. Le ministre explique que la sophistication des cybermenaces les rend difficiles à découvrir. Les solutions de cybersécurité du CST ajoutent une couche supplémentaire de défense pour détecter des compromissions possibles qui pourraient avoir des conséquences dévastatrices comme la perte d'information ou de la fonctionnalité du système.

32. Le dossier contient de l'information sur l'efficacité des activités. Le ministre explique notamment que pendant la durée des autorisations antérieures, le CST a utilisé de l'information recueillie par les capteurs déployés sur les systèmes du GTNO pour préparer des rapports d'activités malveillantes ou de vulnérabilités et les remettre au GTNO […]. Dans la décision 2200-B-2024-06, j'ai indiqué que la simple existence de rapports partagés avec l'entité non fédérale relativement à une « vulnérabilité » ne constitue pas nécessairement un élément de preuve qui étaye le caractère raisonnable de la présence continue du CST sur le système non fédéral. L'existence d'un rapport ne témoigne pas des répercussions de la vulnérabilité sur le système. Je suis convaincu en l'espèce que le dossier contient assez de détails sur l'information dans le rapport qui, lui, étaye la conclusion du ministre selon laquelle les activités du CST sont efficaces. Même s'il ressort du dossier que les trois territoires ont été la cible d'activités malveillantes par le passé, […].

33. De plus, il ressort du dossier que le GTNO a instauré des mesures fondées sur les conseils et l'orientation du CST. Je souligne que le dossier de l'année dernière fait état de quatre

recommandations que le GTNO est en train de mettre en œuvre. Il n'y a aucune mise à jour quant à l'application de ces recommandations. En outre, il ressort du dossier que le GTNO est en train de mettre en application une recommandation émise par le CST, mais qui ne fait pas partie des quatre recommandations formulées l'année dernière. Lorsqu'une autorisation est sollicitée à l'égard des mêmes activités que celles qui étaient visées au cours d'une année antérieure, je m'attendrais à ce que le dossier permette au ministre de constater les progrès réalisés, le cas échéant.

34. Je conviens, selon l'information au dossier, que les activités du CST ont été, et continuent d'être, efficaces, et elles ont renforcé la posture de cybersécurité de chaque gouvernement territorial.

35. Le deuxième motif à l'appui de la conclusion que les activités du CST sont raisonnables est que les entités non fédérales en cause offrent, avec des ressources limitées, des services publics essentiels aux Canadiens. Comme le ministre l'a expliqué, elles conservent des renseignements personnels de nature délicate et jouent un rôle central dans la gouvernance de l'Arctique canadien, qui revêt un intérêt géopolitique primordial pour les adversaires.

36. Le ministre étaye davantage ses conclusions en invoquant le rôle de prestation de services des entités non fédérales ainsi que l'importance géopolitique de la région où se trouvent ces entités. Compte tenu de l'accès accru à l'Internet, la région arctique du Canada est assujettie à plus d'activités de cybermenaces et elle doit être protégée.

37. Le ministre explique que l'état actuel des trois entités non fédérales en matière de cybersécurité ne suffit pas pour découvrir et combattre [...]. Étant donné l'importance de l'Arctique, le soutien du CST s'impose.

38. Bien que le dossier n'indique pas explicitement que les solutions de cybersécurité du CST se veulent permanentes, rien ne donne à penser que le soutien du CST finira par ne plus être nécessaire. Cela semble conforme au rapport annuel du CST 2023–2024, qui précise que le CST entend, afin de sécuriser le Nord, déployer ses solutions de cybersécurité pour exercer une « surveillance permanente ».

39. Comme je l'ai souligné dans la décision 2200-B-2024-06, la *Loi sur le CST* ne limite pas expressément la période pendant laquelle le CST peut aider une entité non fédérale, à condition qu'il obtienne une autorisation ministérielle chaque année. Dans cette décision, j'ai accepté le raisonnement du ministre selon lequel la présence du CST s'imposait encore parce que certaines de ses recommandations essentielles pour assurer une posture de cybersécurité solide n'avaient pas encore été mises en œuvre. Dans la présente autorisation, le raisonnement ne s'appuie pas sur des recommandations en suspens du CST ou sur le rétablissement et le renforcement du système à la suite d'un cyberincident. Même si les trois entités non fédérales ont fait face à des cyberactivités malveillantes par le passé, le ministre n'invoque pas présentement de telles activités pour justifier ses conclusions.

40. Ces conclusions reposent plutôt en grande partie sur l'importance stratégique de l'Arctique. À titre d'exemple, il ressort du dossier que le déploiement continu de solutions de cybersécurité du CST « favorisera la résilience à long terme aux acteurs de cybermenaces et conféra d'importants avantages stratégiques au Canada et à ses alliés. » En ce sens, l'autorisation est de nature préventive ou proactive plutôt que réactive. J'aborde une question précise à cet égard dans mes remarques.

41. J'accepte le raisonnement du ministre selon lequel le maintien de la présence du CST est nécessaire pour veiller à ce que les systèmes des gouvernements territoriaux soient bien protégés contre des cybermenaces. Ma conclusion tient compte de l'efficacité des capteurs du CST, de la situation actuelle de chaque gouvernement territorial en matière de cybersécurité ainsi que de l'information au dossier quant à l'importance de l'Arctique à l'intérêt national du Canada. Par conséquent, j'estime que les conclusions du ministre quant au caractère raisonnable des activités énoncées dans l'autorisation sont raisonnables.

iii. Examen de la conclusion du ministre selon laquelle les activités en cause sont proportionnelles

42. Le ministre a conclu, au paragraphe 52 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités en cause sont « proportionnelles compte tenu de la manière dont elles sont menées ».

43. Je suis convaincu que les conclusions du ministre à cet égard sont raisonnables. Il reconnaît que les activités de cybersécurité proposées peuvent mener à l'acquisition de grands volumes d'information pour découvrir des cybermenaces. Bien que certaines informations puissent empiéter sur les intérêts en matière de vie privée, le ministre affirme que le CST s'intéresse aux comportements anormaux concernant l'information plutôt qu'à son contenu.

44. Le ministre présente des mesures et des contrôles pour démontrer que les activités sont proportionnelles. Le ministre énonce sept mesures et contrôles internes qui ont été appliqués par le CST :

a) aucune information non évaluée n'est conservée plus longtemps que […] à compter de la date à laquelle elle a été acquise;
b) le CST conserve moins de 1 % de toutes les données qui ont initialement été acquises dans le cadre d'activités de cybersécurité;
c) l'analyse et l'atténuation sont principalement effectuées par des processus automatisés qui limitent l'exposition des employés à l'information non évaluée et toute l'information est protégée conformément à la politique d'exploitation du CST;
d) chaque recherche effectuée sur l'information non évaluée acquise est vérifiable conformément à l'EMP;
e) l'accès à l'information acquise au titre de la présente autorisation est limité aux employés qui ont besoin d'en avoir connaissance dans le cadre de leur travail. Avant d'accéder à de l'information non évaluée, les employés doivent réussir un examen annuel noté portant sur les exigences établies par les lois et les politiques qui s'appliquent au traitement de ce type d'information;

f) tous les outils de cybersécurité sont passés en revue pour veiller à ce qu'ils soient conformes aux lois et aux politiques;
g) les mêmes conditions s'appliquent à l'information utilisée par le CST pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux et à d'autres systèmes d'importance.

45. Le ministre s'appuie principalement sur les mesures qui ont été appliquées à l'information après son acquisition pour étayer sa conclusion sur la proportionnalité. Le ministre confirme que le CST dégage une vaste gamme d'information de ses activités de cybersécurité en vue de mieux protéger les systèmes fédéraux et non fédéraux. Cela comprend notamment l'accès à une grande quantité d'information comme […] pour laquelle les Canadiens et les personnes se trouvant au Canada peuvent avoir une attente raisonnable en matière de protection de la vie privée.

46. Je conviens que le ministre ne bénéficiait pas des commentaires que j'ai formulés dans la décision 2200-B-2024-06. Par conséquent, je réitère que le dossier n'indique pas la quantité globale d'information acquise dans le passé. Bien que 1 % puisse sembler minime, le CST a un vaste accès au système non fédéral. Le ministre et le commissaire au renseignement bénéficieraient de renseignements supplémentaires relativement au volume total de données recueillies pour mieux déterminer la proportionnalité des activités menées par le CST et la façon dont elles portent une atteinte minimale aux droits en matière de vie privée des Canadiens et des personnes se trouvant au Canada.

47. Le rapport sur les résultats indique que le CST a conservé, pendant la durée de l'autorisation précédente, 384 « articles » acquis à partir des systèmes des entités non fédérales, ce qui représente moins de 1 % du total des données acquises. J'estime que cette comptabilisation précise de l'information conservée constitue un progrès au titre de la responsabilité ministérielle et de la transparence. Comme je l'ai dit dans la décision 2200-B-2024-06, un contexte supplémentaire afin de comprendre ce qui constitue un « article » serait utile pour le ministre en moi.

48. En outre, le rapport sur les résultats comporte une description des mesures que le GTNO a menées à bien pendant la période de validité de l'autorisation 2023–2024 ainsi que de la recommandation du CST qui est mise en œuvre. Il ne contient toutefois pas de calendrier de mise en œuvre des recommandations en suspens. Le temps dont le CST a besoin pour atteindre cet objectif peut être un facteur à prendre en considération dans l'examen de la question de savoir si les activités sont proportionnelles. Je m'attends à ce qu'il en soit question dans le cadre de demandes futures.

49. Le ministre explique que l'accès à l'information qui est liée aux droits des Canadiens en matière de vie privée est limité aux employés désignés du CST qui sont formés pour traiter ce type d'information et l'utiliser selon le principe du « besoin de savoir » dans le cadre de leurs fonctions. Cela limite l'accès à l'information qui peut être liée aux droits des Canadiens en matière de vie privée.

50. Je peux suivre le raisonnement du ministre lorsqu'il s'est appuyé sur ces mesures. Il conclut que les activités proposées justifient toute atteinte possible aux intérêts des Canadiens en matière de vie privée. Il explique également comment les activités avaient pour objectif l'atteinte d'une mise en balance raisonnable entre elles. Je suis convaincu que les intérêts des Canadiens et des personnes se trouvant au Canada ont été pris en compte et que la mise en balance est raisonnable.

51. En ce qui concerne les lois canadiennes susceptibles d'être enfreintes, l'autorisation précise qu'elles sont limitées, car les activités ne seraient menées que dans les systèmes à l'égard desquels le CST a reçu le consentement exprès du propriétaire. Comme le CST a obtenu ce consentement, le risque d'éventuelles infractions aux lois canadiennes est faible. Si une loi fédérale est enfreinte, les répercussions seront limitées et si une loi fédérale qui ne figure pas dans la demande de la chef en enfreinte, la chef en informera le ministre et le commissaire au renseignement.

52. 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.

B. Paragraphe 34(3) de la *Loi sur le CST* — Les conditions nécessaires à la délivrance d'une autorisation

53. 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 :

    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 de s'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à des Canadiens ou à des personnes 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 (art 34(3)a))

54. L'information est conservée conformément aux exigences définies dans les politiques du CST et elle est régie par un calendrier de conservation visant les différentes catégories d'information recueillie. Le ministre explique que les exigences du CST concernant la gestion de l'information et la disposition de dossiers énoncées dans les politiques du CST sont conformes à la *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21 et à la *Loi sur la Bibliothèque et les Archives du Canada*, LC 2004, c 11. Comme la chef l'a signalé, les entités non fédérales en cause peuvent, en tout temps, demander au CST de supprimer l'information qu'il a acquise à partir ou par l'intermédiaire de ses systèmes.

55. Le CST n'est pas en mesure de déterminer, avant la collecte, quelle information serait utile pour repérer des activités malveillantes. Il acquiert donc un grand volume d'information. Le CST traite cette information, principalement au moyen de méthodes automatisées qui limitent

son exposition à l'information contenue dans un dossier. L'utilisation de méthodes automatisées permet de s'assurer que les employés n'interagissent qu'avec l'information nécessaire pour élaborer des mesures de détection et d'atténuation, ou pour déterminer les processus de conservation et de traitement. Ce processus permet de déterminer que certaines informations sont « nécessaires » ou « essentielles ». Le reste de l'information est considérée comme étant de l'information non évaluée, même si elle a été assujettie au processus automatisé.

56. La période de conservation de l'information non évaluée est de [...], alors que l'information jugée « nécessaire » ou « essentielle » pour aider à protéger les systèmes non fédéraux, ou les systèmes fédéraux et les systèmes désignés comme étant d'importance, peut être conservée « indéfiniment ou jusqu'à ce qu'elle ne soit plus utile à ces fins ».

57. Le raisonnement du ministre quant à la période de conservation de l'information non évaluée est simple. Il précise qu'il y a souvent une période entre le moment où la compromission débute et celui où elle est découverte. Lorsqu'un indicateur de compromission est découvert, l'efficacité des activités du CST est tributaire de la capacité d'examiner l'information non évaluée pour découvrir toute compromission qui n'avait pas encore été découverte. Le CST estime qu'une période de conservation [...] de l'information non évaluée suffit pour lui permettre de remonter aux origines d'un événement ou d'examiner son évolution dans le temps. La comparaison entre une compromission et des données non évaluées ou des activités malveillantes non détectées aide le CST à élaborer de meilleures mesures d'atténuation et des moyens de défense qui peuvent être utilisés non seulement pour le système non fédéral, mais aussi pour les autres systèmes d'importance et les systèmes fédéraux.

58. Après la période [...], l'information non évaluée sera automatiquement supprimée, à moins qu'elle soit jugée « nécessaire » ou « essentielle » pour aider à protéger le système non fédéral ou les systèmes fédéraux et les systèmes désignés comme étant d'importance. En outre, l'information non évaluée ne peut pas être divulguée à l'extérieur du CST. Dans la demande, la chef confirme que les trois entités non fédérales ont connaissance de l'utilisation de cette information et l'acceptent.

59. Comme il est indiqué au dossier, le critère du caractère « nécessaire » s'applique à l'information qui ne se rapporte pas à un Canadien ou à une personne se trouvant au Canada; quant au critère du caractère « essentiel », il s'applique à l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada. L'information est jugée « nécessaire » lorsqu'elle est requise pour comprendre la cyberactivité malveillante, y compris […], dans le but d'aider à protéger les systèmes non fédéraux. Par sa nature, l'information jugée « nécessaire » ne contient pas d'éléments liés à des Canadiens ou à des personnes se trouvant au Canada et est donc moins sensible que l'information jugée « essentielle ». Le but est d'aider à réaliser des analyses de détection et de prévention et à renforcer l'écosystème de cyberdéfense.

60. L'information sur les Canadiens et les personnes se trouvant au Canada est considérée comme « essentielle » si, sans elle, le CST ne pourrait pas découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux. Cela peut inclure […]. L'information acquise peut être hautement sensible pour des Canadiens, et la plupart des analyses sont faites suivant des processus automatisés qui détectent les comportements anormaux et limitent l'exposition des employés au contenu des fichiers.

61. L'information qui a été jugée nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés au système non fédéral est conservée conformément à l'article 11.2 de l'EPM. Le personnel du programme de conformité interne du CST transmet des rappels trimestriels aux analystes de la cybersécurité afin de s'assurer que les données conservées dans un dépôt ministériel qui n'ont pas été jugées nécessaires ou essentielles soient supprimées dans les […] suivants leur acquisition. De plus, les gestionnaires opérationnels doivent vérifier sur une base trimestrielle si l'information demeure essentielle. L'information qui n'est plus essentielle doit être supprimée.

62. J'estime que le ministre explique de façon raisonnable le motif pour lequel il faut conserver l'information pendant la durée nécessaire — […] pour l'information non évaluée et jusqu'à ce qu'elle ne soit plus utile pour l'information qui est « nécessaire » ou « essentielle ». Ces

périodes de conservation permettent au CST de mener des activités de cybersécurité de manière efficace.

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

63. Les activités de cybersécurité du CST ne sont efficaces qu'avec l'acquisition d'information. Le ministre explique que les auteurs de menaces […] délibérément. Afin d'atténuer efficacement les cybermenaces sophistiquées décrites dans le présent cas et de prévenir les cybermenaces potentielles, le CST doit acquérir un large éventail d'information qui peut ensuite être évaluée pour repérer les activités malveillantes. L'information comprend […].

64. Rien dans le dossier ne donne à entendre que le CST peut atteindre les mêmes résultats de cybersécurité en employant des activités de cybersécurité différentes qui permettent d'acquérir moins d'information, tout particulièrement de l'information se rapportant à des Canadiens.

65. Les conclusions du ministre contiennent des exemples de la façon dont l'information acquise au titre de cette autorisation peut aussi être utilisée par le CST pour appuyer des activités au titre d'autres autorisations de cybersécurité et sous d'autres volets de son mandat. Toute autre utilisation, analyse, conservation ou divulgation de l'information acquise conformément à une autorisation de cybersécurité est assujettie aux restrictions et aux conditions imposées par des clients ou des entités qui divulguent l'information.

66. Pour ces motifs, je suis convaincu que les conclusions du ministre sont raisonnables et qu'il a des motifs raisonnables de croire que l'acquisition d'information est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux.

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 (art 34(3)d))

67. 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 d'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.

68. Le ministre énonce les exigences établies par les politiques du CST pour étayer sa conclusion selon laquelle toute information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui est acquise incidemment ne sera conservée que si elle est jugée essentielle pour découvrir, isoler ou prévenir des dommages aux systèmes des entités non fédérales.

69. Pour ce qui est de la conservation de l'information liée aux Canadiens, toute l'information acquise est traitée conformément à l'article 8 de l'EPM. Plus particulièrement, l'article 8.2.2 précise que le critère du « caractère essentiel » est appliqué par des employés formés et accrédités du CST, à l'aide de processus manuels ou automatisés. Les employés doivent consigner les raisons pour lesquelles ils estiment que l'information est essentielle. Cette façon de procéder limite l'accès au contenu de l'information qui est très sensible pour les Canadiens et l'exposition à l'information non évaluée. À mon avis, ces mesures contribuent au respect de l'obligation prévue à l'article 24 de la *Loi sur le CST* et soutiennent les conclusions du ministre.

70. 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). La liste du personnel ayant un accès approuvé à l'information non évaluée est surveillée aux fins de reddition de comptes.

71. Comme il est indiqué de l'article 24 de l'EPM, des mesures 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 divulguée. Par exemple, les renseignements personnels peuvent être supprimés afin d'éviter de dévoiler l'identité d'une personne. L'EPM prévoit les niveaux requis d'approbation de la divulgation qui s'appliquent si de l'information qui se rapporte à un Canadien est divulguée et il indique que ces niveaux doivent être répertoriés.

72. Les conclusions du ministre et le dossier contiennent des explications sur la façon dont l'information qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada peut être communiquée, ce qui reflète l'obligation prévue à l'article 44 de la *Loi sur le CST*. L'information n'est communiquée qu'aux personnes ou aux catégories de personnes désignées en vertu de l'*Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu de l'aspect de cybersécurité et de l'assurance de l'information du mandat du CST* pris le 13 juin 2023, conformément à 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. Afin de recevoir de l'information divulguée par le CST qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada, l'information doit être nécessaire pour aider à protéger des systèmes non fédéraux ou fédéraux.

73. Dans sa lettre de demande au CST, chaque entité non fédérale a demandé que toute l'information personnelle ou confidentielle qui peut être recueillie et conservée soit masquée avant la divulgation. De plus, toute l'information qui n'est pas pertinente pour le mandat du CST doit être supprimée en conformité avec le calendrier de conservation du CST. Je comprends donc que toute divulgation d'information acquise au titre de l'autorisation devra d'abord respecter cette directive.

74. L'EPM établit des politiques complexes pour contrôler et protéger l'information concernant des Canadiens et des personnes se trouvant au Canada 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'exigence législative de protéger suffisamment cette information.

75. En outre, le rapport préparé après l'expiration de l'autorisation qui est remis au ministre conformément à l'article 52 contient des renseignements sur la conservation, l'utilisation et la divulgation d'information liée aux Canadiens; une copie de ce rapport est transmise au commissaire au renseignement. La préparation de rapports ajoute un niveau supplémentaire de responsabilité. Les rapports se sont améliorés depuis l'approbation de l'autorisation de cybersécurité initiale concernant le GTNO en 2022 et ils comportent plus de détails sur le volume et la nature de l'information qui est conservée.

76. Compte tenu de ce qui précède, je suis convaincu que la conclusion du ministre est raisonnable et qu'il a des motifs raisonnables de croire que l'information qui se rapporte aux Canadiens ou aux personnes se trouvant au Canada ne sera utilisée, analysée ou conservée que si elle est essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes des entités non fédérales.

V. REMARQUES

77. J'aimerais faire les deux remarques suivantes, qui ne modifient pas mes conclusions concernant le caractère raisonnable des conclusions du ministre.

78. Je signale que le rapport préparé conformément à l'article 52 après l'expiration de l'autorisation relativement à l'autorisation ministérielle de 2022 a soulevé un incident de non-conformité dont il n'était pas question au dossier. L'incident avait trait à une demande soumise par le ministère de la Justice pour que le CST conserve, en raison d'un litige, de l'information qui avait été recueillie conformément à l'autorisation et qui aurait dû être supprimée dans un délai précis. Cet incident a été décrit dans la décision 2200-B-2024-06 où j'ai déclaré que même si la non-conformité ne remettait pas en cause la validité de l'autorisation en jeu, le ministre aurait dû disposer de toute l'information pertinente. La même remarque s'applique dans le contexte de la présente autorisation.

A. Renseignements supplémentaires pour le ministre sur l'utilisation légale de l'information par une entité non fédérale

79. Comme je l'ai souligné dans des décisions antérieures, la *Loi sur le CST* n'oblige pas expressément le ministre à se pencher sur la question de savoir si l'entité non fédérale dispose du pouvoir conféré par la loi de recueillir, d'utiliser et de conserver des renseignements personnels de Canadiens et de personnes au Canada à des fins de cybersécurité. Pour cette raison, j'ai déclaré dans la décision 2200-B-2024-06 que le ministre devrait être en mesure de comprendre facilement que l'entité non fédérale a la compétence initiale de recueillir l'information, et qu'il existe un fondement juridique pour sa communication au CST à des fins de cybersécurité.

80. Les entités non fédérales ne devraient autoriser le CST à exercer que les activités qu'elles-mêmes pourraient mener légalement. La préoccupation évidente est la situation hypothétique où le ministre accorde une autorisation pour permettre au CST de mener des activités de cybersécurité dans le cadre desquelles de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada est recueillie pour le compte de l'entité non fédérale lorsque cette entité ne dispose pas du pouvoir de recueillir ou d'utiliser cette information à des fins de cybersécurité. À mon avis, lorsque nous donnons cette assurance au ministre, nous renforçons le régime d'autorisation ministérielle.

81. Je conviens que le CST et le ministre ne bénéficiaient pas encore de la décision 2200-B-2024-06 lorsque l'autorisation a été accordée. Dans l'autorisation visée en l'espèce, le ministre explique qu'il incombe aux entités non fédérales d'offrir des programmes et des services essentiels aux résidents, entreprises et visiteurs ainsi qu'aux ministères et organismes du gouvernement et aux sociétés d'État. Pour exercer ces responsabilités, elles détiennent de l'information importante, notamment des renseignements personnels concernant des Canadiens et des personnes se trouvant au Canada. Je recommande, dans l'intérêt d'autorisations de cybersécurité futures, de présenter au dossier un lien plus clair entre le pouvoir légal des entités de recueillir l'information et de l'utiliser à des fins de cybersécurité pour le ministre. Cela peut viser des éléments liés au consentement d'utilisateurs des systèmes qui appartiennent aux entités non fédérales.

B. Caractère raisonnable d'activités dans un contexte de prévention

82. Comme je l'ai indiqué dans mes motifs, le maintien de la présence du CST est de nature préventive ou proactive. Je veux toutefois préciser que mes conclusions ne signifient pas qu'une désignation en tant qu'entité non fédérale d'importance pour le gouvernement fédéral soit, en soi, suffisante pour soutenir les conclusions du ministre selon lesquelles une autorisation de cybersécurité serait raisonnable si elle visait un objet préventif.

83. J'estime que les conclusions du ministre sont raisonnables. Pour en arriver à cette décision, je me suis appuyé sur son raisonnement concernant l'importance stratégique de l'Arctique pour le gouvernement fédéral ainsi que sur la preuve faisant état d'activités malveillantes. Le dossier contient des documents qui étayent et expliquent en long et en large l'importance stratégique de l'Arctique ainsi que la nature des activités malveillantes.

84. Une autorisation de cybersécurité au titre du paragraphe 27(2) de la *Loi sur le CST* est délivrée afin d'aider à protéger le système d'une entité non fédérale contre tout méfait, toute utilisation non autorisée ou toute perturbation de son fonctionnement. Lorsque des activités de cybersécurité sont menées à des fins préventives ou proactives, j'estime que le ministre doit néanmoins démontrer qu'il existe un fondement factuel pour demander l'aide du CST.

VI. CONCLUSIONS

85. D'après mon examen du dossier, je suis convaincu que les conclusions que le ministre a tirées au titre des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités énumérées au paragraphe 79 de l'autorisation sont raisonnables.

86. J'approuve donc, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, l'autorisation de cybersécurité pour des activités sur des infrastructures non fédérales, délivrée par le ministre le 22 octobre 2024.

87. 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.

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

Le 15 novembre 2024

(Original signé)

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