

Discours à la mémoire de John Tait
Conférence de l'ACESR
Le 15 octobre 2004

Transformation du CST à la suite des événements du
11 septembre 2001

Merci Tony.

Je dois d'abord vous dire que c'est un honneur pour moi d'avoir été invité cette année à prononcer le discours à la mémoire de John Tait.

Comme pour la plupart des fonctionnaires de ma génération, le nom de John est pour moi synonyme d'excellence dans la fonction publique. J'ai eu la chance de le connaître, car nous avons travaillé ensemble au Bureau du Conseil privé au milieu des années 1990. Il avait une capacité intellectuelle extraordinaire et une très grande compréhension de ce pays, de son système de gouvernement fédéral et des Canadiens qui se dévouent dans la fonction publique. Sa sagesse et son leadership nous manquent beaucoup.

Après avoir été sous-ministre de la Justice, John s'est joint au Bureau du Conseil privé où, à titre de coordonnateur de la sécurité et du renseignement du gouvernement, il était le sous-ministre responsable de la politique et des opérations du CST. Dans le cadre

de ses fonctions, il a travaillé en étroite collaboration avec le CST et, de bien des façons, il a grandement contribué à préparer l'organisme pour l'avenir.

Par exemple, c'est sous la direction de John que le CST a entrepris les travaux en vue de l'analyse formelle et approfondie de son mandat, de ses pouvoirs et de sa structure stratégique – des travaux qui ont servi de base à l'élaboration des mesures législatives pour le CST à la suite des événements du onze septembre deux mille un. Et c'est aussi sous l'œil attentif de John que le CST a commencé à établir des liens professionnels importants et essentiels avec le nouveau commissaire du CST de l'époque et son bureau.

Notre cadre de valeurs constitue l'un des liens les plus forts établis entre le CST et John, et ce lien est là pour durer.

Comme plusieurs d'entre vous le savent, John a dirigé le Groupe de travail sur les valeurs et l'éthique dans la fonction publique du gouvernement fédéral, lequel a produit le rapport historique intitulé « De solides assises » en 1996.

Peu après, le CST a adopté son propre cadre de valeurs. Même si l'organisme s'était pleinement engagé à élaborer un cadre

spécifique au CST reposant sur les travaux du groupe de travail, c'est grâce au leadership et au soutien de John que nous disposons aujourd'hui d'un cadre qui fait partie intégrante de la culture organisationnelle du CST. Il va sans dire que grâce aux efforts de John, le respect de la loi est en tête de la liste des valeurs du CST, et que cette valeur est absolument essentielle à la mise en place de nouveaux pouvoirs et programmes dans le contexte qui a suivi les événements du onze septembre deux mille un.

Tout cela pour dire que John a eu une influence positive immense sur le CST, ainsi que sur la fonction publique en général. À titre de chef actuel du CST, je considère que c'est un privilège de prononcer le discours à la mémoire de John Tait.

Toutefois, avant d'accepter cette invitation, j'ai longuement réfléchi, car je me demandais si je pouvais vous transmettre assez d'information sur le CST pour que mon discours soit intéressant.

Comme vous le savez, tout au long de son histoire, qui s'étend maintenant sur presque 60 ans, le CST a en général été décrit comme étant un organisme « ultra secret » et, jusqu'à récemment, on parlait peu de cet organisme en public. En effet, comme l'a mentionné Margaret Bloodworth il y a deux ans à cette même

conférence lorsqu'elle a pris la parole en tant que sous-ministre de la Défense nationale et après que j'eus présidé un des groupes d'experts et que j'eus fait des observations préliminaires sur le CST, il aurait été impensable il n'y a pas si longtemps que le chef du CST se présente à ce genre d'événement public. Qu'il s'y présente et, qui plus est, qu'il y prononce un discours, est un signe marquant de changement fondamental!

À mes yeux, la nouvelle équation qui s'applique au CST est plutôt simple. Pour être un organisme efficace, le CST doit pouvoir compter sur la bonne structure de pouvoirs. Ce que je veux dire, c'est que pour être efficace dans le milieu actuel du renseignement, le CST doit avoir un cadre juridique et stratégique clair qui lui permette de réaliser son mandat et être doté du niveau adéquat de responsabilité.

Dans le contexte actuel, cela n'est possible que si le CST a l'appui des parlementaires et des Canadiens. Et pour obtenir cet appui, nous devons diffuser plus d'information sur le CST que par le passé. C'est la voie que nous suivons depuis trois ans, et ma participation à cette conférence est selon moi un autre pas dans cette direction.

Cela dit, je sais que vous serez d'accord avec moi pour dire qu'il existe des limites à ce que nous pouvons divulguer sur un organisme tel le CST. Règle générale, au cours des trois dernières années, nous avons divulgué beaucoup plus d'information que par le passé aux parlementaires et à d'autres Canadiens concernés sur nos activités et sur les raisons pour lesquelles nous les menons. Mais un organisme tel le CST ne peut simplement pas divulguer les méthodes qu'il utilise et les activités qu'il mène, car, si nous divulguons les moyens et les méthodes dont nous disposons, nous perdrons rapidement notre efficacité.

Puisque vous me paraissez un auditoire bien renseigné, je crois que vous comprendrez tous que je m'en tiendrai à certains paramètres lorsque je vous ferai part de mes opinions sur les changements qui doivent être apportés et qui ont été apportés au CST pour faire face aux réalités existantes depuis les événements du onze septembre deux mille un.

Il est important que vous compreniez dès le départ que la mission du CST comporte deux dimensions qui sont complémentaires – fournir et protéger l'information au moyen de techniques de pointe.

Depuis presque 60 ans, c'est ce que fait le CST en maintenant des connaissances spécialisées à la fine pointe en cryptographie, ou

codage, et en cryptanalyse, ou décodage. Ensemble, ces deux disciplines connexes se nomment la cryptologie. Donc, le CST est l'organisme national de cryptologie du Canada.

Laissons les termes ésotériques de côté. Ce que je désire vous expliquer, c'est que le CST est structuré et organisé pour à la fois recueillir et protéger les renseignements. Sur le plan offensif, notre travail consiste à utiliser l'infrastructure mondiale d'information pour recueillir des renseignements pertinents conformément aux priorités du gouvernement en matière de renseignements étrangers. Sur le plan défensif, notre travail consiste à contribuer à la protection des systèmes de communication et d'information du gouvernement, la priorité étant accordée aux systèmes les plus importants pour la sauvegarde de la sécurité nationale.

C'est pourquoi le CST compte deux secteurs d'activité : le renseignement électromagnétique étranger, ou SIGINT, et la sécurité des technologies de l'information, ou sécurité des TI.

J'aimerais commencer par la sécurité des technologies de l'information. Dans ce domaine, le mandat du CST est de « fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information ».

Notre niche se situe à la fine pointe de la technologie. Nous possédons le plus haut niveau d'expertise technique au gouvernement et au pays. Par exemple, nous fournissons les produits cryptographiques du plus haut niveau – soit les codes qui protègent les communications les plus sensibles du gouvernement, comme les communications militaires.

Nous vivons maintenant à une époque où notre sécurité et notre prospérité reposent de plus en plus sur l'échange et le stockage sécurisés de l'information. La protection efficace de l'information et des infrastructures essentielles est maintenant vitale pour la sécurité de notre pays.

Compte tenu de ces nouvelles réalités, la politique de sécurité nationale lancée en avril 2004 indique que le gouvernement fédéral s'engage à renforcer son approche à l'égard de la cybersécurité. Comme l'explique cette politique, les risques de cyberattaque sont réels, et les conséquences d'une telle attaque peuvent être importantes.

Pour mettre en place une approche plus proactive et pour que nos efforts soient en harmonie avec ceux de nos principaux alliés, le

gouvernement renforce sa capacité de prévoir et de prévenir les cyberattaques en apportant d'importantes améliorations à la qualité de ses analyses sur la menace et la vulnérabilité. Il renforce aussi sa capacité de défendre ses systèmes et de réagir lorsque surviennent des incidents et des attaques.

Le programme de sécurité des TI du CST fournira les connaissances techniques spécialisées à la fine pointe requises pour l'atteinte de ces objectifs stratégiques. Pour ce faire, nous avons récemment reçu d'importantes ressources supplémentaires à même les fonds consacrés aux questions de sécurité nationale dans le budget de 2004.

Par conséquent, le secteur d'activités de la sécurité des TI du CST est maintenant en phase de croissance et il se prépare à relever les défis de cybersécurité de l'avenir. Il s'agit d'une composante essentielle de nos objectifs organisationnels en ce moment et, selon moi, le rôle du CST est absolument essentiel, et pour la mise en œuvre efficace de la nouvelle politique de sécurité nationale et pour la sécurité à plus long terme de notre pays.

J'aimerais souligner que la majeure partie de notre infrastructure essentielle – réseaux électriques, hôpitaux, entreprises, principales

institutions économiques et ainsi de suite – dépend maintenant des capacités informatiques. Puisque le secteur privé et d'autres ordres de gouvernement détiennent la majeure partie de cette infrastructure, les incidences de ce secteur en matière de sécurité nationale ne peuvent certainement pas être traitées efficacement par le gouvernement fédéral s'il agit seul.

C'est précisément pour cette raison que, comme l'indique la politique de sécurité nationale, le gouvernement fédéral « créera un groupe de travail national de haut niveau, composé de représentants des secteurs public et privé, en vue d'élaborer une stratégie nationale de cybersécurité. Cette stratégie réduira la vulnérabilité du Canada aux cyberattaques et aux cyberaccidents ». Sécurité publique et Protection civile Canada a entrepris les préparatifs de cet exercice, et le groupe de travail entreprendra ses travaux au cours des prochains mois.

Certains de nos principaux partenaires internationaux, en particulier les États-Unis avec lesquels nous partageons une grande infrastructure commune, ont déjà réalisé des exercices nationaux de la sorte, et ils ont élaboré des stratégies nationales visant à sécuriser le cyberspace et à protéger leur propre infrastructure

essentielle. À mon avis, il est essentiel que nous prenions aussi ce genre de mesure.

Alors que nous entrons dans l'avenir du cyberspace, j'espère que les futurs événements organisés par l'Association canadienne pour l'étude de la sécurité et du renseignement (ACESR) prévoiront plus de temps pour les discussions portant sur la cybersécurité. Comme je le dis à mes collègues, cet aspect de notre sécurité nationale est beaucoup trop important pour qu'il ne soit traité que lors des conférences techniques. Un dialogue de niveau stratégique doit aussi être tenu, et je crois que l'ACESR peut apporter une contribution très importante dans ce domaine comme ce fut le cas dans de nombreux autres domaines.

J'aimerais maintenant parler du secteur d'activité SIGINT du CST et comment ce secteur a évolué depuis le onze septembre deux mille un.

Le CST a été créé peu après la Deuxième Guerre mondiale. Pendant les quarante-cinq années qui ont suivi, la culture et les capacités du SIGINT étaient axées sur la guerre froide. Nos efforts étaient dirigés principalement contre l'Union soviétique.

Cette cible était vaste, évoluait lentement et était assez prévisible. Elle avait une organisation hiérarchique bien connue, une présence diplomatique dans le monde entier et un groupe stable d'alliés et de partisans.

Le plus grand défi pendant la période de la guerre froide était la cryptographie. Les communications soviétiques délicates étaient codées à l'aide de cryptogrammes ou de codes complexes, et il était difficile d'en comprendre le contenu même avec les techniques les plus spécialisées.

Après la fin de la guerre froide, le CST a changé de voie. Dans les dix ans qui ont suivi, l'organisme a produit une gamme plus diversifiée de produits de renseignement et a offert des services à un plus grand nombre d'organisations gouvernementales.

Cette évolution qui est survenue après la guerre froide a permis au CST de maintenir des effectifs hautement spécialisés et professionnels, ainsi que les relations solides qu'il avait établies avec les principaux services de renseignement alliés de l'étranger. Toutefois, lorsque les événements du onze septembre deux mille un se sont produits, le CST s'est tout de même retrouvé devant un scénario difficile.

En termes simples, dans un tel contexte de tempête extrême, la révolution mondiale des technologies de communication ainsi que les lacunes en matière de ressources et de cadre décisionnel à jour des années 1990, se sont combinées pour produire une érosion importante des capacités du SIGINT du CST.

Laissez-moi d'abord vous expliquer comment le cadre juridique est devenu problématique pour le CST.

Plusieurs d'entre vous savent que la partie six du Code criminel protège les communications privées qu'on définit comme toute communication donnant lieu à une attente raisonnable de respect de la vie privée et qui prend sa source ou se termine au Canada. Cette disposition touchait le CST de deux façons.

La première conséquence est évidente. Le CST ne pouvait pas intercepter une communication envoyée du Canada ou reçue au Canada par une cible de renseignement étrangère. Dans le domaine du renseignement de sécurité où les communications d'un terroriste ou d'un groupe terroriste situé à l'étranger étaient ciblées, cette restriction signifiait que le CST ne pouvait pas fournir de services de renseignement même si la situation constituait une

menace considérable pour le pays, lorsqu'un groupe terroriste communiquait avec un membre ou un complice au Canada.

Par exemple, si un membre connu d'Al-Qaïda opérant à l'étranger communiquait avec quelqu'un au Canada, et même si la personne au Canada était un agent étranger d'Al-Qaïda, la partie six du Code criminel interdisait au CST d'intercepter la communication.

La deuxième conséquence est moins évidente, mais plus profonde. Dans le nouveau contexte technologique, la variété, la rapidité et le volume des communications étaient en expansion exponentielle et les communications se déplaçaient d'un endroit à l'autre d'une multitude de façons imprévisibles.

Toutefois, le CST ne pouvait intercepter une communication que lorsqu'il pouvait démontrer que cette communication ne prenait pas sa source et ne se terminait pas au Canada. En d'autres termes, le CST devait être en mesure de démontrer, avant d'acquiescer une communication, que l'origine et la destination de la communication étaient situées à l'étranger.

De plus, dans ce nouveau contexte, les communications se déplaçaient en groupes complexes qui devaient être cartographiés et analysés avant que leur acquisition ne soit possible.

Mais, d'après une analyse juridique approfondie effectuée par le ministère de la Justice, le Code criminel interdisait au CST de faire une première analyse des groupes ou des systèmes lorsqu'il y avait un risque que ceux-ci contiennent des communications d'une personne au Canada.

Le résultat est donc évident : les efforts du CST dans les nouveaux contextes des communications et de la sécurité devenaient beaucoup moins efficaces.

Je devrais souligner que nos principaux partenaires internationaux du SIGINT – les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande – avaient déjà trouvé des façons de régler ce problème afin d'assurer l'efficacité à long terme de leurs activités SIGINT tout en continuant à protéger le droit fondamental à la vie privée de leurs citoyens.

Lorsque les événements du onze septembre deux mille un sont survenus, il est devenu essentiel pour le CST de résoudre ce

problème puisque nous avons l'intention de participer pleinement à la lutte mondiale contre le terrorisme avec nos partenaires internationaux.

Au cours des années qui ont précédé les événements du onze septembre, le CST a dû faire face à un autre problème majeur : la révolution technologique progressait à une vitesse effarante.

Le mandat du CST en matière de renseignement étranger, sous la direction administrative avant les événements du onze septembre deux mille un et maintenant en vertu de la *Loi sur la défense nationale*, est « d'acquérir et d'utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement ».

On peut envisager « l'infrastructure mondiale d'information » comme étant l'ensemble du paysage des communications modernes, où les communications se déplacent sur chaque plateforme et médium possible du spectre électromagnétique pour passer d'un point à un autre.

Certains d'entre vous ont peut-être entendu ou ont peut-être même utilisé l'analogie de « l'aspirateur » pour décrire le mode de fonctionnement des organisations du SIGINT – les gens croient que nous aspirons toutes les communications. Mais ce n'est pas ainsi que les choses se passent aujourd'hui.

En réalité, nous utilisons nos ressources intellectuelles et la toute dernière technologie pour faire une chasse sélective dans la jungle pratiquement infinie des communications et sur les autoroutes électroniques, qui sont toutes en constante évolution.

En ce qui concerne ses ressources intellectuelles, le CST a toujours eu un effectif incroyablement talentueux qui adore relever des défis. Nous pouvons compter sur des informaticiens, des ingénieurs, des mathématiciens et d'autres experts techniques qui se tiennent à la fine pointe des changements technologiques. Nous pouvons aussi compter sur des analystes qui peuvent cibler des communications difficiles à capter et analyser leur signification et leurs nuances.

Notre effectif est bien informé en matière de technologie, de linguistique et de sécurité nationale. En fait, notre effectif a toujours été notre meilleur atout.

En ce qui concerne la technologie, l'efficacité du CST a toujours reposé sur sa capacité d'adaptation aux changements d'environnement grâce à la mise en application des tous derniers progrès en matière de recherche et de technologie. Puisque tout change à une vitesse effarante de nos jours, notre matériel, nos logiciels et tous nos appareils doivent continuellement être mis à niveau.

À la fin de deux mille un, alors que nous avons dû faire face aux incidences des événements du onze septembre, les ressources humaines et techniques requises pour maintenir la cadence étaient insuffisantes au CST. Notre effectif était dispersé et nous n'arrivions pas à maintenir la cadence requise par les changements technologiques. Nous avons besoin d'un investissement financier pour aller de l'avant.

Le CST avait déjà mis en évidence ses besoins financiers dans le cadre du processus budgétaire de deux mille et deux mille un. Par conséquent, la nécessité d'un investissement à long terme relativement au SIGINT était déjà reconnue.

Toutefois, la liste de priorités concurrentes était longue et, même si le CST avait reçu des fonds additionnels pour assurer l'intégrité des programmes dans le cadre du processus budgétaire des exercices 2000-2001 et 2001-2002, cela ne représentait qu'une partie des fonds requis pour maintenir sa capacité. De plus, les perspectives d'investissement à long terme étaient incertaines.

Donc, notre situation en septembre deux mille un était difficile. Nos employés avaient le talent et les compétences nécessaires pour répondre aux besoins du vingt-et-unième siècle mais ils n'étaient pas assez nombreux. Et nous n'avions pas non plus la structure des pouvoirs, ni les ressources financières nécessaires pour réagir efficacement aux événements du onze septembre.

Immédiatement après ces événements, c'était évident que ceci allait complètement transformer la politique mondiale, la politique étrangère des États-Unis et les relations du Canada avec les États-Unis. Peu de temps après, je savais aussi que le scénario de base du CST allait changer radicalement et rapidement.

En rétrospective, il est clair que rien n'aurait pu faire ressortir aussi clairement les limites des pouvoirs et des ressources du CST que les événements du onze septembre. Dans ce contexte, le

gouvernement a réagi très rapidement et a pris des mesures décisives pour que le CST puisse aller de l'avant et pour qu'il participe efficacement à la lutte mondiale contre le terrorisme.

En ce qui concerne les pouvoirs du CST, le véhicule de changement a été le projet de loi C-36, la *Loi antiterroriste*. Dans le cadre de cette initiative, la *Loi sur la défense nationale* a été modifiée de sorte à inclure des mesures législatives accordant au CST un statut juridique lui permettant d'avoir accès plus efficacement à l'infrastructure mondiale d'information dans le contexte technologique actuel, tout en établissant des limites précises visant à protéger le droit à la vie privée des Canadiens et des personnes se trouvant au Canada qui est prévu par la Charte.

En vertu de la loi, le CST ne peut cibler que les entités étrangères à l'extérieur du pays, comme c'était le cas auparavant. Mais la loi tient compte du fait que, pour acquérir efficacement des communications de cibles étrangères à l'extérieur du pays, le CST peut par accident intercepter une petite quantité de communications provenant ou à destination du Canada.

Cette loi repose sur le jugement selon lequel le droit à la vie privée d'une personne au Canada, même s'il doit être respecté

conformément à des règles très strictes, ne devrait pas automatiquement empêcher le gouvernement de recueillir des renseignements essentiels si une cible de renseignement étrangère légitime communique avec une personne au Canada.

Les mesures législatives rendent cette approche opérationnelle grâce à un mécanisme spécifique qui permet au CST d'acquérir des communications privées accessoires lorsqu'il intercepte les communications de cibles étrangères légitimes, telles que définies par le Code criminel. Ce mécanisme consiste en une autorisation par le ministre responsable du CST, le ministre de la Défense nationale.

En termes plus clairs, la loi ne permet jamais au CST de diriger ses activités vers des personnes situées à l'intérieur des limites territoriales canadiennes, incluant les douze milles extracôtiers, que ces personnes soient canadiennes ou étrangères. Elle ne permet pas non plus au CST de cibler des Canadiens à l'étranger, lesquels sont définis dans la loi comme étant des citoyens canadiens ou des résidents permanents. Mais la loi permet au CST, sous autorisation spéciale écrite du ministre, d'intercepter des communications étrangères, sachant que des communications privées peuvent aussi être incidemment acquises.

Certaines conditions principales doivent être remplies avant que le ministre n'émette une autorisation : toutes les interceptions doivent être faites sur des cibles étrangères situées à l'extérieur du Canada; la valeur des renseignements étrangers prévus doit justifier l'effort; des mesures satisfaisantes doivent être en place pour protéger la vie privée des Canadiens et pour faire en sorte que toute communication privée acquise par le CST soit utilisée ou conservée seulement si cela est essentiel pour les affaires internationales, la défense ou la sécurité.

Des mesures spécifiques ont été mises en place pour faire en sorte que le CST respecte ces conditions et pour qu'il suive des mécanismes stricts assurant la protection de la vie privée des Canadiens et des personnes se trouvant au Canada.

- Premièrement, une équipe juridique nommée par le ministère de la Justice travaille en étroite collaboration avec notre équipe de haute direction, notre groupe stratégique ainsi que nos gestionnaires et notre personnel de première ligne pour faire en sorte que nos mécanismes respectent toutes les exigences imposées par la loi.

- Deuxièmement, nous fournissons des directives complètes aux employés dans tous les secteurs pour qu'ils soient tous en mesure de respecter le cadre juridique dans leurs activités, et nous avons mis en place des processus internes, dont la surveillance active, veillant à ce que toute lacune en ce qui concerne les mécanismes ou leur mise en application soit immédiatement détectée.
- Troisièmement, le commissaire du CST examine les activités du CST, en particulier celles nécessitant une autorisation du ministre, en ayant un accès complet à notre personnel et à nos bases de données.
- Finalement, nous sommes assujettis à un examen par le commissaire à la protection de la vie privée. Nous avons d'ailleurs fait l'objet de deux examens de la sorte, l'un d'eux ayant été effectué depuis que les nouvelles mesures législatives sont en vigueur.

Les activités du CST sont axées sur le respect du cadre juridique de l'organisme pour deux raisons, la première se rapportant à nos valeurs. Au début de mon discours, je vous ai parlé de notre cadre

de valeurs. Ce cadre de valeurs comprend le respect de la loi, une valeur fortement ancrée au sein de notre effectif.

La deuxième raison pour laquelle nous tenons à respecter notre cadre juridique est pragmatique. Le CST sait que toute activité qui déborde de son cadre juridique aurait un effet dévastateur sur la confiance que nous témoignent notre ministre, le Parlement du Canada et les Canadiens, une confiance qui est essentielle à notre efficacité.

Outre ces modifications à sa structure décisionnelle, le CST a reçu d'importantes ressources pour le SIGINT afin d'améliorer son efficacité dans le contexte technologique actuel et de mener les nouvelles activités de sécurité requises.

Dans la première vague d'investissement qui a suivi les événements du onze septembre deux mille un, nous avons bénéficié d'un investissement important en cours d'exercice dans les secteurs de la technologie et autres dans le budget de décembre deux mille un. Cet investissement devait nous permettre de bâtir des capacités à plus long terme et il faisait partie d'un ensemble plus vaste d'initiatives et d'investissements visant à renforcer le milieu de la sécurité et du renseignement.

Au cours des deux années suivantes, alors que nous renforçons notre capacité de fournir des services de renseignement pouvant contribuer à la sécurité nationale du Canada, y compris des services de renseignement sur les organisations terroristes et sur la prolifération des armes de destruction massive, nous avons acquis une compréhension beaucoup plus grande de ce que nous devons faire pour être efficaces.

Par conséquent, nous avons pu présenter des propositions spécifiques comprenant des analyses de ressources détaillées en vue du budget de deux mille quatre et de l'élaboration de la politique de sécurité nationale.

Conformément aux engagements pris dans cette politique, selon lesquels nous devons renforcer nos activités de renseignement et accorder une plus grande importance au renseignement de sécurité, le CST a récemment bénéficié d'une deuxième vague d'investissement pour le SIGINT, des fonds qui avaient été prévus dans le budget de deux mille quatre pour régler certains problèmes en matière de sécurité. Le secteur d'activités SIGINT du CST, tout comme le secteur d'activités de la sécurité des TI, est donc toujours en croissance et en préparation en vue de l'avenir.

Certes, les nouveaux investissements consacrés au SIGINT et à la Sécurité des TI doivent être gérés efficacement pour que le CST puisse obtenir la plus grande valeur possible pour l'argent versé et pour qu'il soit le plus efficace possible. À cette fin, nous avons mis en place tous les piliers du programme de modernisation de la fonction de contrôleur du gouvernement, y compris les processus financiers, la mesure du rendement et la gestion des risques.

Afin de mettre en place avec succès le nouveau programme de sécurité nationale, il est essentiel de continuer à renforcer nos liens avec nos partenaires clés, tant au Canada qu'à l'étranger. Mais ce n'est pas toujours facile parce que chaque organisation a sa propre histoire, culture et problèmes. Cela dit, à mon avis, le contexte actuel exige une coopération parfaite.

Au cours des deux dernières années, le CST a mené des efforts importants en vue d'améliorer ses relations de partenariat avec les Forces canadiennes et le SCRS. Le CST et certains éléments des Forces canadiennes collaborent efficacement depuis quelques décennies mais, au cours de la dernière année, nous avons établi un nouveau modèle opérationnel pour intensifier l'intégration de

toutes les activités du SIGINT sous la gestion et la direction du CST.

La mise en place de ce modèle a été entreprise et ce dernier permettra au CST de mieux appuyer les activités des Forces canadiennes sur le terrain et de mettre à contribution les capacités des Forces canadiennes à des fins nationales.

Le CST a aussi collaboré plus étroitement avec le SCRS depuis les événements du onze septembre deux mille un. Nous avons maintenant une meilleure vision partagée de la lutte au terrorisme et d'autres défis en matière de sécurité, et nous collaborons plus étroitement à différents niveaux. Je crois que cette relation continuera de se renforcer au cours des années à venir alors que nos deux organisations continueront de mettre en place une culture de collaboration améliorée au sein de laquelle la formation d'équipes poursuivant des objectifs communs sera la stratégie par défaut.

De façon plus générale, le CST travaille en collaboration plus étroite avec certains autres ministères et organismes du gouvernement pour appuyer les priorités en matière de sécurité nationale, notamment le Bureau du Conseil privé, les Affaires

étrangères et le nouveau ministère de la Sécurité publique et de la Protection civile.

Sur la scène internationale, le CST entretient depuis des dizaines d'années des rapports opérationnels très étroits avec ses homologues des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande.

Nous partageons du renseignement, mais aussi les technologies et les connaissances spécialisées qui servent à recueillir, à traiter et à analyser des communications étrangères pour obtenir du renseignement. Nous échangeons aussi du personnel et nous participons à des opérations conjointes qui reposent sur nos efforts collectifs.

Nous devons accorder une importance particulière à nos relations avec notre organisme homologue américain, la National Security Agency ou NSA. Cette coopération est étroite et productive à tous les niveaux.

Le CST et la NSA partagent des renseignements, s'attaquent à des problèmes communs découlant des changements technologiques et surveillent les menaces à la sécurité des deux pays. Ce partenariat

fournit au Canada un accès de très grande valeur aux technologies et aux renseignements américains.

Même si le CST est de loin le plus petit des deux partenaires, les deux pays tirent profit de cette relation. En effet, en ce moment même, le partage de certains renseignements uniques au CST représente un élément important de la contribution du Canada à la lutte mondiale contre le terrorisme.

Finalement, j'aimerais faire quelques commentaires sur une autre relation qui a une importance cruciale pour le CST : notre relation avec le commissaire du CST. Le très honorable Antonio Lamer, ancien juge en chef de la Cour suprême du Canada, a été nommé deuxième commissaire du CST en juin deux mille trois.

En vertu de la *Loi sur la défense nationale*, le mandat du commissaire consiste à examiner les activités du CST pour s'assurer de leur conformité aux lois, à informer le ministre de la Défense nationale et le procureur général de toute activité qu'il croit non conforme aux lois et, en réponse aux plaintes, à mener toute enquête qu'il considère nécessaire.

Le commissaire présente des rapports annuels sur ses activités et ses constatations au ministre de la Défense nationale qui, à son tour, dépose ce rapport au Parlement. À ce jour, le commissaire a produit huit rapports publics dans lesquels il expliquait que les activités du CST qu'il avait examinées pendant l'année étaient conformes aux lois et n'étaient pas dirigées vers des Canadiens ou des personnes se trouvant au Canada.

Outre ses rapports publics, le commissaire du CST présente aussi des rapports protégés au ministre sur une variété de sujets choisis par le commissaire. À ce jour, environ trente de ces rapports, portant sur les activités du SIGINT et de la sécurité des TI, ont été présentés et étaient tous fondés sur des analyses détaillées des programmes et activités du CST. Une fois de plus, aucun de ces rapports ne fait mention de comportements non conformes aux lois de la part du CST.

La relation hautement professionnelle qui a été établie entre le CST et le bureau du Commissaire facilite cet examen indépendant.

Légalement, le commissaire a un accès total à l'information, aux documents et aux bases de données dont il a besoin pour effectuer des examens complets des activités du CST. Afin d'appuyer les efforts du commissaire et de son personnel, le CST leur fournit des

comptes rendus détaillés et met son personnel à leur disposition afin de répondre à leurs questions.

Au fil des ans, le personnel du commissaire a acquis une compréhension approfondie du mandat et des activités du CST. Lorsque le commissaire présente son rapport au ministre, il le fait en se fondant sur une base solide d'information se rapportant aux activités et aux méthodes du CST.

Une fois de plus, j'aimerais souligner que les résultats de tous les examens du commissaire ont une importance essentielle puisque, pour être efficace, le CST doit avoir la confiance du ministre de la Défense nationale, du Parlement et des Canadiens. Par conséquent, le CST se soucie tous les jours de mener ses activités en respectant les paramètres établis.

Bien sûr, le Comité parlementaire chargé de la sécurité nationale aura les mêmes préoccupations lorsqu'il sera formé. Depuis les événements du onze septembre deux mille un, le CST s'est présenté devant plusieurs comités parlementaires et il en a reçu deux dans ses locaux. Il est évident qu'un dialogue plus approfondi avec les parlementaires sera possible lorsque le nouveau comité

sera formé et qu'il pourra traiter des renseignements de nature hautement délicate.

Le CST est enthousiaste à l'idée de travailler avec ce nouveau comité, et je crois que cette collaboration permettra aux parlementaires et aux Canadiens d'être rassurés sur la nature adéquate des activités du CST.

En tenant compte de toutes ces initiatives, je crois que nous pouvons affirmer à juste titre que le CST a été très occupé au cours des trois dernières années et qu'il l'est toujours. Une pression plus forte que jamais s'exerce sur notre organisme pour qu'il fournisse des produits et services de SIGINT et de sécurité des TI. Nous fournissons donc de tels produits et services tout en poursuivant notre croissance et tout en apportant les changements requis à notre organisme. On nous a attribué de plus grandes ressources et on s'attend à plus de nous. De plus, nous occupons une place centrale importante en ce qui concerne la mise en œuvre de la politique de sécurité nationale du gouvernement.

Même si certaines étapes de ce défi de taille et une grande partie de notre transformation demeurent à accomplir, je dois dire que je suis fier des initiatives prises par mon organisme depuis les trois

dernières années, soit depuis le onze septembre deux mille un – le personnel du SIGINT, le personnel de la Sécurité des TI et le personnel d'appui. Je me suis joint au CST seulement cinq semaines avant les événements du onze septembre deux mille un, et c'est un privilège pour moi de diriger un groupe de Canadiens aussi doués, des Canadiens qui bâtissent les capacités opérationnelles et la force organisationnelle dont aura besoin le Canada pour relever les défis qui se présenteront à lui en matière de sécurité nationale.

Je vous remercie de m'avoir invité à vous adresser la parole aujourd'hui et je vous souhaite une très belle conférence. Merci.