Madame la Ministre/Monsieur le Ministre,

Félicitations et bienvenue à votre nouveau poste de ministre de la Défense nationale. En tant que ministre, votre portefeuille comprend le Centre de la sécurité des télécommunications Canada (CST) qui joue un rôle important dans l'écosystème de sécurité et de défense du Canada et contribue aux investissements du Canada en matière de défense. Cette lettre vise à vous présenter brièvement le mandat du CST et vos responsabilités par rapport à nos pouvoirs. Dans mon rôle de Chef (Sous-ministre) du CST, j'attends avec intérêt notre collaboration et nos discussions visant à mettre à profit notre expertise pour aider le gouvernement du Canada à s'acquitter de ses priorités et de ses engagements.

Le CST et ses activités

Le CST est l'autorité nationale en renseignement étranger : nous recueillons du renseignement électromagnétique étranger, aussi appelé SIGINT, pour fournir en temps opportun, à vous et vos collègues du Cabinet et d'autres leaders du gouvernement, du renseignement important sur les priorités, les crises et les enjeux stratégiques émergents. Les capacités de collecte de renseignement étranger du CST sont guidées par les priorités du gouvernement du Canada en matière de renseignement, qui sont approuvées par le Cabinet. Le CST fournit du renseignement étranger sur des priorités clés, y compris la souveraineté dans l'Arctique, l'invasion de l'Ukraine par la Russie, la sécurité frontalière, la sécurité économique et du commerce, la République populaire de Chine et la stabilité de la région indo-pacifique, le terrorisme et l'extrémisme violent, et les activités d'États hostiles (par exemple, l'ingérence étrangère, les vols de propriété intellectuelle et les activités de cybermenace). De plus, le CST compte une longue histoire de collaboration avec les Forces armées canadiennes (FAC) en appuyant les missions militaires du Canada à l'étranger et en fournissant de l'information pour permettre l'atteinte des objectifs militaires et assurer la sécurité du personnel.

Le CST a également le mandat de mener des cyberopérations qui permettent de faire progresser les intérêts canadiens, notamment en relevant certains des défis les plus complexes auxquels le Canada est confronté en matière de défense nationale et de sécurité, y compris la sécurité économique. Dans votre rôle de ministre, vous supervisez les pouvoirs de cyberopérations étrangères du CST qui permettent au Canada d'agir directement pour perturber, dégrader ou influencer les réseaux de nos adversaires. Comme ces outils constituent un élément important du pouvoir militaire et étatique nécessaire pour dissuader

et contrer les menaces externes contre le Canada, vous vous acquitterez de ces fonctions en étroite consultation avec le ou la Ministre des Affaires étrangères et le ou la Commissaire au renseignement (CR). Le CST conduit souvent des cyberopérations étrangères de concert avec ses partenaires de la collectivité des cinq, en vue d'atteindre des objectifs communs. Il mène également des cyberopérations conjointes avec les FAC et ses partenaires chargés de l'application de la loi à l'appui des objectifs liés à leur mission.

Le CST comprend le Centre canadien pour la cybersécurité (Centre pour la cybersécurité), un chef de file mondial en matière de cyberdéfense et de cybersécurité. À l'aide de notre réseau de capteurs que nous avons placés dans l'ensemble des institutions fédérales, nous défendons les systèmes du gouvernement du Canada contre les attaques visant les systèmes, bases de données et sites Web fédéraux. Lorsque des cyberincidents se produisent, le Centre pour la cybersécurité offre un soutien rapide en reconnaissant que le fait de prendre les bonnes mesures rapidement peut réduire considérablement les dommages et les répercussions économiques, et accélérer le processus de reprise des activités. Lors de ses opérations, le Centre pour la cybersécurité acquiert des connaissances sur les tendances et le contexte des menaces, qu'il utilise ensuite pour fournir des avis et conseils pratiques aux entreprises et aux différents ordres de gouvernement du Canada, et pour informer les Canadiennes et Canadiens sur les mesures à prendre pour se protéger et protéger leurs réseaux. Avoir sous le même toit ce qui touche le renseignement, la cybersécurité, l'assurance de l'information, les technologies d'entreprise et toutes les fonctions de soutien à la mission permet au Centre pour la cybersécurité de collaborer avec les différentes équipes du CST pour atteindre des résultats uniques dont bénéficient les Canadiennes et Canadiens, par exemple la campagne en cours du CST contre le cybercrime.

Comme la résilience des infrastructures essentielles du Canada est vitale pour notre sécurité nationale, le mandat du Centre pour la cybersécurité touche également des systèmes importants pour le Canada. C'est pourquoi nous mettons l'accent sur le renforcement des relations de confiance avec nos partenaires des infrastructures essentielles dans tous les secteurs. La Stratégie nationale de cybersécurité lancée récemment démontre le virage du gouvernement du Canada vers un partenariat à l'échelle de la société et, comme première étape, annonce la création du Collectif canadien de cyberdéfense qui servira d'organisme de mobilisation des parties prenantes pour faire progresser la cyberrésilience du Canada au moyen d'un partenariat public-privé direct sur les défis nationaux en matière de cybersécurité, les priorités en matière de politiques et les efforts de défense. Étant donné que les cybermenaces visent de plus en plus les réseaux des infrastructures essentielles et la technologie utilisée pour exploiter des secteurs vitaux, le Centre pour la cybersécurité est bien placé pour appuyer d'autres activités visant à accroître la résilience collective du Canada en matière de cybersécurité – cela pourrait comprendre des mesures législatives sur la cybersécurité comme l'ancien projet de loi C-26, *Loi concernant la cybersécurité*, qui a été présenté mais n'a pas été adopté au cours de la dernière session parlementaire et qui aurait obligé les exploitants des secteurs de l'énergie, des finances, des télécommunications et des transports sous réglementation fédérale à signaler les cyberincidents au Centre pour la cybersécurité du CST – une pratique exemplaire déjà adoptée par certains partenaires.

La cryptographie est une partie fondamentale de la cybersécurité. Depuis presque 80 ans, le CST est l'organisme national de cryptologie, qui génère et casse des codes. À titre d'autorité nationale en matière de sécurité des télécommunications (COMSEC), le CST joue un rôle essentiel dans la protection (par le chiffrement) des renseignements et des données les plus classifiés du gouvernement du Canada, pour s'assurer que les ministères et organismes, ainsi que des partenaires de l'industrie privée qui travaillent avec le gouvernement, déploient de l'équipement dont l'utilisation est approuvée et efficace pour protéger les renseignements du Canada. Par exemple, lorsque vous utiliserez de l'équipement pour discuter avec vos collègues du Cabinet de sujets de niveau SECRET ou TRÈS SECRET, vous saurez désormais que la technologie et les normes nécessaires ont été élaborées, testées et mises en œuvre par le CST. Grâce à ses recherches et son partenariat avec la collectivité des cinq, le CST joue un rôle clé pour s'assurer que le Canada soit prêt pour l'émergence de nouvelles technologies, comme l'informatique quantique qui sera capable de déchiffrer les efforts de cryptologie moderne. Il existe des possibilités pour le Canada d'accroître sa souveraineté, d'améliorer la résilience dans l'ensemble de l'organisation du Traité de l'Atlantique Nord et de la collectivité des cinq, et de contribuer à sa propre base industrielle en investissant dans l'industrie cryptologique du Canada.

Le CST est unique, car il réunit les pouvoirs de renseignement étranger, de cybersécurité, de cyberopérations et de sécurité des télécommunications en un seul organisme. C'est ce que j'aime appeler « la recette secrète » du Canada qui nous permet de réagir rapidement et agilement en cas de menace. Nos rapports de renseignement ou sur les cybermenaces nous servent à éclairer nos cyberopérations, et vice versa, ce qui renforce les conseils que le gouvernement donne aux Canadiennes et Canadiens, à nos partenaires canadiens de l'industrie et solidifie notre posture collective de sécurité. La capacité du CST à capitaliser sur les différents aspects de notre mandat fait de l'organisme un partenaire clé par rapport à certaines priorités comme la sécurité économique et le plan relatif aux frontières du Canada dans le cadre duquel le CST travaille avec ses partenaires canadiens et américains pour perturber et atténuer le trafic du fentanyl, ainsi que le crime organisé transnational.

Selon moi, les partenariats et la collaboration sont en grande partie ce qui permet au CST et ses partenaires d'intervenir dans l'environnement dynamique de la menace avec lequel nous devons composer à l'heure actuelle. Le CST fait partie de la collectivité des cinq, un partenariat mis en place il a presque 80 ans entre le Canada, l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.

Cette alliance décuple les forces du CST et du Canada en rendant possibles les échanges de renseignement, de technologies et de connaissances afin de mieux comprendre les menaces, les risques, nos adversaires, et de renforcer nos défenses collectives. La collectivité des cinq diffuse des publications conjointes (p. ex. lignes directrices sur le développement et l'utilisation sécuritaires de l'intelligence artificielle (IA)) afin de faire résonner ces messages aux quatre coins du monde. En plus d'être membre de la collectivité des cinq, le CST entretient des relations bilatérales et multilatérales avec des alliés qui partagent nos valeurs dans le cadre de nos activités liées au SIGINT et à la cybersécurité. Par exemple, le CST participe à deux forums multinationaux de renseignement pour coordonner ses activités avec celles d'alliés partageant

les mêmes valeurs en ce qui a trait à la sécurité dans l'Arctique. L'un de ces forums, présidé par le CST, est expressément consacré au renseignement électromagnétique et s'intéresse aux deux régions polaires. L'autre forum concentre le renseignement de toutes les sources et porte exclusivement sur l'Arctique.

Le CST s'efforce d'être à la fine pointe de l'innovation et de la recherche. Le CST et le Centre pour la cybersécurité organisent plusieurs événements pendant l'année pour travailler intensément sur des problèmes liés à la mission. Ces ateliers sont des laboratoires d'innovation qui réunissent des participantes et participants de tout le Canada, de la collectivité des cinq, du milieu universitaire, de l'industrie et du secteur public. Le CST compte également ses propres chercheuses et chercheurs qui se concentrent sur la recherche fondamentale liée à la cryptographie, à la recherche de vulnérabilités et à la science des données. Nos recherches classifiées et nos partenariats de recherche nous permettent d'avoir l'expertise nécessaire pour relever les défis actuels et émergents. En tant qu'organisme axé sur les données, le CST est l'avant-garde de la science des données fondamentale qui sous-tend l'intelligence artificielle, ainsi que de l'utilisation de l'intelligence artificielle et de l'apprentissage machine pour appuyer les activités liées à sa mission. Nous travaillons en étroite collaboration avec des partenaires du gouvernement fédéral, du milieu universitaire et de l'industrie pour assurer la sécurité pratique de l'IA. Bien que le CST possède certains des ordinateurs les plus performants au pays, nous prévoyons que nos besoins en matière de calcul augmenteront de façon exponentielle tandis que nous chercherons à recueillir davantage de données et à tirer parti des technologies émergentes. À l'avenir, de nouvelles mesures seront essentielles pour renforcer les systèmes communs et interopérables qui permettent aux organismes à sécurité élevée du Canada de communiquer en toute sécurité et de collaborer pour contrer les menaces contre la souveraineté et la sécurité du Canada.

Je tiens à conclure en vous assurant que le CST exécute les différents volets de son mandat de façon responsable. Les pouvoirs du CST sont alignés sur les priorités et l'orientation du gouvernement, protègent la vie privée des Canadiennes et Canadiens et des personnes au Canada et font l'objet de contrôles, d'une surveillance et d'examens rigoureux. La loi interdit explicitement au CST de mener des activités de renseignement étranger ou de cybersécurité, ou des cyberopérations, contre des Canadiennes ou Canadiens, où qu'ils ou elles se trouvent dans le monde, ou contre des personnes se trouvant au Canada. En vertu de la loi, l'organisme est également tenu de mettre en place des mesures pour protéger la vie privée de Canadiennes et Canadiens qui pourraient accidentellement être visés par des activités du CST. Les activités du CST font l'objet d'examens indépendants de la part du CR, de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et du Comité des parlementaires sur la sécurité nationale et le renseignement. Le CST peut également faire l'objet de vérifications par la vérificatrice générale, d'examens par le Commissariat à la protection de la vie privée, de demandes d'accès à des documents en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, ainsi que d'examens par le Commissariat aux langues officielles et la Commission des droits de la personne, principalement en réponse à des plaintes.

À votre convenance, je serai heureuse de vous inviter à visiter l'édifice Edward-Drake du CST pour observer le travail exceptionnel que nous effectuons comme membre de la Défense nationale et de la collectivité de la sécurité et du renseignement. D'ici là, je vous invite, ainsi que le personnel de votre bureau, à utiliser ce code QR pour accéder à un dossier numérique constitué de documents sur le mandat et les priorités du CST, et ce, dans les deux langues officielles.

Ce code QR renvoie vers un classeur numérique (www.cse-cst.gc.ca/documents-cles) qui comprend des documents supplémentaires sur le mandat et l'aperçu du CST dans les deux langues officielles.

Nous traversons une période où le Canada est la cible d'autant de menaces d'États hostiles que pendant la guerre froide et le contexte des menaces est de plus en plus complexe avec l'ingérence étrangère, les cyberattaques, et un environnement géopolitique déstabilisé. Je serai heureuse de travailler avec vous, Madame la Ministre/Monsieur le Ministre, pour protéger le Canada et les Canadiennes et Canadiens, et pour accroître notre résilience nationale.

Veuillez agréer mes salutations distinguées,

Caroline Xavier
Chef
Centre de la sécurité des télécommunications Canada