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-2022-06

AFFAIRE INTÉRESSANT UNE DEMANDE PRÉSENTÉE PAR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS À LA MINISTRE DE LA DÉFENSE NATIONALE AU SUJET D'UNE AUTORISATION DE CYBERSÉCURITÉ CONCERNANT DES ACTIVITÉS MENÉES DANS DES INFRASTRUCTURES NON FÉDÉRALES – [redacted]

EN VERTU DU PARAGRAPHE 27(2) DE LA *LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS*

COMMISSAIRE AU RENSEIGNEMENT

DÉCISION ET MOTIFS

Le 8 décembre 2022

Canada

TABLE DES MATIÈRES

I. APERÇU

1. Le [redacted] la ministre de la Défense nationale (la ministre) a délivré une *Autorisation de cybersécurité concernant des activités menées dans des infrastructures non fédérales* – [redacted] (l'*autorisation*) en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (la *Loi sur le CST*).

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

3. Conformément à l'article 23 de la *Loi sur le CR*, la ministre a confirmé dans sa lettre de présentation qu'elle m'avait fourni tous les renseignements dont elle disposait lorsqu'elle a délivré l'*autorisation*.

4. Mon examen du dossier confirme que la ministre, avant d'accorder l'*autorisation*, avait reçu une demande écrite (la *demande*) de la chef du CST, qui était accompagnée notamment de la demande écrite du propriétaire ou de l'opérateur de l'infrastructure de l'information, comme l'exigent les paragraphes 33(1) et (3) de la *Loi sur le CST*.

5. La *demande* expose les faits qui ont permis à la ministre de conclure, conformément au paragraphe 33(2) de la *Loi sur le CST*, qu'il y avait des motifs raisonnables de croire que l'*autorisation* est nécessaire et que les conditions de sa délivrance énoncées à l'article 34 de la *Loi sur le CST* sont remplies.

6. Plus précisément, la ministre a conclu, conformément au paragraphe 34(1) de la *Loi sur le CST*, qu'elle avait des motifs raisonnables de croire que les activités de cybersécurité proposées décrites dans l'autorisation sont raisonnables et proportionnelles compte tenu de la nature de l'objectif à atteindre et des activités.

7. La ministre a également conclu qu'elle avait des motifs raisonnables de croire que les conditions énoncées au paragraphe 34(3) de la *Loi sur le CST* étaient remplies.

8. Pour les motifs exposés ci-dessous, je suis convaincu que les conclusions de la ministre sont raisonnables. Par conséquent, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR,* j'approuve l'*autorisation* délivrée par la ministre relativement à [redacted]

II. CONTEXTE

9. [redacted]

10. [redacted]

11. Dans l'exercice de ces fonctions, [redacted] détient des informations d'importance pour le gouvernement fédéral, dont [redacted]

12. [redacted] les informations électroniques et l'infrastructure de l'information constituent un système d'importance au sens de *l'Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada*, qui a été émis le 25 août 2020.

13. Le [redacted] le Centre de la sécurité des télécommunications (CST) a reçu de l'information de [redacted]

[redacted]

14. [redacted] a également informé le CST que [redacted]

15. [redacted]

16. Le dossier montre que [redacted] Plus précisément, selon le dossier, [redacted] serait presque assurément constitué de [redacted]

17. [redacted]

18. [redacted]

19. [redacted]

20. [redacted]

21. Le [redacted] le CST, se fondant sur informations reçues de [redacted] a informé [redacted] du compromis.

22. Le [redacted] le chef de l'information [redacted] de [redacted] – qui a le pouvoir de donner accès aux dispositifs et réseaux électroniques de [redacted] – ont transmis une demande écrite au CST. Ils demandaient essentiellement au Centre canadien pour la cybersécurité (CCC) de mener des activités de cyberdéfense afin d'aider [redacted] à protéger les informations électroniques et l'infrastructure de l'information dont le contrôle et la surveillance relèvent de sa responsabilité.

23. Le [redacted] la chef du CST a présenté une *demande* à la ministre de la Défense nationale afin d'obtenir l'*autorisation* de mener des activités qui peuvent contrevenir à des lois fédérales ou risquent de porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

24. Il est expliqué dans la *demande* que la posture de sécurité actuelle de [redacted] ne permet pas de repérer et de contrer de façon satisfaisante [redacted]

25. De fait, [redacted]

26. Ce qu'on sait, c'est que le compromis [redacted]

27. Comme il est précisé dans la *demande*, il est probable que [redacted]

28. [redacted]

29. Par conséquent, la *demande* fait état des motifs justifiant le déploiement des solutions de cybersécurité [redacted] du CST : les solutions [redacted] Celles-ci, permettront de veiller à ce que les lacunes soient repérées et à ce que la posture de [redacted] soit adéquate pour protéger l'information cruciale.

30. Ces solutions de cybersécurité proposées serviraient à acquérir de l'information appuyant les solutions avancées en matière de détection et d'analyse des intrusions grâce auxquelles le CST pourra isoler, prévenir ou atténuer des dommages aux informations électroniques ou à l'infrastructure de l'information de [redacted] Elles permettraient également au CST de recommander les mesures d'atténuation qui seraient appliquées soit par [redacted] soit par lui-même avec le consentement de [redacted]

31. Comme le précise la *demande*, les solutions de cybersécurité auraient pour effet de [redacted] l'infrastructure de l'information. Ces solutions [redacted] la récupération d'informations pertinentes.

32. En déployant les solutions de cybersécurité proposées, le CST fournirait à [redacted] une évaluation de [redacted] Le CST donnerait aussi à [redacted] des instructions et un soutien continu durant le déploiement. Tout incident d'envergure qui est

découvert serait par ailleurs signalé à [redacted] De la sorte, [redacted] pourrait renforcer et améliorer sa posture de cybersécurité à long terme.

33. Il est également souligné dans la *demande* que le CST, en aidant [redacted] améliorerait sa propre compréhension de [redacted] ce qui lui permettrait de mieux protéger les institutions fédérales et d'autres systèmes d'importance pour le gouvernement fédéral.

34. La *demande* renferme l'explication selon laquelle l'information acquise par le CST sur l'infrastructure de [redacted] serait aussi nécessaire pour comprendre les cyberactivités malveillantes, notamment [redacted]

35. Outre les objectifs à atteindre, la *demande* décrit comment l'information recueillie au moyen des solutions de cybersécurité serait stockée, analysée et conservée. Elle énonce aussi les mesures et les mécanismes en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada.

36. Le [redacted] la ministre de la Défense nationale a délivré l'*autorisation*.

III. LÉGISLATION

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

37. Comme l'énonce le paragraphe 15(1) de la *Loi sur le CST*, le CST est l'organisme du renseignement électromagnétique du Canada en matière de renseignement étranger et l'expert technique de la cybersécurité et de l'assurance de l'information.

38. Le mandat du CST comporte cinq volets, dont la cybersécurité et l'assurance de l'information. Comme le précise l'article 17 de la *Loi sur le CST*, le CST peut, en ce qui a trait à ce volet :
a) fournir des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral

désignées comme telles en vertu du paragraphe 21(1) de la *Loi sur la CST* et b) acquérir, utiliser et analyser de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir de tels avis, conseils et services.

39. Lorsqu'il mène ces activités, il peut arriver que le CST contrevienne à d'autres lois fédérales, comme la partie VI du *Code criminel,* qui traite des atteintes à la vie privée. Il peut aussi se livrer à des activités visant l'acquisition d'information qui risque de porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada, pourvu qu'il les mène au titre d'une autorisation délivrée en vertu du paragraphe 27(2) de la *Loi sur le CST*.

40. Le paragraphe 27(2) de la *Loi sur le CST* décrit le régime de délivrance d'autorisations dans la réalisation du volet du mandat du CST touchant la cybersécurité et l'assurance de l'information relativement aux activités menées dans une infrastructure non fédérale désignée comme étant d'importance pour le gouvernement fédéral. La désignation est une condition préalable à la délivrance de l'autorisation par la ministre.

41. Plus précisément, ce paragraphe dispose que la ministre peut autoriser le CST, malgré toute autre loi fédérale, à : 1) accéder à une infrastructure de l'information d'importance pour le gouvernement fédéral désignée comme telle au titre du paragraphe 21(1) de la *Loi sur la CST* et 2) acquérir de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée afin d'aider à protéger cette infrastructure, dans les cas visés à l'alinéa 184(2)e) du *Code criminel*, LRC 1985, c C-46, contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

42. La ministre délivre l'autorisation de cybersécurité si elle conclut que les conditions énoncées aux paragraphes 34(1) et (3) de la *Loi sur le CST* sont remplies.

B. La *Loi sur le commissaire au renseignement*

43. Selon l'article 12 de la *Loi sur le CR*, le commissaire au renseignement est chargé d'examiner les conclusions sur lesquelles reposent certaines autorisations accordées au titre de la *Loi sur le CST*. Si les conclusions sont raisonnables, il approuve l'autorisation dans une décision écrite et motive sa décision.

44. L'article 14 de la *Loi sur le CR*, qui porte sur la délivrance des autorisations de cybersécurité, énonce que le commissaire au renseignement doit examiner si les conclusions de la ministre sur lesquelles repose l'autorisation sont raisonnables.

45. Le paragraphe 23(1) de la *Loi sur le CR* dispose que l'examen quasi judiciaire du commissaire au renseignement doit se fonder sur les renseignements dont disposait la ministre pour accorder l'autorisation. Ceci inclut toutes les informations orales et écrites.

46. Le commissaire au renseignement approuve l'autorisation s'il est convaincu que les conclusions de la ministre sont raisonnables (paragraphe 20(1) de la *Loi sur le CR*).

47. L'autorisation est valide seulement une fois qu'elle est approuvée par le commissaire au renseignement (paragraphe 28(1) de la *Loi sur le CST*). Avant cette approbation, le CST ne peut mener les activités décrites dans l'autorisation.

48. La décision du commissaire au renseignement peut faire l'objet d'un appel à la Cour fédérale sur présentation d'une demande de contrôle judiciaire, en application de l'article 18 de la *Loi sur les cours fédérales*, LRC 1985, c F-7.

IV. LA NORME DE CONTRÔLE

49. Comme il est indiqué plus haut, le commissaire au renseignement doit, conformément aux articles 12 et 14 de la *Loi sur le CR*, examiner si les conclusions de la ministre sont raisonnables.

50. Le terme « raisonnable » n'est pas défini dans la *Loi sur le CR* ni dans la *Loi sur le CST*. Toutefois, dans la jurisprudence en droit administratif, c'est un terme qui a été associé au processus de contrôle judiciaire des décisions administratives.

51. Selon le paragraphe 4(1) de la *Loi sur le CR*, le commissaire au renseignement doit être un juge à la retraite d'une juridiction supérieure. Toutefois, le commissaire n'est pas une cour de justice. Par conséquent, il n'effectue pas un « contrôle judiciaire », mais bien un « contrôle quasi judiciaire » des conclusions de la ministre, qui joue le rôle de décideur administratif. Les décisions rendues par le commissaire au renseignement ont établi que, quand le législateur emploie le terme « raisonnable » dans le contexte de l'examen quasi judiciaire de décisions administratives, il entend lui donner le même sens que dans la jurisprudence en droit administratif. Pour ces raisons, je vais appliquer la norme de la décision raisonnable lors de mon examen.

52. L'arrêt de principe relativement à la norme de contrôle applicable en droit administratif est *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65 (*Vavilov*). Dans *Vavilov*, les juges de la majorité de la Cour suprême du Canada ont clairement indiqué que, lorsqu'une cour examine une décision administrative sur le fond, la norme de contrôle présumée s'appliquer est celle de la décision raisonnable.

53. Pour décider si les conclusions de la ministre sont raisonnables, je m'appuie sur l'extrait suivant de l'arrêt *Vavilov*, au para 99 :

> [99] 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 : *Dunsmuir*, par. 47 et 74; *Catalyst*, par. 13.

54. Dans cette décision, les juges de la majorité de la Cour suprême du Canada ont également précisé qu'une décision raisonnable est fondée sur un raisonnement intrinsèquement cohérent

et qu'elle doit être justifiée à la lumière des contraintes juridiques et factuelles qui ont une incidence sur la décision.

55. Afin de mieux comprendre le rôle du commissaire au renseignement lorsqu'il effectue un contrôle quasi judiciaire, il faut se reporter aux objectifs du projet de loi C-59, la *Loi de 2017 sur la sécurité nationale*, LC 2019, c 13, et à son préambule. Ce texte a mené à l'édiction de la *Loi sur le CR* ainsi que de la *Loi sur le CST* et a apporté des modifications importantes à la *Loi sur le Service canadien du renseignement de sécurité*, LRC 1985, c C-23.

56. Je reproduis ci-dessous les extraits pertinents qui, selon moi, se rattachent directement à mon rôle de commissaire au renseignement :

> Préambule
>
> Attendu :
>
> que la protection de la sécurité nationale et de la sécurité des Canadiens est l'une des responsabilités fondamentales du gouvernement du Canada;
>
> que le gouvernement du Canada a l'obligation de s'acquitter de cette responsabilité dans le respect de la primauté du droit et d'une manière qui protège les droits et libertés des Canadiens et qui respecte la *Charte canadienne des droits et libertés*;
>
> que le gouvernement du Canada est résolu à consolider le cadre fédéral de sécurité nationale dans le but d'assurer la sécurité des Canadiens tout en préservant leurs droits et libertés;
>
> [...]
>
> que la confiance de la population envers les institutions fédérales chargées d'exercer des activités liées à la sécurité nationale ou au renseignement est tributaire du renforcement de la responsabilité et de la transparence dont doivent faire preuve ces institutions;
>
> que ces institutions fédérales doivent constamment faire preuve de vigilance pour assurer la sécurité du public;
>
> que ces institutions fédérales doivent en outre disposer de pouvoirs leur permettant de faire face aux menaces en constante évolution et exercer ces pouvoirs d'une manière qui respecte les droits et libertés des Canadiens.

57. Il est intéressant de souligner, dans ces extraits du préambule, l'équilibre important qui doit être préservé entre les intérêts en matière de sécurité nationale, d'une part, et le respect de la « primauté du droit » ainsi que des « droits et libertés des Canadiens », d'autre part. Dans le but de mettre ces objectifs en équilibre, le Parlement a confié au commissaire au renseignement le rôle de « gardien » et de surveillant des autorisations ministérielles relativement à la cybersécurité.

58. Compte tenu de ce qui précède, j'estime que je dois, afin de juger si les conclusions de la ministre sont raisonnables dans le contexte de la sécurité nationale, examiner et pondérer soigneusement les intérêts en matière de protection de la vie privée et les intérêts d'autre nature des Canadiens ou des personnes se trouvant au Canada. Par conséquent, je considère qu'il s'agit là de ma raison d'être en qualité de commissaire au renseignement du Canada.

59. À l'appui de cette position, j'aimerais citer l'*Énoncé concernant la Charte* préparé par la ministre de la Justice à l'époque du dépôt du projet de loi C-59. Mon attention s'est portée sur les extraits suivants, où les attributions du commissaire au renseignement sont décrites ainsi :

> En outre, la Partie 2 du projet de loi C-59, la *Loi sur le commissaire au renseignement*, créerait un poste indépendant et quasi judiciaire de commissaire au renseignement, chargé d'évaluer et d'examiner certaines décisions ministérielles concernant les activités en matière de collecte de renseignements et de cybersécurité. Cela assurerait un examen indépendant de la protection de la vie privée et des autres intérêts visés par ces activités d'une manière dûment adaptée au contexte délicat de la sécurité nationale.
>
> [...]
>
> Un changement clé proposé dans le projet de loi C-59 est que les activités devraient également être approuvées d'avance par le commissaire au renseignement indépendant qui, à titre de juge à la retraite d'une cour supérieure, serait habilité à agir judiciairement.

60. Je suis conscient que mon examen quasi judiciaire indépendant doit prendre en considération le caractère raisonnable des conclusions de la ministre au regard des intérêts liés à la vie privée

des Canadiens et des personnes se trouvant au Canada, compte tenu d'autres droits pertinents et importants qui entrent en jeu lorsque des activités de cybersécurité sont menées dans un contexte de sécurité nationale.

61. Examinons maintenant les conclusions de la ministre à la lumière de ce qui précède.

V. ANALYSE

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

63. À la lumière des faits présentés dans la *demande*, la ministre a conclu qu'elle 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.

64. La ministre a reconnu également que, sans l'*autorisation*, les activités autorisées au paragraphe 67 peuvent contrevenir à d'autres lois fédérales ou porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

65. En conséquence, la ministre a délivré l'*autorisation*; celle-ci comporte des conditions et des restrictions, et est valide pour une durée d'un an.

i. 34(1) – Les activités sont-elles raisonnables et proportionnelles?

66. Selon le paragraphe 34(1) de la *Loi sur le CST*, la ministre 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.

67. Pour ce qui est de l'évaluation du caractère raisonnable et proportionnel des activités, la jurisprudence du commissaire au renseignement définit ce qui est « raisonnable et proportionnel » d'après le critère de proportionnalité élaboré par la Cour suprême du Canada dans l'arrêt *R c Oakes*, [1986] 1 RCS 103.

68. Sera jugée « raisonnable » une activité qui est équitable, solide, logique et bien fondée au regard de l'objectif.

69. La notion de « proportionnalité » nécessite que l'activité ait un lien rationnel avec l'objectif, qu'elle porte le moins possible atteinte aux droits et libertés de tierces parties et qu'elle endommage le moins possible leurs équipements et infrastructures. Qui plus est, elle suppose que l'acquisition de l'information ne l'emporte pas sur l'objectif d'aider à protéger l'information électronique et les infrastructures de l'information des institutions non fédérales d'importance pour le gouvernement fédéral. De plus, des mesures visant à restreindre l'acquisition et la conservation de l'information devraient être mises en place si cela s'avère nécessaire pour atteindre l'objectif.

70. Au paragraphe 31 de l'*autorisation*, la ministre a précisé qu'elle avait des motifs raisonnables de croire ce qui suit :

> [TRADUCTION]
> Les activités visées dans la présente autorisation sont raisonnables, parce qu'elles offrent un moyen équitable, solide, logique et bien fondé d'atteindre l'objectif, soit d'aider à protéger l'information électronique et les infrastructures de l'information de [redacted] ainsi que de protéger potentiellement les systèmes fédéraux et d'autres systèmes d'importance pour le gouvernement du Canada contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

71. Après avoir examiné soigneusement les conclusions de la ministre, je suis convaincu qu'elles sont raisonnables pour ce qui est de confirmer que les activités qui y sont décrites sont effectivement raisonnables et proportionnelles compte tenu de la nature de l'objectif du CST – c'est-à-dire d'aider à protéger de l'information électronique et des infrastructures de l'information non fédérales – et de la nature de ces activités de cybersécurité.

72. Je suis parvenu à cette décision en m'appuyant sur les facteurs suivants :

i. [redacted] est un système non fédéral d'importance pour le gouvernement fédéral;

ii. [redacted]

iii. [redacted]

iv. Les activités de cybersécurité sont soumises aux mesures et contrôles décrits dans l'*autorisation*;

v. Le CST recommande la mise en œuvre de mesures par [redacted] et ne peut appliquer ces mesures qu'avec le consentement de [redacted]

vi. Les solutions de cybersécurité proposées font l'objet d'un examen destiné à vérifier leur conformité aux règles juridiques et aux politiques;

vii. D'importants mécanismes de protection ont été mis en place dans l'éventualité où de l'information acquise par le CST présenterait le risque de porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada;

viii. Toute recherche exécutée sur la base de l'information acquise est susceptible d'un audit visant à en assurer la conformité à *l'Ensemble des politiques sur la mission en matière de cybersécurité* et à d'autres politiques organisationnelles. Les journaux d'audit sont conservés et peuvent être consultés à des fins d'examen et de surveillance.

ii. 34(3) – Les conditions sont-elles remplies?

73. Comme le précise le paragraphe 34(3) de la *Loi sur le CST*, la ministre peut délivrer une autorisation de cybersécurité concernant des activités menées dans une infrastructure non fédérale seulement si elle conclut qu'il y a des motifs raisonnables de croire que les trois conditions énumérées dans ce paragraphe sont remplies.

74. Dans l'*autorisation*, la ministre a décrit ce qui suit : (1) l'information à acquérir au titre de l'*autorisation* ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire; (2) l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages à l'information électronique et aux infrastructures de l'information de [redacted] (3) les mesures prévues à l'article 24 de la *Loi sur le CST* feront en sorte que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques et aux infrastructures de l'information de [redacted]

75. Je suis convaincu que ces conditions ont été remplies.

iii. Les conclusions de la ministre sont-elles raisonnables?

76. À la lumière du dossier dans son ensemble, mon examen quasi judiciaire m'amène à conclure que les conclusions de la ministre se fondent sur un raisonnement intrinsèquement cohérent. Suivant les directives énoncées par la Cour suprême du Canada dans *Vavilov*, les conclusions sont justifiées, transparentes et intelligibles, et elles sont justifiées au regard des contraintes factuelles et juridiques pertinentes qui ont une incidence sur la décision.

77. Les conclusions de la ministre montrent également qu'elle avait des motifs raisonnables de croire, à la lumière des informations crédibles et convaincantes présentées dans la *demande* et, de façon générale, dans le dossier, que toutes les conditions énoncées aux paragraphes 34(1) et (3) de la *Loi sur le CST* pour justifier la délivrance de l'*autorisation* ont été remplies.

78. Pour les motifs exposés plus haut, je suis convaincu que les conclusions de la ministre sont raisonnables en ce qui concerne les activités de cybersécurité proposées décrites dans l'*autorisation*.

VI. REMARQUES

79. Dans ma décision antérieure portant sur une autorisation de cybersécurité liée à des activités menées dans des infrastructures non fédérales (2200-B-2022-05), j'ai formulé quatre remarques.

80. Ma première remarque concernait l'énoncé figurant dans l'*autorisation* et dans la *demande* relativement à une autre utilisation de l'information acquise en vertu de l'autorisation [redacted]

81. Ma deuxième concernait les périodes de conservation des informations acquises de [redacted] et [redacted] Ma troisième et ma quatrième remarques se rapportaient au moment où il faut aviser le commissaire au renseignement de certaines informations qui ont trait à des communications protégées par le secret professionnel de l'avocat et à une contravention à toute loi fédérale.

82. J'estime que la ministre et la chef du CST ont tenu compte de ces remarques d'une façon qui me satisfait dans l'*autorisation* et la *demande*.

83. Ceci étant dit, je voudrais formuler les deux remarques suivantes pour éclairer les demandes et autorisations futures.

i. Le temps écoulé

84. Ma première porte sur le temps qui s'est écoulé entre [redacted] ce qui s'est produit le [redacted] et le signalement de l'incident [redacted] au CST le [redacted] soit [redacted] après l'événement.

85. Le dossier n'explique pas ce délai, d'où certaines interrogations quant à l'urgence pour le CST de fournir [redacted] Par exemple, le dossier aurait pu préciser si [redacted]

86. Il aurait été préférable pour la ministre et pour moi-même de disposer d'informations plus détaillées à cet égard. Si le CST ne peut justifier ce délai de [redacted] une explication aurait dû être fournie à la ministre et reconnue par celle-ci dans ses conclusions.

ii. [redacted]

87. Ma deuxième remarque concerne [redacted]

88. Le dossier contient des informations nombreuses et utiles sur ce [redacted] Un des documents présentés par la ministre a été préparé par le Centre canadien de la cybersécurité (CCC), qui décrit [redacted] (c'est-à-dire l'annexe III). Je constate que ce document n'est pas daté. Malgré le chiffre inscrit dans la partie inférieure du document se terminant par [redacted] je ne pouvais pas savoir vraiment s'il s'agissait de la date à laquelle le document a été communiqué.

89. J'ose croire que, dans l'avenir, tous les documents versés au dossier comporteront une date.

90. De plus, j'ai remarqué que l'information contenue dans le document du CCC se rapporte à [redacted] Même si la *demande* répète une partie de cette information, elle ne précise pas [redacted]

91. Étant donné ce trou important dans le temps, des détails manquent en ce qui concerne [redacted]

92. Selon moi, une mise à jour relative à [redacted] si elle existait, aurait aidé la ministre, qui devait prendre une décision, à étayer ses conclusions à ce sujet. Par ailleurs, s'il n'y avait aucune information plus à jour, ce fait aurait dû être précisé dans le dossier.

93. Malgré leur importance, ces deux remarques ne modifient en rien mes constatations quant au caractère raisonnable des conclusions tirées par la ministre, car ces conclusions respectent les critères de transparence et d'intelligibilité.

VII. CONCLUSIONS

94. À la lumière de mon examen du dossier présenté, je suis convaincu que les conclusions de la ministre sont raisonnables en ce qui concerne les activités de cybersécurité décrites au paragraphe 67 de l'*autorisation*.

95. Par conséquent, j'approuve *l'Autorisation de cybersécurité pour des activités menées dans des infrastructures non fédérales* – [redacted] du [redacted] en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*.

96. Comme l'a précisé la ministre, et conformément au paragraphe 36(1) de la *Loi sur le CST*, l'*autorisation* est valide pour une période d'un an à compter de la date de mon approbation.

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

Le 8 décembre 2022

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