Office of the Intelligence Commissioner
Bureau du commissaire au renseignement

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

~~TRÈS SECRET//SI//RAC~~

Dossier : 2200-B-2023-06

[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 30 novembre 2023

TABLE DES MATIÈRES

I. APERÇU

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

2. Le CST est l'organisme national du Canada en matière de cryptologie, et assure la cyberdéfense du gouvernement du Canada. Le CST a pour mandat d'assurer la sécurité des technologies de l'information du gouvernement contre les cybermenaces. Le mandat du CST s'étend à aider à la protection de l'information électronique et de l'infrastructure des entités qui ne font pas partie du gouvernement du Canada lorsque les infrastructures non fédérales importantes pour le gouvernement ont été désignées comme telles.

3. Afin de mener ses activités de cybersécurité de manière efficace, le CST peut devoir contrevenir à certaines lois canadiennes. Par ailleurs, lorsqu'il obtient de l'information sur la cybersécurité liée à des activités malveillantes, le CST peut incidemment acquérir de l'information qui nuit à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

4. Dans les situations où le CST souhaite mener des activités de cybersécurité qui dépassent les limites de la loi et qui empiètent sur les intérêts des Canadiens en matière de protection de la vie privée, il doit d'abord obtenir les autorisations requises. Le législateur a créé un régime de mise en balance pour s'assurer que la nécessité de protéger les informations électroniques et les infrastructures d'importance ne l'emporte pas sur le respect des intérêts des Canadiens en matière de protection de la vie privée et la primauté du droit.

5. Le régime découle d'une demande écrite de la chef du CST (la chef) au ministre pour obtenir une autorisation de cybersécurité qui énonce les activités que le CST serait autorisé à mener. Le ministre peut délivrer l'autorisation de cybersécurité si, entre autres conditions,

il conclut que les activités proposées sont raisonnables et proportionnelles. Une autorisation de cybersécurité ne devient valide qu'après que le commissaire au renseignement l'a ensuite approuvée.

6. Le [redacted], en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*), le ministre a délivré une autorisation de cybersécurité relativement à des activités visant des infrastructures non fédérales (l'autorisation) pour [redacted]; l'autorisation est [redacted]

7. Le [redacted], le Bureau du commissaire au renseignement a reçu l'autorisation à des fins d'examen et d'approbation, au titre de la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*).

8. Pour les motifs ci-après, je suis convaincu que les conclusions que le ministre a tirées en application des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités et aux catégories d'activités énumérées au paragraphe 70 de l'autorisation sont raisonnables.

9. Par conséquent, conformément à l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation ministérielle visant des activités de cybersécurité visant des infrastructures non fédérales.

II. CONTEXTE LÉGISLATIF

A. *Loi sur le Centre de la sécurité des télécommunications*

10. En juin 2019, la *Loi concernant des questions de sécurité nationale (*appelée *Loi de 2017 sur la sécurité nationale*, LC 2019, c 13) est entrée en vigueur et a créé le poste de commissaire au renseignement. Les pouvoirs et les devoirs du CST ont également été élargis par la création de la *Loi sur le CST*, laquelle est entrée en vigueur en août 2019.

11. Le mandat du CST comprend la cybersécurité et l'assurance de l'information. Le libellé de l'article 17 de la *Loi sur le CST* dispose que le CST peut fournir des conseils, de l'orientation et des services pour aider à protéger l'information électronique et les infrastructures appartenant aux institutions fédérales ainsi qu'aux entités qui ne font pas partie du gouvernement fédéral, mais sont d'importance pour le gouvernement du Canada et désignées comme telles par le ministre en vertu du paragraphe 21(1) de la *Loi sur le CST* (les systèmes qui ne relèvent pas du gouvernement fédéral), par exemple dans les secteurs de la santé, de l'énergie et des télécommunications.

12. Les entités non fédérales peuvent compter sur un certain nombre de services pour protéger leurs systèmes contre divers acteurs de cybermenaces sophistiqués, comme des moyens de protection offerts sur le marché (antivirus, logiciels pare-feu, etc.) et des entreprises tierces offrant des services de sécurité en matière de technologies de l'information. Néanmoins, le législateur estime que l'expertise du CST pourrait s'avérer nécessaire pour protéger les entités qui exercent leurs activités dans des secteurs d'importance pour le gouvernement du Canada. Au cours des dernières années, cette expertise est devenue très importante pour réagir aux cybermenaces complexes provenant de groupes parrainés par des États et d'acteurs non étatiques.

13. Pour comprendre les points d'entrée vulnérables et les atteintes à l'intégrité des systèmes non fédéraux, le CST doit accéder aux systèmes et acquérir de l'information. Ces activités, menées dans le but de protéger les systèmes, pourraient néanmoins contrevenir à certaines lois et porter atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens et des personnes se trouvant au Canada. La *Loi sur le CST* exige une autorisation ministérielle, approuvée par la suite par le commissaire au renseignement, chaque fois que les activités de cybersécurité du CST contreviennent à une loi fédérale ou entraînent l'acquisition d'information qui nuit à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada (paragraphes 22(4) et 27(2) de la *Loi sur le CST*). La *Loi sur le CST* établit le processus que doit suivre le CST pour obtenir une autorisation de cybersécurité.

14. Le propriétaire ou l'opérateur du système non fédéral doit amorcer le processus en demandant par écrit au CST de mener des activités de cybersécurité pour protéger le système et ses informations électroniques (paragraphe 33(3) de la *Loi sur le CST*). La chef doit ensuite présenter au ministre une demande écrite énonçant les faits qui lui permettraient de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire (paragraphe 33(2) de la *Loi sur le CST*). Les paragraphes 34(1) et (3) de la *Loi sur le CST* énoncent les conditions légales pour que le ministre puisse délivrer une autorisation de cybersécurité. L'autorisation ministérielle n'est valide qu'une fois approuvée par le commissaire au renseignement (paragraphe 28(1) de la *Loi sur le CST*). Ce n'est qu'à ce moment-là que le CST peut exercer les activités autorisées précisées dans l'autorisation.

15. Conformément au paragraphe 27(2) de la *Loi sur le CST*, le ministre peut, en vertu d'une autorisation de cybersécurité, autoriser le CST à acquérir de l'information qui provient ou passe par le système non fédéral, qui 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 leur fonctionnement. L'alinéa 184(2)e) du *Code criminel* s'applique généralement aux personnes qui gèrent la qualité du service d'un système informatique ou sa protection.

16. Malgré toute autorisation de cybersécurité, la *Loi sur le CST* impose des limites aux activités du CST. Le CST 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* (la *Charte*) (paragraphe 22(1) de la *Loi sur le CST*). Toutefois, dans le cadre de ses activités en vertu d'une autorisation, il est permis au CST d'acquérir incidemment de l'information concernant un Canadien ou une personne se trouvant au Canada. Le mot « incidemment » signifie que l'information acquise n'a pas été délibérément recherchée (paragraphe 23(5) de la *Loi sur le CST*).

17. Dans le contexte d'une autorisation de cybersécurité, le CST explique que l'information relative à un Canadien ou à une personne se trouvant au Canada qui peut être acquise

comprend notamment les renseignements personnels au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*, les communications entre un avocat et son client, les renseignements commerciaux (propriété intellectuelle, secrets commerciaux, etc.), le nom de domaine, l'adresse électronique et l'adresse IP. Il peut également s'agir de communications privées qui ont le Canada comme origine comme destination, et dont l'auteur a une attente raisonnable de protection en matière de vie privée. Je remarque que, bien que l'interception de communications privées constitue une infraction criminelle, l'article 50 de la *Loi sur le CST* prévoit une exemption et dispose que la partie VI du *Code criminel* (Atteinte à la vie privée) ne s'applique pas à l'interception d'une communication autorisée par le ministre.

18. En cas de telle interception de communication, il faut suivre des mesures législatives et politiques strictes pour utiliser, analyser et conserver cette information. 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 (article 24 de la *Loi sur le CST*).

B. *Loi sur le commissaire au renseignement*

19. Selon l'article 12 de la *Loi sur le CR*, le rôle du commissaire au renseignement consiste à mener un examen quasi judiciaire des conclusions du ministre en vertu desquelles certaines autorisations sont délivrées, pour déterminer si ces conclusions sont raisonnables.

20. L'article 14 de la *Loi sur le CR* précise que, dans le cas d'une autorisation de cybersécurité, le commissaire au renseignement examine les conclusions que le ministre a tirées au titre des paragraphes 34(1) et (3) de la *Loi sur le CST*.

21. Le ministre est tenu par la loi de fournir au commissaire au renseignement toute l'information dont il disposait à titre de décideur (article 23 de la *Loi sur le CR*). Comme l'établit la jurisprudence du commissaire au renseignement, cette obligation vise toute information verbale consignée par écrit, dont ceux des séances d'information ministérielles.

Le commissaire au renseignement n'a cependant pas droit aux documents confidentiels du Cabinet (article 26 de la *Loi sur le CR*).

22. Conformément à l'article 23 de la *Loi sur le CR*, le ministre a confirmé dans sa lettre de présentation qu'on m'avait transmis tous les documents dont il disposait pour prendre sa décision. Voici les documents qui composent le dossier :

    a) la lettre du ministre adressée au commissaire au renseignement, datée du [redacted];
    b) l'autorisation du ministre, datée du [redacted];
    c) la note d'information de la chef adressée au ministre, datée du [redacted];
    d) la demande de la chef, datée du [redacted], accompagnée de douze annexes, lesquelles comprennent notamment :
        i. les lettres de demande de [redacted];
        ii. l'ensemble des politiques sur la mission en matière de cybersécurité (les politiques sur la mission), approuvé le 28 février 2022;
        iii. deux arrêtés ministériels et
    e) le document intitulé « Summary Deck – Overview of the Activities » [présentation sommaire – aperçu des activités].

III. NORME DE CONTRÔLE

23. La *Loi sur le CR* exige que le commissaire au renseignement examine si les conclusions du ministre sont raisonnables. La jurisprudence du commissaire au renseignement établit que la norme de la décision raisonnable qui s'applique au contrôle judiciaire d'un acte administratif est la même que celle qui s'applique aux examens menés par le commissaire au renseignement.

24. Dans le cadre d'un examen 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 [*Mason*]). Au paragraphe 99 de l'arrêt *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65 [*Vavilov*], la Cour suprême du Canada décrit brièvement en quoi consiste une décision raisonnable :

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

25. Les contraintes factuelles et juridiques pertinentes peuvent comprendre le régime législatif applicable, l'incidence de la décision et les principes d'interprétation des lois. En fait, il est nécessaire, pour comprendre ce qui est raisonnable, de tenir compte du contexte de la décision faisant l'objet de l'examen et de celui de l'examen lui-même. Il est donc nécessaire de comprendre le rôle du commissaire au renseignement, qui fait partie intégrante du régime législatif institué par la *Loi sur le CR* et la *Loi sur le CST*.

26. Un examen de la *Loi sur le CR* et de la *Loi sur le CST*, de même que les débats législatifs, montrent que le législateur a créé le rôle de 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 fins de sécurité nationale ainsi que le respect de la primauté du droit et des droits et libertés des Canadiens. Pour maintenir cet équilibre, je considère que le législateur m'a attribué un rôle de gardien et de surveillant des autorisations ministérielles.

27. Une fois convaincu (*satisfied*, en anglais) que les conclusions ministérielles en cause sont raisonnables, le commissaire au renseignement « approuve l'autorisation » (alinéa 20(1)a) de la *Loi sur le CR*). Si, au contraire, les conclusions sont jugées déraisonnables, il « n'approuve pas l'autorisation » (alinéa 20(1)b) de la *Loi sur le CR*).

IV. ANALYSE

28. Le [redacted], la chef a transmis au ministre une demande écrite d'autorisation de cybersécurité (la demande) relativement à des systèmes appartenant à [redacted] dans le cadre de son mandat. [redacted] Bien que la question ne se pose pas en l'instance, le fait d'inclure [redacted] pourrait en élargir la portée, ce qui ajouterait à la complexité des conclusions du ministre et de l'examen du commissaire au renseignement.

29. [redacted] a demandé l'aide du CST par écrit. La demande sollicitait une autorisation ministérielle pour [redacted] la demande constitue [redacted]

30. [redacted] d'importance pour le gouvernement du Canada, au sens de l'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada*, émis le 25 août 2020. Une description de [redacted], ainsi que des activités énoncées dans l'autorisation, figure à l'annexe de la présente décision (annexe A), laquelle n'est pas destinée à la diffusion publique pour le moment, afin que les activités puissent être menées à bien. L'inclusion de cette information dans une annexe facilite la lecture de la future version publique de la présente décision et garantit qu'elle contient la nature des faits qui me sont relatés, ce qui, autrement, ne serait possible qu'en consultant le dossier.

31. En bref, les activités proposées consistent à déployer [description de l'activité] [redacted] sur [redacted] systèmes. [redacted]

[redacted] acquis par les systèmes. [redacted]

32. L'autorisation autorise la mise en œuvre d'activités de cybersécurité sur les systèmes de [redacted] Les annexes X, XI et XII du dossier énumèrent les organismes qui utilisent les systèmes [redacted] et qui seraient donc admissibles à recevoir les services de cybersécurité du CST en vertu de l'autorisation. Le CST a adopté le protocole utilisé dans l'autorisation ministérielle fédérale de cybersécurité qui consiste à aviser le ministre et le commissaire au renseignement lorsque le CST intègre de nouveaux organismes. À l'heure actuelle, je ne vois aucune entrave d'ordre juridique à ce que le CST procède de cette façon, dans la mesure où les organismes utilisent les systèmes décrits dans l'autorisation. Je comprends que les organismes ne sont pas intégrés sans leur participation.

33. Compte tenu de ces faits, le ministre a conclu que les conditions prévues aux paragraphes 34(1) et (3) de la *Loi sur le CST* étaient respectées, puis a délivré l'autorisation. Je dois maintenant me demander si les conclusions du ministre sont raisonnables.

A. Paragraphe 34(1) de la *Loi sur le CST*

i. Déterminer si les activités sont raisonnables et proportionnelles

34. Pour que le ministre délivre une autorisation de cybersécurité, il doit conclure « qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités » (paragraphe 34(1) de la *Loi sur le CST*).

35. Déterminer si une activité est « raisonnable » diffère de l'examen selon la norme de la « décision raisonnable » effectué par le commissaire au renseignement. Le ministre doit conclure que toute activité qui serait permise par l'autorisation est raisonnable et proportionnelle en appliquant sa compréhension de ce que ces seuils impliquent. Déterminer si une activité est raisonnable et proportionnelle constitue un exercice contextuel, et le ministre peut tenir compte d'un certain nombre de facteurs. Néanmoins, je suis d'avis que la compréhension des deux seuils doit refléter au minimum certains éléments fondamentaux. Une activité raisonnable doit être permise par une interprétation raisonnable de la loi et avoir un lien rationnel avec ses objectifs. Quant à la nature « proportionnelle », il s'agit d'équilibrer les intérêts en jeu, ce qui, dans le contexte d'une autorisation de cybersécurité, inclura la protection des systèmes et l'incidence sur les intérêts des Canadiens en matière de protection de la vie privée.

36. Le commissaire au renseignement détermine si les conclusions du ministre, lesquelles comprennent sa compréhension des seuils, sont « raisonnables », en procédant à un examen quasi judiciaire selon la norme de décision raisonnable, expliquée précédemment.

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

37. Le ministre a conclu, au paragraphe 34 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 de protéger les systèmes fédéraux et les systèmes d'importance contre les méfaits, l'utilisation non autorisée ou la perturbation.

38. En délivrant l'autorisation, le ministre a implicitement accepté que les activités de cybersécurité ne contreviendraient pas aux dispositions législatives qui interdisent d'acquérir délibérément de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada et de mener des activités visant un Canadien ou à une personne se trouvant au Canada (paragraphes 22(1), 23(4) et (5) de la *Loi sur le CST*). Les politiques sur la mission en matière de cybersécurité du CST, approuvées le 28 février 2022 — l'ensemble des principes et des exigences stratégiques visant à guider le

personnel du CST travaillant dans le cadre du volet du mandat du CST touchant la cybersécurité — énoncent au paragraphe 5.2.1 que les activités de cybersécurité ne sont pas considérées comme visant les personnes physiques, à condition qu'elles mettent l'accent sur la cybermenace qui pèse sur le système. Cette position implique logiquement que toute information se rapportant à un Canadien ou à une personne se trouvant au Canada qui a été acquise dans le cadre de ces activités ne l'a pas été délibérément, mais incidemment.

39. À titre de précision, le CST acquerra nécessairement de l'information au sujet de Canadiens ou de personnes se trouvant au Canada dans le cadre de ses activités de cybersécurité énoncées dans l'autorisation. Les systèmes de [redacted] sont situés au Canada et l'information qui y est stockée, de par sa nature, 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 l'information au sujet des employés de [redacted], mais comprend également de l'information provenant de membres du public canadien qui, par exemple, communiquent avec [redacted] par courriel.

40. J'estime que la position du CST selon laquelle les activités ne visent pas des Canadiens et, par conséquent, la conclusion du ministre sont raisonnables. En effet, la conclusion du ministre concorde avec le paragraphe 23(3) de la *Loi sur le CST*, qui stipule expressément que, malgré la disposition qui lui interdit de mener des activités qui visent des Canadiens ou des personnes se trouvant au Canada, le CST peut mener des activités dans les systèmes afin de découvrir ou d'isoler des logiciels malveillants et de les empêcher d'y causer des dommages ou d'atténuer ceux-ci. La conclusion du ministre cadre également avec les volets du mandat du CST touchant la cybersécurité et l'assurance de l'information, qui ne peuvent être réalisés qu'en accédant aux systèmes au Canada. Je suis convaincu que le dossier appuie la conclusion du ministre selon laquelle les activités menées par le CST sont axées sur l'acquisition d'informations sur les cybermenaces et ne visent pas des Canadiens, et qu'elles respectent donc l'interdiction prévue par la loi.

41. Le ministre justifie le caractère raisonnable des activités pour deux raisons principales : la participation du CST à l'intervention en matière de cybersécurité est nécessaire compte

tenu du rôle clé joué par [redacted], et les activités visées par l'autorisation demandée sont efficaces.

42. En ce qui concerne la première raison, [redacted] délivre, [redacted] De plus, le ministre explique que [redacted] joue un rôle central dans [redacted]

43. Le dossier explique que [description des menaces] [redacted] Le CST évalue que [redacted] Le CST évalue également que [redacted] le système de [redacted], ce qui a donné lieu à l'autorisation de cybersécurité actuelle afin d'aider à protéger son système.

44. D'après l'information fournie par la chef, le ministre signale que, même avec l'aide que le CST apporte actuellement à [redacted] En effet, le CST a observé [redacted] Selon le ministre, [redacted] solutions de cybersécurité dans le système de [redacted] est raisonnable compte

tenu de [redacted]

45. En ce qui concerne [redacted], le CST a observé [redacted] Le CST a été informé [redacted] Le CST évalue que [redacted].

46. Par conséquent, le ministre conclut que la situation actuelle de [redacted] en matière de cybersécurité ne suffit pas pour découvrir et combattre [nature de la menace] [redacted] Le ministre étaye également sa conclusion en s'appuyant sur [redacted] de [redacted] et [redacted] où [redacted] sont situés. Je note que le dossier n'indique pas la durée prévue de la présence du CST dans les systèmes [redacted] au-delà de la période de validité d'un an de l'autorisation demandée.

47. Le deuxième motif invoqué par le ministre à l'appui de la conclusion que les activités sont raisonnables est qu'elles seraient efficaces. Il peut être difficile de détecter les cybermenaces et les compromissions peuvent avoir un effet rapide et dévastateur. L'objectif de ces activités est d'aider [redacted] à identifier [redacted] les indicateurs de compromission, suprimer la présence de tout acteur de menace identifié et

renforcer la posture de cybersécurité pour se protéger contre les menaces futures. Les activités permettraient au CST de découvrir et de mieux comprendre les cyberactivités malveillantes ou d'autres indicateurs de compromission, pour ainsi conseiller [redacted] sur la façon de protéger leurs systèmes. Ces activités permettraient également au CST de prendre des mesures d'atténuation [redacted]

48. Le dossier comprend des preuves à l'appui de l'efficacité des activités. [redacted] Le [redacted] rapports d'activités malveillantes. De plus, le CST a fourni des recommandations à [redacted] sur [redacted] Le CST continue également de fournir des recommandations touchant l'architecture de sécurité de [redacted].

49. Le ministre s'appuie à juste titre sur la demande de la chef pour tirer des conclusions sur l'état des systèmes de [redacted] ainsi que sur l'efficacité des activités de cybersécurité proposées (paragraphe 33(2) de la *Loi sur le CST*). En effet, on ne s'attend pas à ce que le ministre possède l'expertise technique du CST. Néanmoins, une conclusion ministérielle raisonnable doit être justifiée, transparente et intelligible (*Vavilov*, au para 99). Cela signifie que le ministre doit démontrer qu'il comprend les raisons qui justifient ses conclusions.

50. Je suis d'avis que les conclusions du ministre témoignent de cette compréhension. Ses conclusions indiquent qu'il a tenu compte du lien entre les besoins actuels de [redacted] et les activités proposées du CST, et qu'il en était satisfait. Il existe un lien rationnel clair entre les activités de cybersécurité proposées par le CST et leur objectif, lequel consiste à aider à protéger des systèmes non fédéraux. Le ministre s'appuie sur le rôle essentiel et stratégique joué par [redacted], ce qui, à mon avis, étaye sa conclusion. Il est également évident, à l'examen du dossier, que les activités de cybersécurité sont fondées et qu'elles aident à remplir le mandat du CST en matière de cybersécurité et d'assurance de l'information quant aux systèmes de [redacted]

[redacted] Compte tenu de la nature de l'objectif et de l'information figurant au dossier concernant la nature des activités, j'estime raisonnable la conclusion du ministre lorsqu'il qualifie les activités de raisonnables.

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

51. Le ministre a conclu, au paragraphe 45 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités autorisées sont proportionnelles, parce qu'elles sont liées de façon rationnelle à l'objectif et qu'elles portent une atteinte minimale aux droits et aux libertés des tiers ainsi qu'à la capacité d'accéder aux systèmes de [redacted] et de les utiliser. Selon le ministre, l'atteinte est minimale en raison des mesures suivantes qui ont été mises en place pour protéger l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada et qui serait acquise incidemment :

a. seule l'information nécessaire pour protéger les systèmes sera recueillie;
b. l'information ne sera conservée que si elle est considérée comme nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages causés au système, aux systèmes fédéraux et aux autres systèmes d'importance;
c. l'information qui porte sur un Canadien ou sur une personne se trouvant au Canada ne sera conservée que si elle est jugée essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés au système, aux systèmes fédéraux et aux autres systèmes d'importance;
d. l'information non évaluée ne sera pas conservée plus de [redacted];
e. la plupart des analyses et des mesures d'atténuation sont effectuées au moyen de processus automatisés qui limitent l'accès des employés du CST à l'information;
f. l'accès à l'information acquise en vertu de l'autorisation est réservé aux employés autorisés du CST qui ont reçu la formation appropriée et qui ont besoin de la connaître pour accomplir leurs fonctions;
g. toute l'information est protégée conformément aux politiques sur la mission;
h. chaque recherche effectuée sur l'information non évaluée acquise est vérifiable conformément aux politiques sur la mission et aux autres politiques organisationnelles;

i. la technologie utilisée est sujette à un contrôle de conformité aux lois et aux politiques.

52. Le ministre a étayé sa conclusion quant au caractère proportionnel en s'appuyant sur les mêmes mesures que celles décrites dans la décision 2200-B-2023-05, qui traitait également d'une autorisation de cybersécurité pour une entité non fédérale (*décision en matière de cybersécurité pour une entité non fédérale*). Je reconnais que le ministre n'avait pas encore pris connaissance de mes commentaires dans la *décision en matière de cybersécurité pour une entité non fédérale* au moment de délivrer l'autorisation visée par la présente décision. Dans cette décision, je remarquais que les mesures énoncées aux points a) à d) reflètent essentiellement les exigences énoncées au paragraphe 34(3) de la *Loi sur le CST* et que toute autorisation de cybersécurité doit respecter. Ces mesures ne sont pas très utiles pour étayer la conclusion du ministre selon laquelle les activités sont proportionnelles, car il s'agit d'une condition légale distincte qui doit être satisfaite de façon indépendante (paragraphe 34(1) de la *Loi sur le CST*). J'ai également remarqué qu'il manquait d'information précise pour certaines des mesures énoncées par le ministre, notamment en ce qui concerne le type d'information ne faisant pas partie de [TRADUCTION] « la majeure partie de l'analyse » qui est effectuée au moyen de processus automatisés, et la nature de l'information en question.

53. J'ai aussi fait observer que l'élément c) énonce que l'information se rapportant au Canada peut être conservée lorsqu'elle est essentielle à la protection de [redacted] ou d'autres systèmes fédéraux et systèmes d'importance. Toutefois, dans le cas des autorisations délivrées en vertu du paragraphe 27(2) – autorisations de cybersécurité pour les systèmes non fédéraux, le sous-alinéa 34(3)d)(ii) de la *Loi sur le CST* stipule que la conservation d'information liée au Canada doit avoir pour but de protéger les systèmes désignés comme étant d'importance pour le gouvernement fédéral en vertu du paragraphe 21(1) (systèmes non fédéraux). J'ai souligné que la conservation initiale doit respecter les exigences législatives. Mes commentaires s'appliquent également à la présente autorisation.

54. Les mesures mises en place pour contrôler l'information une fois qu'elle a été acquise constituent la question centrale à l'appui de la conclusion du ministre concernant la proportionnalité. Je conviens qu'il peut être raisonnable de s'appuyer sur des politiques et des pratiques qui limitent l'utilisation et la divulgation de l'information acquise, et l'accès à celle-ci, pour conclure que les activités sont proportionnelles. Ces limites peuvent être particulièrement pertinentes lorsque les activités de cybersécurité permettent l'acquisition d'un grand volume d'information, notamment de l'information pour laquelle il existe une attente raisonnable de protection en matière de vie privée. Néanmoins, dans le contexte du droit administratif, le décideur doit être attentif et sensible à toutes les questions clés (*Mason*, au para 74). Le fait que le ministre se soit fié aux mesures strictes de contrôle de l'information acquise soulève la question de savoir s'il s'est suffisamment penché sur d'autres questions clés pour arriver à sa conclusion concernant la proportionnalité.

55. La responsabilité du ministre de cerner les questions clés et d'y être attentif et sensible est lourde dans un contexte non contradictoire, y compris lorsque le ministre décide de délivrer ou non une autorisation. La Cour suprême du Canada a insisté sur l'importance de cerner et de traiter les questions clés, déclarant que le fait que le décideur n'ait « pas réussi à s'attaquer de façon significative aux questions clés ou aux arguments principaux formulés par les parties permet de se demander s'il était effectivement attentif et sensible à la question qui lui était soumise » (*Mason*, au para 74). Toutefois, en vertu du régime d'autorisation, le ministre ne dispose pas des observations des parties adverses.

56. L'examen quasi judiciaire du commissaire au renseignement consiste notamment à déterminer si le ministre a suffisamment examiné les questions clés. En effet, la jurisprudence du commissaire au renseignement a souligné à maintes reprises que, pour que les conclusions ministérielles soient raisonnables, il faut qu'elles démontrent une compréhension des activités et de leurs effets sur la primauté du droit et les intérêts des Canadiens en matière de protection de la vie privée (voir, par exemple, la décision 2200-B-2023-01, au para 78; décision 2200-A-2023-02, au para 61). L'examen selon la norme de la décision raisonnable que je dois effectuer s'étend logiquement à la question de savoir si le ministre a tout simplement omis de cerner une question clé. La fonction de surveillance du

commissaire au renseignement dans un contexte où aucune partie ne s'oppose à l'autorisation du ministre m'oblige à le faire. De plus, les tribunaux reconnaissent que les juges qui tranchent des questions dans le cadre d'une procédure *ex parte* doivent jouer un rôle actif pour veiller à ce que les questions pertinentes soient examinées et prises en considération, en particulier dans le contexte de la sécurité nationale (*Canada (Citoyenneté et Immigration) c Harkat*, 2014 CSC 37, para 46). Bien que je ne sois pas juge, je suis d'avis que les mêmes principes s'appliquent en ce qui concerne le rôle du commissaire au renseignement.

57. Veiller à ce qu'une autorisation ministérielle raisonnable tienne compte de façon significative de toutes les questions clés est également tout à fait cohérent avec le régime législatif. En effet, la délivrance d'une autorisation est une responsabilité ministérielle qui ne peut être déléguée. Il s'agit d'une lourde responsabilité, car les activités autorisées pourraient contrevenir aux lois canadiennes et empiéter sur les intérêts des Canadiens en matière de protection de la vie privée. Le législateur ne demande rien de moins au ministre que de confirmer personnellement que le CST a la justification de mener des activités illégales.

58. Cette responsabilité revêt un poids supplémentaire compte tenu de la dimension constitutionnelle associée aux activités du CST qui portent atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens et des personnes se trouvant au Canada. La violation de l'attente raisonnable de protection en matière de vie privée par l'État – en l'occurrence, le CST en tant que représentant du gouvernement – peut équivaloir à une fouille, à une perquisition ou à une saisie. L'article 8 de la *Charte* protège les Canadiens et les personnes se trouvant au Canada contre les fouilles, les perquisitions et les saisies abusives effectuées par l'État. En effet, pour que le ministre puisse délivrer une autorisation, le législateur lui demande également de confirmer que les activités qui pourraient s'apparenter à une perquisition ou à une saisie sont conformes à la *Charte*. La gravité des conséquences d'une autorisation ministérielle doit se refléter dans les conclusions ministérielles; il est donc primordial que les questions clés ne soient pas ignorées ou négligées.

59. Conclure qu'une autorisation ministérielle est déraisonnable, parce qu'une question clé n'a pas été suffisamment étudiée se distingue sur le plan analytique d'un examen déguisé selon la norme de la « décision correcte » qui consiste à décider de manière indépendante quelles devraient être les questions clés. Les questions clés doivent être fondées sur le dossier, et non inventées.

60. Pour en revenir à l'affaire dont je suis saisi, le dossier montre que, pour déterminer si les activités sont proportionnelles, le ministre ne s'est pas contenté d'examiner les mesures de contrôle de l'information acquise et ne s'est pas fié qu'à celles-ci. Il s'est penché sur d'autres questions clés. Premièrement, le ministre reconnaît que les activités mèneraient à l'acquisition d'information à l'égard de laquelle les Canadiens et les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée, ce qui est nécessaire pour assurer l'efficacité des activités de cybersécurité. En effet, dans la demande, la chef déclare que le CST [obtiendra nécessairement des informations pour lesquelles il existe une attente raisonnable de protection en matière de vie privée] [redacted] Le ministre confirme que le CST [redacted] Deuxièmement, il reconnaît également que les activités donnent accès à de grands volumes d'information [redacted]

61. Ainsi, même si le ministre n'analyse aucun contexte précis dans lequel l'acquisition de l'information porterait atteinte à l'attente raisonnable de protection en matière de vie privée, il reconnaît que certains types d'informations sensibles [redacted] seront acquis. De même, bien que les conclusions du ministre ne fournissent pas de détails sur le volume d'informations qui seront acquises au sujet d'un Canadien ou d'une personne se trouvant au Canada, elles montrent qu'il comprend que ces volumes seront importants étant donné que l'information est acquise à partir de systèmes non fédéraux au Canada.

62. En examinant le dossier de façon globale et contextuelle, je suis d'avis que le ministre a tenu compte des principaux enjeux enracinés dans le dossier lors de l'exercice de mise en balance de son analyse de la proportionnalité. Bien que les mesures d'arrière-plan énoncées dans les politiques du CST visant à contrôler l'information acquise aient pesé lourdement en faveur de la conclusion que les activités étaient proportionnelles, ses conclusions montrent qu'il était conscient – du moins de façon générale – des questions liées aux activités d'acquisition d'information initiales, plus particulièrement en ce qui concerne le volume et la nature de l'information. Dans le cadre de mon examen selon la norme de la décision raisonnable, les conclusions du ministre ne doivent pas être jugées au regard d'une norme de perfection et ne doivent pas nécessairement faire référence à tous les détails que j'aurais, à titre de commissaire au renseignement, voulu y lire (*Vavilov*, au para 91). Bien que je suis d'avis qu'un examen plus approfondi des questions clés aurait étayé le raisonnement du ministre, j'estime que sa mise en balance est justifiée compte tenu du contexte factuel.

63. En ce qui concerne les lois canadiennes susceptibles d'être enfreintes, l'autorisation mentionne que leur nombre est limité, car le CST mènerait ses activités uniquement sur les systèmes non fédéraux pour lesquels il a reçu le consentement exprès du propriétaire. Étant donné que le CST détiendra le consentement requis pour accéder aux systèmes, le risque d'éventuelles infractions aux lois canadiennes est très peu élevé. En cas de violation d'une loi fédérale, les répercussions de l'atteinte seront limitées compte tenu de l'utilisation faite par le CST de l'information acquise. En outre, en cas de contravention à une loi fédérale qui ne figure pas dans la demande du chef, ce dernier en informera le ministre et le commissaire au renseignement.

64. À la lumière de ce qui précède, j'estime que le ministre a suffisamment justifié ses conclusions et qu'elles sont appuyées par le dossier. Il a examiné et compris les questions principales et il a procédé à une mise en balance qui est justifiée par les faits au dossier. Par conséquent, je suis convaincu que la conclusion du ministre concernant la proportionnalité des activités est raisonnable.

B. Paragraphe 34(3) – Conditions d'autorisation – Cybersécurité

65. Le paragraphe 34(3) de la *Loi sur le CST* prévoit que le ministre peut délivrer une autorisation de cybersécurité seulement s'il conclut qu'il y a des motifs raisonnables de croire que les trois conditions suivantes 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 visées à l'article 24 permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux.

i. L'information à acquérir ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire

66. L'information évaluée aux fins de protection des systèmes non fédéraux est conservée conformément aux politiques du CST. Le dossier comprend un tableau de conservation et suppression (*Retention and Disposition Table*) des différentes catégories d'information à acquérir (annexe VIII). Je remarque que la chef écrit dans la demande que [redacted], comme décrit dans l'autorisation, peut, en tout temps, demander au CST de supprimer l'information qu'il a acquise à partir ou par l'intermédiaire de ses systèmes.

67. Étant donné que le CST n'est pas en mesure de déterminer quelle information serait utile pour repérer les activités malveillantes, les activités prévues dans l'autorisation permettent d'obtenir un grand volume d'information. Le ministre explique que le CST traite cette information, principalement par des méthodes automatisées. Ce processus permet de déterminer que certaines informations sont « nécessaires » ou « essentielles ». Toute autre information est jugée comme étant de l'information non évaluée, même si elle a été assujettie au processus automatisé.

68. Le critère du caractère « nécessaire » s'applique à l'information qui ne concerne pas un Canadien ou une personne se trouvant au Canada. Comme il est écrit dans l'autorisation et la section des définitions des politiques sur la mission, l'information est jugée nécessaire lorsqu'elle est requise pour comprendre les activités cybernétiques malveillantes, [redacted] pour aider à protéger les institutions fédérales et les systèmes non fédéraux d'importance.

69. Pour sa part, le critère du caractère « essentiel » défini dans l'autorisation et la section des définitions des politiques sur la mission s'applique à l'information acquise incidemment au sujet d'un Canadien ou d'une personne se trouvant au Canada. L'information est jugée essentielle lorsque, sans elle, le CST ne serait pas en mesure de protéger les systèmes non fédéraux d'importance, les systèmes fédéraux et l'information électronique qui s'y trouve. L'information au sujet de Canadiens et de personnes se trouvant au Canada qui est conservée fait l'objet d'un suivi interne au CST, conformément aux exigences stratégiques énoncées tout au long des politiques sur la mission.

70. Selon le tableau de conservation et suppression du CST (« *Retention and Disposition Table* »), l'information jugée nécessaire ou essentielle peut être conservée [TRADUCTION] « jusqu'à ce qu'elle ne soit plus utile à ces fins, ou à moins de restrictions imposées par le client ». Je comprends que le critère [TRADUCTION] « jusqu'à ce qu'elle ne soit plus utile » signifie que l'information pourrait être utile indéfiniment, mais qu'elle ne sera pas conservée lorsque son utilité à ces fins cessera.

71. En ce qui concerne l'information qui est jugée « essentielle » et qui porte sur un Canadien ou sur une personne se trouvant au Canada, les gestionnaires de l'exploitation doivent examiner l'information sur une base trimestrielle afin de déterminer si elle est toujours essentielle. L'information qui n'est plus essentielle doit être supprimée. Le dossier n'indique pas que le CST effectue des examens périodiques de l'information qui a été jugée « nécessaire ».

72. En ce qui concerne la période de conservation de l'information non évaluée, le ministre explique que certaines atteintes peuvent être repérées seulement après le début d'une activité malveillante. Par conséquent, l'efficacité des activités du CST dépend de sa capacité à analyser plusieurs sources d'information acquise et à faire des renvois entre ces dernières, notamment à l'aide d'indicateurs de compromission. Le ministre explique qu'une période de conservation de [redacted] pour l'information non évaluée constitue une [TRADUCTION] « période d'analyse raisonnable » qui donne au CST le temps de remonter aux origines d'un événement cybernétique et d'examiner son évolution au fil du temps. Il permet également au CST de comparer les nouvelles vulnérabilités par rapport à l'information non évaluée et de déterminer si elles existent au sein des systèmes fédéraux et d'autres systèmes d'importance.

73. Après une période de [redacted], l'information non évaluée sera automatiquement supprimée, sauf si elle est jugée nécessaire ou essentielle pour aider à protéger les systèmes [redacted], les systèmes fédéraux ou les autres systèmes d'importance. L'article 10.2 des politiques sur la mission énonce que l'accès à l'information non évaluée [redacted] doit être strictement contrôlé et limité aux personnes autorisées à mener ou à soutenir des activités de cybersécurité. La liste du personnel autorisé à accéder à l'information non évaluée fait l'objet d'un suivi à des fins de responsabilisation. L'information non évaluée ne peut pas être transmise à d'autres organismes que le CST.

74. Une fois qu'elle est conservée en fonction du critère du caractère « nécessaire » ou « essentiel », l'information est utilisée pour protéger les systèmes non fédéraux, dans ce cas, ainsi que les systèmes fédéraux et les autres systèmes d'importance pour le gouvernement du Canada. La chef indique dans la demande que [redacted], dans ce cas, comprend et accepte l'utilisation de cette information.

75. Compte tenu des importantes restrictions à l'accès à l'information non évaluée et du fait que les cyberactivités malveillantes ne peuvent être détectées qu'après le passage du temps, j'estime que la conclusion du ministre concernant la période de conservation de [redacted] est raisonnable. Dans une décision précédente au sujet des infrastructures

non fédérales (décision 2200-B-2022-05), j'ai suggéré que le CST présente des exemples opérationnels démontrant le caractère raisonnablement nécessaire de la période de conservation de [redacted] pour l'information non évaluée. Mon commentaire n'est que renforcé, puisque le CST était [redacted].

76. J'estime également que la conclusion du ministre est raisonnable lorsqu'il conclut que l'information nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes non fédéraux peut être conservée jusqu'à ce qu'elle ne soit plus utile ou à moins d'une directive imposée par l'entité non fédérale, dans la mesure où un examen périodique est mené sur l'utilité de l'information essentielle. Le dossier reflète clairement que [redacted]

ii. Toute information acquise est nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes non fédéraux

77. Cette condition sous-tend les activités pour lesquelles l'autorisation est demandée. L'utilisation des solutions de cybersécurité spécifiques prévues dans l'autorisation entraînerait l'acquisition d'un grand volume d'information, même si la quasi-totalité de l'information ne révélait pas l'existence d'une cybermenace. Cela soulève la question de savoir s'il est nécessaire pour le CST d'acquérir toute l'information alors que la majorité de cette dernière ne contient pas d'information sur les menaces et sera simplement supprimée après la période de conservation de [redacted].

78. Le ministre s'appuie sur l'évaluation de la chef selon laquelle cette acquisition est nécessaire pour détecter, isoler, prévenir ou atténuer les dommages causés aux systèmes [redacted]. Bien que le ministre ne soit pas un expert technique, ses conclusions fournissent, à mon avis, une justification convaincante et facile à comprendre des raisons pour lesquelles l'acquisition de l'information est nécessaire. Il explique que le CST n'est pas en mesure de prédire [comment les systèmes seront affectés]

[redacted]

Par conséquent, afin d'effectivement atténuer les cybermenaces sophistiquées décrites dans ce dossier, le CST doit acquérir une vaste gamme d'information non évaluée afin d'identifier [redacted]

79. De plus, rien dans le dossier n'indique que le CST pourrait obtenir les mêmes résultats en matière de cybersécurité en utilisant différentes solutions de cybersécurité qui permettent d'obtenir moins d'information, en particulier de l'information concernant les Canadiens.

80. Je suis donc convaincu que les conclusions du ministre sont raisonnables et qu'il a des motifs raisonnables de croire que l'acquisition de l'information est nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes.

iii. Les mesures en place font en sorte que l'information acquise qui concerne des Canadiens ou des personnes se trouvant au Canada sera utilisée, analysée ou conservée seulement si elle est essentielle pour isoler, prévenir ou atténuer des dommages causés aux systèmes non fédéraux

81. L'article 24 de la *Loi sur le CST* exige que le CST mette en place des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada lorsqu'il utilise, analyse, conserve et divulgue de l'information à leur sujet acquise dans le cadre des volets de son mandat touchant la cybersécurité et l'assurance de l'information. Au paragraphe 61 de l'autorisation, le ministre conclut qu'il a des motifs raisonnables de croire que les mesures requises à l'article 24 sont en place.

82. Le ministre réitère que l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada ne peut être conservée que si elle est jugée essentielle. Cette condition est énoncée dans les politiques sur la mission. Comme il a été mentionné précédemment, l'information est jugée essentielle lorsque le CST serait autrement incapable de découvrir, d'isoler ou de prévenir des dommages aux systèmes de [redacted], aux systèmes fédéraux et aux autres systèmes d'importance.

83. L'article 8.2.2 des politiques sur la mission énonce qu'un employé autorisé du CST applique le [TRADUCTION] « critère du caractère essentiel » de l'information obtenue. Cette analyse s'effectue au moyen de processus manuels ou automatisés. L'employé doit fournir des justifications lorsqu'il croit que l'information est essentielle. À mon avis, cette mesure favorise le respect de l'obligation prévue à l'article 24 de la *Loi sur le CST* et appuie les conclusions du ministre.

84. Les conclusions du ministre précisent que l'accès à l'information non évaluée acquise en vertu de l'autorisation est limité aux employés autorisés du CST qui sont dûment accrédités pour mener des activités de cybersécurité et qui ont reçu la formation obligatoire sur les procédures de traitement de l'information. De plus, la majeure partie de l'analyse de l'information se fait au moyen de processus automatisés, ce qui limite l'accès des employés au contenu de l'information non évaluée.

85. La conclusion du ministre et le dossier expliquent également comment l'information concernant des Canadiens ou des personnes se trouvant au Canada peut être divulguée, ce qui correspond à l'obligation énoncée à l'article 44 de la *Loi sur le CST*. L'information est seulement communiquée aux personnes ou aux catégories de personnes énoncées dans l'*Arrêté ministériel désignant les destinataires de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui a été acquise, utilisée ou analysée dans le cadre des volets du mandat du CST touchant la cybersécurité et l'assurance de l'information*, délivré le 13 juin 2023 en vertu de l'article 45 de la *Loi sur le CST*. [redacted] Pour obtenir de l'information divulguée par le CST qui concerne un Canadien ou une personne se trouvant au Canada, l'information doit être nécessaire à la protection des systèmes fédéraux ou des systèmes d'importance.

86. Comme indiqué à l'article 24 des politiques sur la mission, des mesures sont en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada lors de la

divulgation d'information concernant des Canadiens. Par exemple, les renseignements personnels peuvent être supprimés afin d'éviter de dévoiler l'identité d'une personne. Les politiques sur la mission décrivent les niveaux d'approbation de divulgation requis pour les différentes catégories d'information. Il faut consigner les approbations.

87. Je note que, [en demandant l'aide du CST] [redacted] a demandé que toutes les informations personnelles ou exclusives soient obscurcies avant d'être partagées et que les informations qui ne sont pas pertinentes pour le mandat du CST soient supprimées conformément au tableau de conservation et suppression. Par conséquent, je crois comprendre que toute divulgation de l'information acquise en vertu de l'autorisation doit d'abord satisfaire à ces directives.

88. Les politiques sur la mission établissent des politiques complexes visant à contrôler et à protéger l'information concernant des Canadiens et des personnes se trouvant au Canada qui est acquise en vertu d'une autorisation de cybersécurité. À titre de rappel, ces politiques et les pratiques du CST ont pesé lourdement sur la conclusion du ministre que les activités sont proportionnelles. Les politiques établissent des processus qui exigent que les employés du CST documentent les justifications pour la préservation, l'utilisation et la divulgation de l'information concernant des Canadiens et des personnes se trouvant au Canada. Si elles sont suivies, ces mesures devraient, à mon avis, permettre au CST de respecter efficacement l'exigence législative de protéger suffisamment cette information.

89. Je suis convaincu que la conclusion du ministre est raisonnable et qu'il a des motifs raisonnables de croire que l'information au sujet de Canadiens ou de 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 de [redacted].

V. REMARQUES

90. Dans la décision 2200-B-2022-06 que j'ai rendue le 8 décembre 2022, j'ai fait une remarque qu'un document dans le dossier préparé par le Centre canadien pour la

cybersécurité [redacted] n'était pas daté. J'ai demandé à ce que tous les documents au dossier soient datés dans les demandes futures. De plus, j'ai indiqué que toute nouvelle information [redacted] doit être fournie afin d'aider le ministre dans sa prise de décision. En effet, les décisions doivent être fondées sur l'information la plus exacte possible. À l'inverse, si aucune nouvelle information n'est disponible, le dossier doit l'indiquer.

91. Cette remarque n'a pas été abordée dans l'affaire dont je suis saisi. Le dossier comportait le même document non daté, mais le dossier démontre que [il y a des informations mises à jour] [redacted] De plus, pendant un exposé du CST à moi-même et à mon équipe en vertu de l'article 25 de la *Loi sur le CR*, [des informations mises à jour ont été fournies] [redacted] Il est nécessaire de s'assurer que l'information est aussi actuelle que possible afin de permettre au ministre de remplir ses responsabilités.

92. Je note aussi que j'ai formulé des remarques dans la décision sur la cybersécurité non fédérale, auxquelles, comme il a été mentionné précédemment, le ministre n'avait pas accès avant l'émission de cette autorisation. Ces remarques s'appliquent aussi dans ce cas. Je m'attends à ce qu'elles soient reflétées dans les autorisations futures. Plus particulièrement, je souligne l'importance de fournir des références aux articles précises des politiques sur la mission sur lesquelles le CST s'est appuyé dans la demande de la chef au ministre, ainsi que de donner des précisions concernant les répercussions sur les droits en matière de vie privée des Canadiens. À cet effet, le dossier de la présente autorisation faisait référence à [redacted] rapports d'activités malveillantes. Dans le contexte où le CST demande l'autorisation pour [redacted] il serait utile pour le ministre de savoir s'il faut conserver l'information concernant les Canadiens afin de détecter les activités malveillantes et si les questions liées à la vie privée ont été abordées dans les rapports. Le CST disposait de cette information dans les rapports et il ne l'a pas transmise au ministre. Je ne vois aucune raison de l'exclure. En effet, cette information permet au ministre de mieux comprendre les répercussions de l'autorisation

qu'il délivrerait et peut constituer une question clé à prendre en considération pour déterminer le caractère raisonnable et proportionnel des activités.

93. Bien que je sois convaincu que les conclusions du ministre sont raisonnables, j'aimerais formuler une observation pour faciliter l'examen et la rédaction des futures autorisations ministérielles. Cette observation ne modifie pas mes conclusions concernant les conclusions du ministre.

A. Utilisation de l'information acquise dans le cadre du mandat du CST

94. J'aimerais aborder la question de l'utilisation de l'information par le CST dans les différents aspects de son mandat. L'autorisation stipule que [TRADUCTION] « les information acquises par le CST dans le cadre d'un aspect de son mandat peuvent ensuite être utilisées au sein du CST pour servir d'autres aspects de son mandat, à condition qu'elles soient pertinentes pour cet aspect et qu'elles répondent à toute exigence particulière de la *Loi sur CST* qui pourrait devoir être respectée, comme l'application de mesures visant à protéger la vie privée d'un Canadien ou d'une personne se trouvant au Canada ». C'est la position du CST pour toutes les autorisations ministérielles touchant la cybersécurité et le renseignement étranger.

95. Une lecture simple de cette déclaration générale suggère que les informations non évaluées acquises dans le cadre d'une autorisation de cybersécurité et qui n'ont pas été jugées nécessaires ou essentielles pourraient, [redacted] être consultées, analysée, utilisées et conservées si elles étaient jugées « pertinentes » pour d'autres aspects du mandat du CST. Étant donné que les activités prévues dans l'autorisation permettraient d'acquérir un grand volume d'information en sachant qu'une certaine quantité répondrait à l'attente raisonnable de protection de la vie privée et que la majorité ne serait pas jugée comme étant nécessaire ou essentielle, la déclaration générale soulève des préoccupations qui ne sont pas abordées dans les conclusions du ministre.

96. Premièrement, l'alinéa 34(3)(d) de la *Loi sur le CST* énonce clairement que l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada acquise en vertu

d'une autorisation de cybersécurité peut être utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux désignés comme étant d'importance pour le gouvernement du Canada. Cela semble indiquer que même si des informations relatives à un Canadien sont acquises en vertu d'une autorisation de cybersécurité, elles ne devraient pas être utilisées pour servir d'autres aspects de son mandat, à moins qu'elles n'aient d'abord été conservées comme étant essentielles pour identifier, isoler, prévenir ou atténuer les dommages à des fins de cybersécurité.

97. Deuxièmement, l'utilisation de l'information par le CST peut être un facteur permettant de déterminer si une autorisation de cybersécurité est raisonnable et proportionnelle. Cela signifie que l'utilisation des informations d'une manière qui n'a pas été clairement reflétée dans les conclusions ministérielles peut aller au-delà de ce qui est permis par l'autorisation.

98. Par exemple, l'acquisition incidentelle d'un grand volume d'information, en sachant qu'une certaine quantité respecterait l'attente raisonnable en matière de vie privée et que la plupart ne serait pas considérée utile, elle pourrait être jugée raisonnable et proportionnelle dans la mesure où elle est nécessaire pour la cybersécurité. Toutefois, cette conclusion peut changer si les informations seront également utilisées à d'autres fins ou pour d'autres aspects du mandat du CST. Les Canadiens peuvent accepter qu'un courriel envoyé par un élève de 12e année à un enseignant puisse être acquis par une entité non fédérale responsable de la cybersécurité du système de l'école en raison de la présence potentielle d'un logiciel malveillant. En même temps, les Canadiens peuvent penser que le CST, au nom du gouvernement fédéral, s'immisce dans la vie privée si ce courriel acquis légalement et ne contenant pas de logiciels malveillants apparaît dans un rapport sur le renseignement étranger. Dans ses conclusions, le ministre ne tient pas compte de l'impact du pouvoir légal du CST d'utiliser des informations dans les cinq aspects de son mandat.

99. Toutefois, après avoir examiné le dossier dans son intégralité, et plus particulièrement l'article 26 des politiques sur la mission en ce qui concerne l'accès et l'utilisation de l'information au sein du CST, il semble que la déclaration générale faite dans l'autorisation soit limitée en pratique. D'après ce que je comprends des politiques sur la mission, tout

accès et toute utilisation d'informations non évaluées acquises en vertu d'une autorisation de cybersécurité doivent être « cohérents » avec l'aspect de cybersécurité du mandat.

100. De plus, l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada peut uniquement être conservée si elle est essentielle pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes. Par conséquent, même si les informations non évaluées peuvent être consultées et utilisées pour d'autres aspects du mandat du CST – pour autant qu'elles soient compatibles avec la cybersécurité – toute information liée au Canada identifiée grâce à cet accès ne pourrait être conservée ou utilisée que si elle répond à l'exigence d'essentialité.

101. J'ajoute que les exemples cités dans le dossier concernant l'utilisation d'informations pour les différents aspects du mandat du CST suggèrent que cela n'est fait que pour les informations qui ont déjà été jugées nécessaires ou essentielles, ce qui donne à penser que le CST n'utilise pas d'informations non évaluées pour ces autres aspects. Par exemple, la chef déclare que les informations acquises dans le cadre d'une autorisation de cybersécurité concernant [redacted] – informations essentielles ou nécessaires – seraient pertinentes pour l'aspect « renseignement étranger » du mandat du CST.

102. La déclaration générale prétend que le CST est libre d'utiliser toutes les informations qu'il acquiert pour tous les aspects de son mandat, pour autant qu'elles soient pertinentes pour cet aspect. Toutefois, le cadre politique et les pratiques du CST, du moins mon examen et ma compréhension de ces derniers, montrent que, dans ce cas, l'accès et l'utilisation de l'information non évaluée sont limités et doivent être cohérents avec les objectifs de cybersécurité. À mon avis, la déclaration générale exige que des détails supplémentaires expliquant ces limites soient clairement définis dans le dossier. Il est impératif que le ministre et moi-même comprenions comment le CST agit dans les limites imposées par la loi. Je m'attends à ce que ce soit le cas dans les autorisations futures.

VI. CONCLUSIONS

103. 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 70 de l'autorisation sont raisonnables.

104. Par conséquent, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation de cybersécurité pour des activités visant à protéger des infrastructures non fédérales, délivrée par le ministre le [redacted].

105. Ainsi que le déclare le ministre et comme le dispose le paragraphe 36(1) de la *Loi sur le CST*, cette autorisation vient à expiration un an après le jour de mon approbation.

106. Comme l'indique 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.

107. Si l'écoulement du temps le permet, je suis d'avis que le public aurait avantage à savoir que le CST a joué un rôle important dans le soutien et le rétablissement de la situation de [redacted] en matière de cybersécurité. La divulgation des activités passées permet au public de constater concrètement l'importance et la valeur du rôle du CST et, par conséquent, crée une aura de confiance essentielle à tout organisme de sécurité nationale.

Le 30 novembre 2023

(Original signé)
L'honorable Simon Noël, C.R.
Commissaire au renseignement