



Gouvernement
du Canada

Government
of Canada

[Canada.ca](#) > [Centre de la sécurité des télécommunications Canada](#) > [Reddition de comptes](#)

> [Transparence](#) > [Rapports](#)

Rapport annuel du Centre de la sécurité des télécommunications 2020-2021

De : [Centre de la sécurité des télécommunications Canada](#)



ISSN 2564-0488

► [Table des matières](#)

Avant-propos du ministre

Le Centre de la sécurité des télécommunications (CST) n'est peut-être pas le premier organisme qui nous vient à l'esprit lorsqu'on parle d'une urgence sanitaire mondiale, mais l'adoption du mode virtuel dû à la COVID-

19 a placé le renseignement étranger, la cybersécurité et l'assurance de l'information au cœur de l'intervention du Canada contre la pandémie.

Pour le CST, et pour le reste du Canada, 2020 et 2021 ont été une période de défis sans précédent et de réussites durement atteintes. Le travail du CST a été une partie essentielle de l'approche

pangouvernementale du Canada, notamment en aidant à sécuriser les

activités en ligne du gouvernement, en fournissant des informations vitales aux preneurs de décisions et en défendant la distribution des vaccins contre les cybermenaces.

En outre, le CST a été au premier plan de la protection des personnes et des organismes canadiens contre les auteurs de menaces cherchant à tirer profit de la pandémie en extorquant de l'argent, en diffusant de la désinformation, en volant des données personnelles ou en dérobant de la propriété intellectuelle.

Ce rapport propose un aperçu de la portée et de l'importance des contributions du CST.



En tant que ministre de la Défense nationale, je félicite le CST de son leadership technique et de ses innovations, de sa souplesse opérationnelle et de son travail acharné au cours des douze derniers mois. Les Canadiens sont plus en sécurité grâce à vos efforts.

- L'honorable Harjit S. Sajjan, ministre de la Défense nationale

Un CST intégré : Message de la chef

J'ai commencé ma carrière au CST il y a 32 ans et j'ai rapidement appris que dans le domaine de la sécurité et du renseignement, les organismes comme le CST ne donnent pas de rappels. Nous sommes habitués de promouvoir et de défendre les intérêts du Canada depuis les coulisses.

Mais les choses ont changé. La cybersécurité fait de plus en plus partie intégrante de la vie des Canadiens. Les nouvelles technologies changent le monde dans lequel nous vivons. De nouveaux adversaires étrangers voient le jour et nos vieux adversaires évoluent. Les Canadiens exigent, comme il se doit, plus de transparence



que jamais de la part des institutions de leur gouvernement. C'est pourquoi le CST apprend à lever un peu plus le rideau sur ses activités et même, parfois, à prendre place sur l'avant-scène.

Depuis le début de la pandémie de COVID-19, il y a un an, la mission du CST a joué un rôle essentiel de nombreuses façons que nous n'avions jamais imaginées et notre collectivité s'est sans cesse dépassée pour atteindre d'importants résultats pour le Canada.

Le présent rapport annuel vous permettra de découvrir certaines de ces contributions.

L'intervention contre la COVID-19

Au début de 2020, nous avons rédigé notre vision stratégique des cinq prochaines années : CST 2025. Au centre de cette vision se trouve le principe d'**un CST intégré** : « Le CST intègre efficacement tous les aspects de son mandat en tant que leader national en cybersécurité. »

Lorsque la pandémie a été déclarée, le CST 2025 a été notre boussole dans ce territoire inconnu. Dans l'esprit d'un CST intégré, nous avons travaillé comme une collectivité unie en vue d'exécuter les différents aspects de notre mandat – cybersécurité, assurance de l'information, renseignement électromagnétique étranger – pour appuyer l'intervention du gouvernement.

Nous avons identifié, bloqué et atténué de nouvelles cybermenaces dirigées contre le gouvernement, le secteur de la santé et d'autres systèmes essentiels du Canada, dont le plan de distribution des vaccins.

Nous avons fourni du renseignement étranger hautement exploitable à nos clients du gouvernement.

Nous avons joué un rôle essentiel dans la sécurité des activités en ligne du Cabinet, du Parlement et du gouvernement.

Nous avons atténué de graves risques envers la cybersécurité en alertant les Canadiens et les entreprises canadiennes, en leur fournissant des avis et conseils et en faisant la promotion des pratiques exemplaires en cybersécurité.

Nous avons trouvé de nouveaux moyens innovants d'acheminer du renseignement à nos clients du gouvernement qui se trouvent loin de nous.

Nous avons aidé le gouvernement à accélérer et à sécuriser sa transition vers le nuage et à renforcer la sécurité des services offerts en ligne aux Canadiens.

Nous avons fourni une assistance technique de pointe et avons mis à l'essai les solutions proposées.

Et tout cela s'est déroulé en plus des activités habituelles du CST, en comptant seulement une fraction de notre effectif dans nos installations sécurisées.

Jour après jour, j'ai été impressionnée par les prouesses techniques, la souplesse opérationnelle et l'état d'esprit positif avec lesquels les employés du CST s'attaquaient aux nouveaux problèmes inédits causés par la pandémie, ce fut une grande leçon d'humilité. J'espère que le présent rapport donnera aux Canadiens une idée de la portée et de l'importance des réalisations du CST qui méritent amplement d'être célébrées.

Iniquités systémiques

Tandis que nous faisons le bilan de la dernière année, il est important de noter que la COVID-19 a révélé des inégalités de longue date dans la société et les institutions canadiennes, dont le CST fait partie.

Dans ce contexte, **Un CST intégré** revêt un nouveau sens, c'est-à-dire un milieu de travail où tout le monde fait partie d'un tout, où il n'y a pas d'obstacles à la participation et où les expériences et les points de vue de nos preneurs de décisions sont le reflet précis de la diversité du pays que nous servons. Nous prenons cette initiative non seulement parce que c'est la bonne chose à faire (il va sans dire), mais aussi parce que cette approche nous aidera à exécuter plus efficacement notre mission envers les Canadiens. Les différents points de vue, compétences, talents et expériences des équipes multidisciplinaires sont le meilleur moyen, et parfois le seul, de résoudre des problèmes épineux. C'est le principe central de notre succès depuis trois quarts de siècle.

Puisque le CST considère la diversité comme un impératif opérationnel, nous en avons fait une priorité depuis les dix dernières années. Mais je suis la première à admettre que les changements ne se font pas assez rapidement et que nous devons en faire plus. Les événements de la dernière année nous rappellent sombrement que le progrès n'est jamais garanti. Les iniquités systémiques ne se résolvent pas d'elles-mêmes.

C'est pourquoi, conformément à [l'appel à l'action en faveur de la lutte contre le racisme](#) du greffier du Conseil privé, les employés et la direction du CST ont entamé l'année 2021 en étant déterminés à écouter, à apprendre et à agir, tout d'abord en examinant attentivement nos politiques et nos pratiques. Il faudra des efforts concertés pour éliminer les obstacles qui touchent les groupes sous-représentés et pour veiller à ce que tout le monde ait des chances égales là où ce n'est pas encore le cas.

J'ai bon espoir pour l'avenir, car je sais comment les employés, gestionnaires et cadres supérieurs du CST s'attaquent aux défis en utilisant leurs grandes capacités de résolution de problèmes.

Donc, lorsque je pense aux événements des douze derniers mois, est-ce que j'ai hâte que cette pandémie soit enfin derrière nous? Oui, mille fois oui.

Et en même temps, j'ai hâte de mettre en œuvre les leçons que nous aurons apprises pour façonner le CST de demain.

Suis-je fière de ce que nous avons accompli pour le Canada au cours de la dernière année, à titre d'organisme, de collectivité et de **CST intégré**?

« Fière » n'est pas assez fort pour exprimer ce que je ressens.

Shelly Bruce

Chef du CST

À propos de ce rapport



Le Centre de la sécurité des télécommunications (CST) est l'organisme canadien responsable du renseignement électromagnétique étranger et l'autorité nationale technique en matière de cybersécurité et d'assurance de l'information.

Le Centre canadien pour la cybersécurité (ou Centre pour la cybersécurité), qui fait partie du CST, a été mis sur pied en 2018 et réunit en un seul lieu de l'expertise en cybersécurité provenant de l'ensemble du gouvernement

fédéral. Il est l'autorité opérationnelle en matière de cybersécurité.

Le présent rapport est non classifié. Il ne contient pas de détails sur les activités liées à nos opérations de renseignement électromagnétique étranger ou à nos cyberopérations à l'étranger, car nos adversaires ne doivent pas connaître ce que nous connaissons pour que ces opérations soient efficaces. Toutefois, ce rapport présente des exemples qui démontrent comment nos activités ont été bénéfiques pour le Canada au cours de la dernière année. Nous pouvons présenter plus en détail les activités publiques du Centre pour la cybersécurité du CST.

À l'exception de la partie intitulée « Appuyer le Canada dans la gestion de la pandémie de COVID-19 », les différentes parties du présent rapport ont pour titre les thèmes de notre cadre stratégique quinquennal, CST 2025.

Ce rapport vise à illustrer comment nos activités de la dernière année ont concrétisé cette stratégie.

Le rapport couvre la période du 1er avril 2020 au 31 mars 2021. Sauf indication contraire, les statistiques et références de « cette année » correspondent à l'année financière.



► Description longue - Cadre stratégique quinquennal du CST : CST 2025

Appuyer le Canada dans la gestion de la

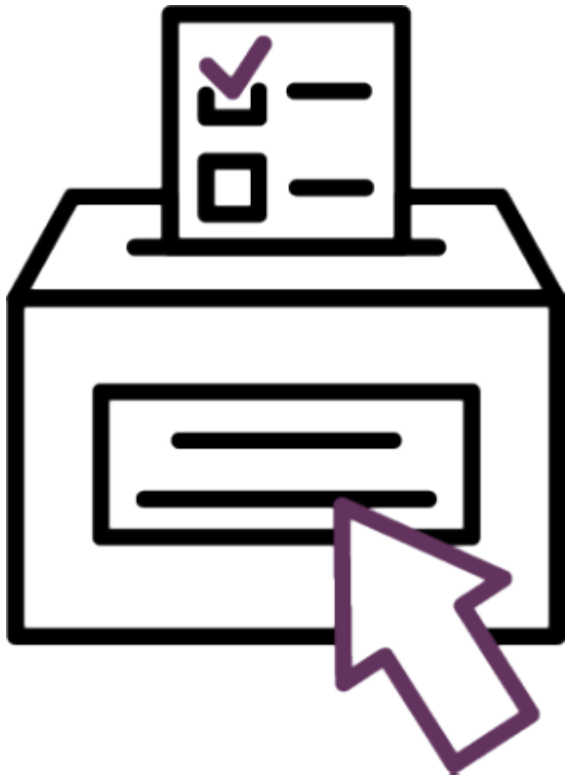
pandémie de COVID-19



Comme la distanciation physique était de rigueur en raison de la COVID-19, le Canada comptait plus que jamais sur les communications sécurisées, la cybersécurité et la collecte opportune de renseignement étranger pour gérer la pandémie. Les équipes du CST ont créé de nouveaux outils, offert de nouveaux services et tissé de nouveaux partenariats afin de protéger les opérations du gouvernement, la population canadienne, le secteur de la santé et la campagne de vaccination contre les cybermenaces.

Protéger le gouvernement et rendre possible son intervention

Dès le début de la pandémie, les solutions de communications protégées du Centre pour la cybersécurité ont permis aux membres du Cabinet de préparer l'intervention du gouvernement fédéral sans avoir à se rencontrer en personne. Les ministres et les hauts dirigeants pouvaient échanger des communications classifiées à partir d'appareils mobiles accessibles sur le marché. Le Centre pour la cybersécurité s'est aussi associé à Services partagés Canada et au Bureau du Conseil privé pour concevoir et mettre en place un service de vidéoconférence classifiée à l'intention des ministres et des hauts dirigeants. Le service est utilisé depuis février 2021.



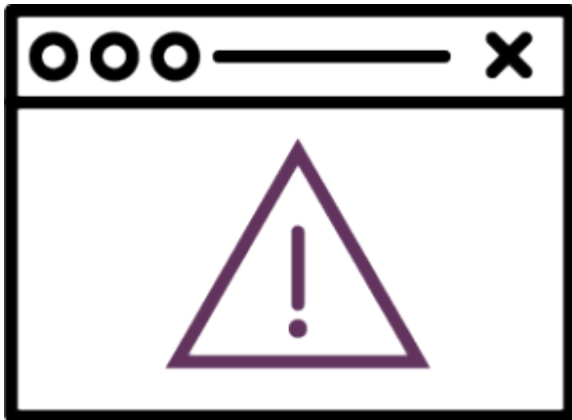
En avril 2020, le Centre pour la cybersécurité a aidé la Chambre des communes à instaurer un système de vidéoconférence pour que les travaux parlementaires puissent aller de l'avant. Enfin, en mars 2021, les parlementaires canadiens ont voté pour la première fois au moyen d'une application de vote électronique sécurisé mise au point par la Chambre des communes avec l'appui technique du Centre pour la cybersécurité. L'application confirme l'identité des parlementaires en recourant à la technologie de la reconnaissance faciale et à l'authentification multifacteur.

Comme les ministères et organismes du gouvernement du Canada ont adopté rapidement l'infonuagique, nous leur avons transmis des pratiques exemplaires pour accélérer la transition et avons déployé des outils novateurs pour assurer la sécurité de leurs réseaux. Par exemple, le Centre pour la cybersécurité a déployé des capteurs au niveau du

nuage pour plus de 50 ministères (dont 39 au cours de l'exercice en cours) pour aider à détecter les cyberactivités malveillantes sur l'infrastructure nuagique.

Des spécialistes du CST ont aussi soumis l'application Alerte COVID (alerte d'exposition) à des évaluations des vulnérabilités et à des tests de résistance pour s'assurer qu'elle répondait aux normes strictes en matière de protection de la vie privée et de sécurité auxquelles la population canadienne est en droit de s'attendre.

Protéger la population canadienne



Lorsqu'une crise sévit, les auteurs de cybermenace sont toujours là pour en profiter. Rapidement, ils ont utilisé des appâts d'hameçonnage et des sites Web frauduleux liés à la COVID-19 pour tenter de duper des Canadiens et Canadiennes. Les sites Web et adresses de courriel appartenant à l'Agence de la santé publique du Canada, à l'Agence des services frontaliers du Canada et à l'Agence du revenu du Canada, de même que les domaines liés à la Prestation canadienne d'urgence (PCU), figurent parmi les plus fréquemment usurpés. Du tout début de la pandémie jusqu'à la fin de mars 2021, le CST a collaboré avec des partenaires commerciaux et étrangers de confiance pour retirer plus de 7 000 de ces domaines frauduleux.

Protéger le secteur de la santé du Canada



Dans la semaine qui a suivi l'arrêt des activités à l'échelle nationale en mars 2020, le Centre pour la cybersécurité a lancé une alerte au secteur de la santé du Canada pour l'informer qu'il était exposé à un risque élevé en raison des cybercriminels qui voulaient soutirer des rançons et des groupes parrainés par des États qui cherchaient à voler des résultats de recherche sur la COVID-19 et des données sensibles. Le Centre pour la cybersécurité avait vu juste et de tels événements se sont produits. Par la suite, en mai 2020, il a publié des conseils à l'intention des organismes de recherche et de développement durant la pandémie de COVID-19.

Au cours de la dernière année, le Centre pour la cybersécurité a conclu des partenariats avec plus de 100 organismes du secteur de la santé, dont des autorités de santé régionales relevant d'une province ou d'un territoire, des établissements de soins aux patients ainsi que des organisations prenant part au développement, à la fabrication et à la distribution des vaccins contre la COVID-19.

Le Centre pour la cybersécurité a émis plus de 20 alertes de cybersécurité à l'intention des partenaires du secteur de la santé et offert du soutien d'intervention dans plus de 85 incidents ayant touchés le secteur.

Tout au long de 2020, le Centre pour la cybersécurité a tenu chaque semaine des appels vidéos avec plus de 100 représentants du secteur de la santé pour leur prodiguer des conseils pratiques et répondre à leurs questions sur les cybermenaces. En 2021, les appels avaient lieu toutes les deux semaines.

Protéger les efforts de vaccination



Plus un événement est important, plus il devient une cible attrayante pour les auteurs de cyberattaque qui cherchent à extorquer des rançons ou à causer de la perturbation. La campagne de vaccination contre la COVID 19 au Canada est justement une telle cible.

Depuis janvier 2021, le Centre pour la cybersécurité collabore avec le Centre national des opérations de l'Agence de la santé publique du Canada pour renforcer la cybersécurité des fournisseurs de vaccin, des entrepôts, des hôpitaux et des sites de vaccination partout au Canada.

Nous avons entre autres :

- renforcé la sécurité du périmètre réseau et le contrôle des accès;
- appliqué des mises à jour et des correctifs aux dispositifs connectés à Internet pour en optimiser la sécurité;
- assuré la protection des données sur la vaccination stockées;
- sensibilisé le personnel aux cybermenaces.

En mars 2021, le Carrefour de l'apprentissage du Centre pour la cybersécurité s'est associé à la Police provinciale de l'Ontario pour concevoir et offrir un cours de sensibilisation aux cybermenaces liées à la COVID-19 destiné au personnel des soins de santé, au personnel technique et aux cadres qui participent à la campagne de vaccination contre la COVID-19.

Les personnes intéressées peuvent assister à la séance de formation offerte en direct chaque semaine ou demander à suivre la version préenregistrée en avril 2021, toutes les deux données par des instructeurs et instructrices du Centre pour la cybersécurité et de la Police provinciale de l'Ontario. L'Agence de la santé publique du Canada a partagé le cours sur son réseau avec les 300 sites de vaccination au Canada.

Communiquer de l'information vitale

Tout au long de la pandémie, le CST a profité du volet de son mandat touchant le renseignement électromagnétique étranger (SIGINT) pour soutenir le gouvernement fédéral et orienter la gestion de la pandémie en offrant aux décideurs de l'information vitale sur l'état de préparation et les réactions d'autres pays.

Après avoir remarqué que le secteur de la santé du Canada était la cible d'activités étrangères de cybermenace, des analystes du SIGINT ont signalé ces activités aux équipes de cyberdéfense pour qu'elles prennent les mesures adéquates pour les bloquer.

Le CST a repéré des activités étrangères de cyberespionnage qui visaient la recherche sur les vaccins contre la COVID-19 et a collaboré avec ses alliés pour attribuer publiquement ces activités à leurs auteurs.

L'équipe du SIGINT du CST a aussi décelé des campagnes étrangères de désinformation dont le but était de miner la crédibilité des consignes de santé publique du Canada ainsi que l'innocuité et l'efficacité des vaccins contre la COVID-19. En signalant ces campagnes à ses clients gouvernementaux, comme à l'Agence de la santé publique du Canada, le CST, par l'entremise de ses rapports classifiés, contribue aux efforts de sensibilisation publique visant à contrer la diffusion d'information fautive et nuisible.

Pendant la période visée, le CST a modifié sa façon de présenter ses rapports de renseignement de sorte que l'information cruciale sur la pandémie soit plus opportune et intelligible. Il a aussi changé sa méthode de diffusion pour pouvoir envoyer en toute sécurité du renseignement pertinent à un plus grand bassin de clients gouvernementaux, dont certains travaillent à distance.

Leadership en matière de cyberopérations



Le CST est le responsable opérationnel de la cybersécurité au sein du gouvernement du Canada. Bien qu'une bonne partie des efforts déployés cette année appuyaient la gestion de la pandémie, on a continué et même intensifié le travail habituel de défense du Canada et de ses intérêts.

Protéger le .gc.ca



Remerciement pour les HBS de la part d'un partenaire britannique :

« Nous voulons profiter de l'occasion pour remercier le Centre canadien pour la cybersécurité de nous avoir donné aide et soutien pour nous permettre d'en arriver là. Le NCSC n'aurait pas pu à lui seul surmonter cette difficulté.

Les leçons que nous avons tirées de la protection des dispositifs d'extrémité nous ont aidés à défendre notre secteur de la santé pendant la crise de la COVID.»

- le National Cyber Security Centre du Royaume-Uni

Le CST est chargé de protéger les réseaux, les systèmes et les bases de données du gouvernement du Canada contre les cybermenaces. Sa capacité de défense dynamique de calibre mondial bloque régulièrement entre 2 et 7 milliards d'actions malveillantes chaque jour, contribuant ainsi à protéger les renseignements personnels des Canadiens et des Canadiennes ainsi que les services sur lesquels ils comptent. Par une journée particulièrement occupée, le CST peut bloquer près de 10 milliards d'actions.

En novembre 2020, le CST a révélé une partie du secret derrière sa capacité de défense : les capteurs au niveau de l'hôte (HBS). Mis au point à l'interne pendant plusieurs années par les spécialistes du CST, les HBS sont

maintenant installés sur plus de 700 000 points d'extrémité du gouvernement du Canada (comme des ordinateurs portables ou de bureau et des serveurs) où ils détectent et neutralisent automatiquement les activités malveillantes, par exemple un maliciel qui tente un téléchargement. Chaque capteur collecte les données des systèmes de façon sécuritaire tout en respectant la vie privée de ceux qui utilisent le service.

Les HBS sont à la fine pointe de la technologie et nous en sommes fiers. En novembre 2020, nos homologues britanniques du National Cyber Security Centre (NCSC) ont officiellement remercié le Centre pour la cybersécurité (anglais seulement) de leur avoir permis d'utiliser la technologie des HBS, affirmant que celle-ci avait « transformé leur capacité de détecter les menaces et de défendre le gouvernement du Royaume Uni dans le cyberspace ».

Protéger les infrastructures essentielles



Le Centre pour la cybersécurité du CST entretient des partenariats stratégiques avec les propriétaires et les opérateurs des infrastructures essentielles du Canada afin d'échanger des connaissances et de développer ensemble de nouvelles solutions de cybersécurité.

En 2020-2021, le Centre pour la cybersécurité a noué de nouveaux partenariats dans 16 secteurs des infrastructures essentielles :

- santé
- sécurité
- alimentation
- eau
- énergie
- transport
- finance
- secteur manufacturier
- technologies de l'information et de la communication (TIC)
- milieu universitaire
- secteur de l'innovation
- gouvernement fédéral
- gouvernements provinciaux et territoriaux et administrations municipales
- institutions démocratiques
- petites et moyennes entreprises
- citoyens canadiens

Ces partenariats sont cruciaux, car comme l'indique notre Évaluation des cybermenaces nationales 2020, les infrastructures essentielles du Canada continueront presque assurément d'être la cible d'activités de cybermenace menées par des entités criminelles ou parrainées par un État.

Une bonne partie des données que nous communiquons sont générées par les HBS (voir ci-dessus) en fonction des menaces qui visent les systèmes du gouvernement du Canada. Un de nos objectifs est de finir par mettre au point une version des HBS qui pourrait être déployée sur les réseaux des principaux partenaires stratégiques afin de protéger les infrastructures essentielles sur lesquelles comptent les Canadiens et les Canadiennes.

Intervenir en cas d'incident

Le Centre pour la cybersécurité du CST est le responsable opérationnel du gouvernement fédéral lors d'événements de cybersécurité, comme les compromissions de SolarWinds et de Microsoft Exchange ainsi que de milliers d'autres incidents qui n'ont jamais fait la une des journaux. Nos équipes travaillent en permanence pour repérer les compromissions et informer les éventuelles victimes au sein du gouvernement fédéral et des infrastructures essentielles du Canada. À la suite d'un cyberincident, l'équipe d'intervention en cas d'incident offre des conseils et de l'assistance pour contenir la menace et atténuer les dommages.

En 2020-2021, le Centre pour la cybersécurité est intervenu dans **2206** incidents de cybersécurité touchant le gouvernement du Canada ou des partenaires des infrastructures essentielles. Ce nombre représente une moyenne de six incidents par jour.

Contrer les menaces étrangères

En 2019, la *Loi sur le CST* accordait au CST de nouveaux pouvoirs de mener des cyberopérations étrangères (tant actives que défensives), autrement dit, elle l'autorise à se livrer à des activités en ligne pour contrer les menaces étrangères qui pèsent sur le Canada.

Au cours de la dernière année, le CST a été autorisé à mener des opérations dans le but de contrer des adversaires de l'étranger dans le cyberspace. Ces opérations en ligne ont contribué à la défense des intérêts du Canada et à la protection de sa population. Elles visent également à dissuader les auteurs de menace de s'en prendre au Canada en modifiant le taux coûts-avantages de toute attaque future.

Les cyberopérations lancées par le Canada respectent la législation du pays ainsi que les normes de comportement responsable des États dans le cyberspace. Par exemple, selon la Loi sur le CST les cyberopérations ne peuvent **pas** :

- cibler des Canadiens ou des personnes se trouvant au Canada;
- contrecarrer le cours de la justice;
- contrecarrer le cours de la démocratie;
- causer, intentionnellement ou par négligence criminelle, des lésions corporelles à une personne physique ou la mort de celle-ci.

Toutes nos activités, y compris nos cyberopérations, sont assujetties à une supervision interne stricte et à des examens externes indépendants réalisés par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et le Comité des parlementaires sur la sécurité nationale et le renseignement.

Un Canada numérique sécurisé



L'un des objectifs de la stratégie CST 2025 vise à améliorer la résilience numérique du Canada en favorisant une culture nationale de cybersécurité.

Protéger les Canadiens sur Internet

Le rôle que joue le CST dans la protection des réseaux du gouvernement du Canada et son mandat lié au renseignement électromagnétique étranger lui confèrent une perspective unique sur le contexte mondial des cybermenaces. Nous mettons cette perspective au service de tous les

Canadiens grâce à notre partenariat avec l’Autorité canadienne pour les enregistrements Internet (ACEI), l’organisme sans but lucratif qui gère le domaine « .ca ».



Le Bouclier canadien de l’ACEI a été lancé officiellement en avril 2020. Il s’agit d’un service DNS (*Domain Name System*) protégé qui empêche les utilisateurs de se connecter aux sites Web malveillants connus. Le fait de cliquer par mégarde sur un lien n’entraînera donc pas l’infection de votre appareil ou le vol de vos renseignements personnels. La connexion est tout simplement bloquée. En décembre 2020, le Bouclier canadien de l’ACEI a atteint son objectif d’un an lorsqu’il a franchi le seuil des 100 000 utilisateurs quatre mois à l’avance. Au cours de cette période, il a bloqué plus de 20 millions de domaines malveillants pour ses utilisateurs.

Rapports publics

Le CST favorise un Canada numérique sécurisé en présentant la bonne information au bon public, et ce, au bon moment.

Par exemple, au cours de la dernière année, le Centre pour la cybersécurité a publié quatre bulletins sur les cybermenaces :

- [Incidence de la COVID-19 sur les activités de cybermenaces](#)
- [Incidence de la COVID-19 sur les cybermenaces pesant sur le secteur de la santé](#)
- [Le rançongiciel moderne et son évolution](#)
- [Les cyberattaques visant le secteur canadien de l'électricité](#)

LES RAPPORTS PUBLICS DU CENTRE POUR LA CYBERSÉCURITÉ EN CHIFFRES



► Description longue - Les rapports publics du Centre pour la cybersécurité en chiffres :

En novembre 2020, le Centre pour la cybersécurité a publié sa deuxième [Évaluation des cybermenaces nationales](#), dans laquelle il présente les tendances récentes dans le contexte des cybermenaces, des rançongiciels à

l'espionnage industriel en passant par les campagnes d'influence étrangère.

Certains documents d'orientation publiés par le Centre pour la cybersécurité cette année formulent des conseils de cybersécurité à l'intention des particuliers et des organisations sur les sujets suivants, entre autres :

- l'infonuagique;
- le travail à distance;
- la COVID-19 et les sites web malveillants;
- les services bancaires en ligne;
- les achats en ligne;
- les vidéoconférences.

Le Centre pour la cybersécurité publie également, à l'intention des professionnels des TI, des centaines d'alertes et de bulletins de sécurité sur des sujets allant de correctifs de sécurité courants à des cyberincidents d'envergure, comme les compromissions liées à la plateforme Orion de SolarWinds et à Microsoft Exchange Server.



Promouvoir la cyberrésilience

Pour favoriser un Canada numérique sécurisé, il faut promouvoir la cyberrésilience de tous les Canadiens.

Pensez cybersécurité

Dans le cadre de la campagne de sensibilisation du public Pensez cybersécurité, des conseils de cybersécurité faciles à suivre sont présentés de façon décontractée et créative.

Tout au long de la pandémie, Pensez cybersécurité a proposé aux Canadiens des ressources sur plusieurs sujets, par exemple les arnaques liées à la COVID-19, le travail à distance et le commerce électronique. Il s'agit notamment d'une page de ressources liées à la COVID-19, de vidéos, à partager, de billets de blogue sur des sujets d'actualité et de capsules dynamiques.

En septembre 2020, le CST a lancé le nouveau site Web de Pensez cybersécurité, y compris l'outil d'autoévaluation sur la cybersécurité.

En octobre, Pensez cybersécurité a été l'organisme responsable du Mois de la sensibilisation à la cybersécurité (MSC) au nom du gouvernement du Canada. Le thème a porté sur l'appréciation des appareils. Sur Twitter, les gazouillis annonçant la diffusion de la vidéo de la chanson thème accrocheuse ont été vus 147 000 fois.

En mars 2021, Pensez cybersécurité a lancé la plus importante campagne publicitaire de l'histoire du CST avec la signature Ne vous laissez pas prendre. Elle portait sur l'hameçonnage, la cybermenace la plus susceptible de toucher les Canadiens, selon le Centre pour la cybersécurité, et a été vue plus de 74 millions de fois.





► Description longue - Statistiques sur les médias sociaux de la campagne Pensez cybersécurité

Carrefour de l'apprentissage

Le Carrefour de l'apprentissage du Centre pour la cybersécurité offre de la formation sur la cybersécurité et la sécurité des communications aux fonctionnaires fédéraux et à des intervenants canadiens d'autres secteurs clés, notamment l'industrie, le milieu universitaire et le secteur de l'éducation.

Au cours de la dernière année, le Carrefour de l'apprentissage a fait passer un grand nombre de ses cours au modèle d'apprentissage en ligne, en plus d'avoir élaboré et donné de nouveaux cours sur la cybersécurité à des groupes particulièrement ciblés par les cybermenaces durant la pandémie, notamment :

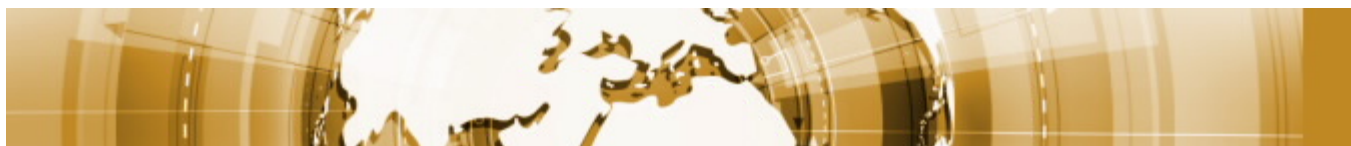
- les travailleurs de la santé;

- les chercheurs et professeurs universitaires;
- les fonctionnaires fédéraux qui travaillent à domicile;
- les enseignants de la 4e à la 12e année.



► Description longue - Le Carrefour de l'apprentissage en 2020-2021
:

Un avantage canadien sur le plan de l'information



Le CST assure la sécurité et la prospérité du Canada en recueillant du renseignement électronique à partir de réseaux étrangers et en protégeant les communications canadiennes de nature sensible.

Fournir du renseignement étranger aux décideurs canadiens

Le programme de renseignement électromagnétique étranger (SIGINT) du CST présente aux hauts responsables du Canada des indications à propos des activités, des motivations, des capacités et des intentions d'adversaires étrangers.

Nos rapports classifiés alertent et informent les représentants du gouvernement au sujet des menaces qui pèsent sur le Canada et leur fournissent des avis et des conseils sur les mesures de défense concrètes à prendre pour contrer ces menaces.

Au cours de la dernière année, en plus de soutenir l'intervention du gouvernement à l'égard de la pandémie, le SIGINT du CST a aidé à contrer les menaces étrangères comme l'espionnage, le terrorisme, l'extrémisme violent à caractère idéologique et l'enlèvement de Canadiens à l'étranger. Nos rapports de renseignement ont également mis en évidence les activités d'États hostiles et ont permis d'appuyer les opérations militaires du Canada et de protéger les forces déployées à l'étranger.

Les relations qu'entretient le CST avec ses partenaires de la collectivité des cinq (les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande) sont très avantageuses pour le Canada, car elles permettent d'accéder à des rapports de renseignement étranger inégalés sur des questions communes. Fort de ce partenariat de 75 ans, le CST est en mesure de fournir au gouvernement du Canada l'information la plus exhaustive qui soit sur les priorités canadiennes en matière de renseignement, ce qui permet de renforcer la sécurité et la prospérité du Canada.

LES RAPPORTS DE RENSEIGNEMENT ÉTRANGER DU CST EN 2020-2021



► Description longue - Les rapports de renseignement étranger du CST en 2020-2021 :

Fournir de l'information sur les cybermenaces

Le SIGINT du CST vient également appuyer l'élaboration de rapports publics non classifiés comme l'Évaluation des cybermenaces nationales 2020 (ECMN 2020), qui présente diverses cybermenaces étrangères pesant sur le Canada, dont l'espionnage industriel et la perturbation des infrastructures essentielles. Le SIGINT soutient aussi les activités du Centre pour la cybersécurité. Il l'informe rapidement des menaces afin que ce dernier puisse prendre les mesures nécessaires pour les atténuer ou les contrer.

L'attribution publique des cyberactivités malveillantes repose également sur l'analyse du SIGINT. Par exemple, en juillet 2020, le CST et ses alliés du Royaume-Uni et des États-Unis ont nommé un groupe d'auteurs de menace dotés de moyens sophistiqués comme étant responsable d'activités de cybermenace ciblant la recherche sur le vaccin contre la COVID-19. Ce groupe menait presque certainement ses activités pour le compte des services de renseignement de la Russie.

Surveiller les menaces étrangères ciblant notre processus démocratique

Comme l'indique l'ECMN 2020, les campagnes d'influence étrangère ne se limitent plus aux périodes électorales. Il s'agit maintenant d'activités courantes, et les adversaires ont recours aux médias sociaux pour :

- faire de la désinformation;
- diviser l'opinion publique;
- discréditer les politiciens;
- influencer les décisions liées aux politiques;
- déstabiliser les relations entre les pays;
- délégitimer la démocratie.

Au cours de la dernière année, le SIGINT du CST a continué d'informer le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, un groupe interministériel créé en 2019 dans le but d'accroître la sensibilisation aux menaces étrangères ciblant le processus électoral du Canada et d'aider le gouvernement à évaluer ces menaces et à y répondre.

Rappel : La *Loi sur le CST* stipule que les activités du CST ne doivent pas cibler les communications de Canadiens ou des personnes se trouvant au Canada. Elle stipule également que le CST doit protéger

la vie privée des Canadiens et des personnes se trouvant au Canada. Les audits internes, la surveillance externe et les organismes d'examen indépendants veillent à ce que nous respections la *Loi sur le CST* et toutes les autres lois canadiennes.

Protéger les communications canadiennes de nature sensible

Le pendant de « l'avantage stratégique sur le plan de l'information », c'est la protection des communications sensibles du Canada contre les adversaires.

Pour atteindre cet objectif, le CST développe, approuve et surveille des solutions de sécurité des communications (COMSEC) pour le gouvernement du Canada. Il s'agit des dispositifs et des procédures qui permettent aux intervenants autorisés de faire des appels, d'envoyer des messages textes ou des courriels et de stocker des données en toute sécurité.

Malgré la pandémie, le Centre pour la cybersécurité a continué de fournir l'ensemble des services COMSEC à ses ministères clients. Cette année, pour appuyer le Bureau du Conseil privé (BCP), le CST a collaboré avec Services partagés Canada pour ajouter des capacités d'appel vidéo aux appareils des hauts responsables (voir *Protéger le gouvernement et rendre possible son intervention*). On compte parmi les clients des ministres du Cabinet, des hauts fonctionnaires et des décisionnaires dans l'ensemble du gouvernement.

Le CST a également continué de gérer le Réseau canadien Très secret (RCTS), qui permet aux ministères et aux entrepreneurs autorisés de stocker et de transmettre de l'information sensible de manière sécurisée.

Innovation éclairée



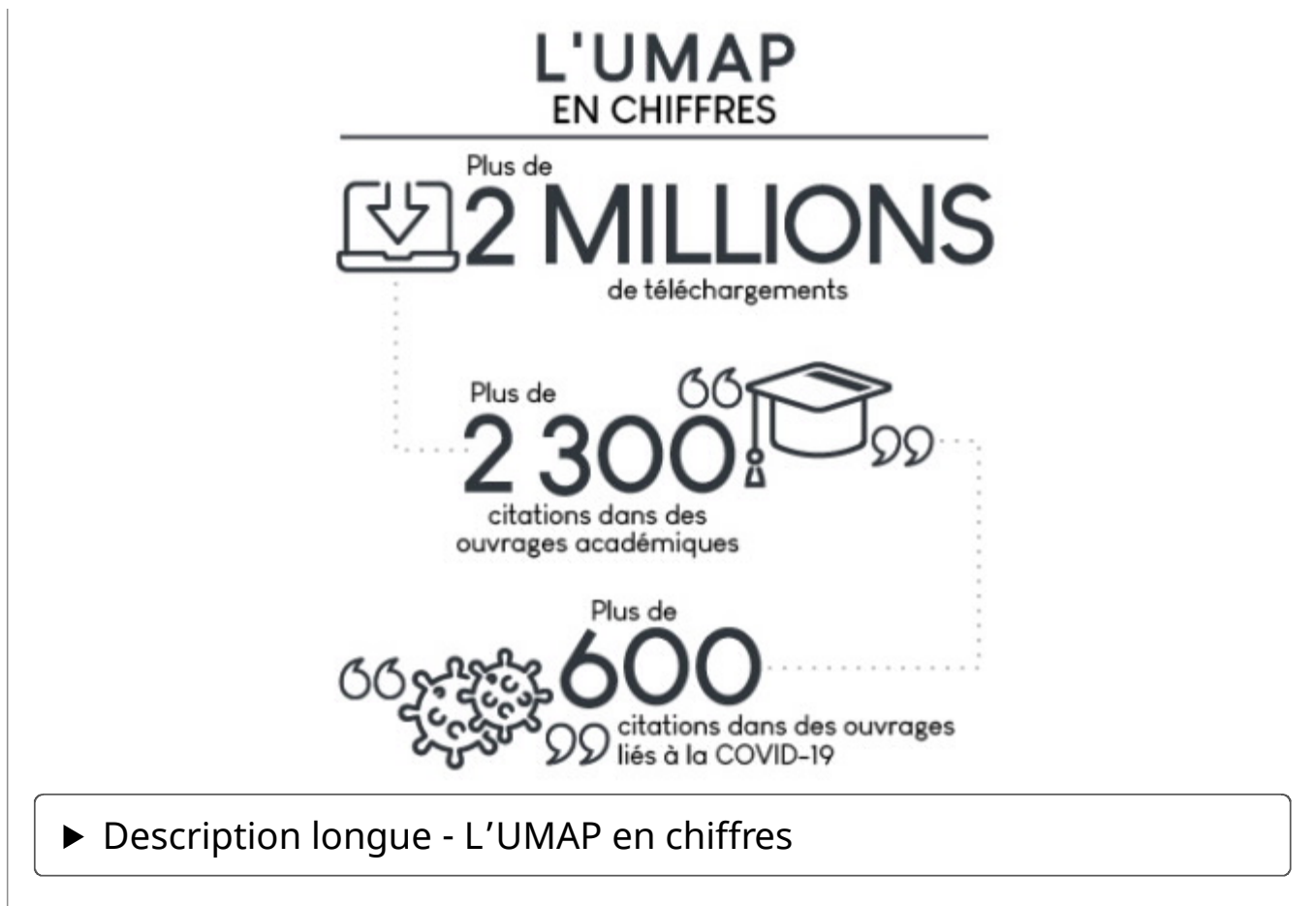
La mentalité cultivée par le CST mise sur l'innovation, car le contexte de menace est en constante évolution. En cybersécurité, il est impératif d'innover, sans quoi on est condamné.

L'innovation par la recherche

L'Institut Tutte pour les mathématiques et le calcul (ITMC) est un institut de recherche gouvernemental relevant du CST, qui est axé sur les mathématiques fondamentales et l'informatique. Il se penche notamment sur l'UMAP (*Uniform Manifold Approximation and Projection*).

À l'origine, l'UMAP a été développée par les chercheurs de l'Institut Tutte en tant que technique d'analyse des maliciels. Mais depuis sa diffusion en 2018 sous forme de source ouverte, on en a fait mention dans plus de 2 300 études portant tant sur l'apprentissage machine que l'astrophysique.

En 2020, des épidémiologistes ont commencé à utiliser l'UMAP pour analyser les nombreuses données complexes qui ont été produites au cours de la pandémie de COVID-19. À ce jour, on en a fait mention dans plus de 600 études liées à la COVID-19 allant de l'analyse des variants du virus à la recherche de candidats pour les traitements.



L'innovation par la collaboration

GeekWeek est un bon exemple de l'approche collaborative adoptée par le CST en matière d'innovation. Au cours de cet atelier de 9 jours animé par le Centre pour la cybersécurité, des praticiens de la cybersécurité venant des secteurs privé et public, ainsi que du milieu universitaire, travaillent ensemble pour trouver de nouvelles solutions à leurs problèmes communs.

Cette année, en raison des restrictions imposées par la pandémie, GeekWeek a été tenu de façon virtuelle pour une toute première fois.

Les équipes ont fait d'importantes percées dans les domaines suivants :

- identification et analyse des URL d'hameçonnage malveillantes;
- étude de l'utilisation des devises virtuelles par les auteurs de menace;
- amélioration de la sécurité pour :

- les technologies infonuagiques émergentes;
- les dispositifs connectés à Internet;
- les communications mobiles.

Tout au long de l'année, le Centre pour la cybersécurité et la communauté de GeekWeek ont continué de travailler sur ces projets et d'autres projets similaires pour aider à renforcer la cyberrésilience du Canada.



GEEKWEEK 2020 EN CHIFFRES



► Description longue - GeekWeek 2020 en chiffres :

Regard tourné vers l'avenir

Le Conseil national de recherches Canada (CNRC) reconnaît le CST en tant que centre de réflexion novatrice pour ce qui est du futur de la cybersécurité et a invité le dirigeant principal de la Recherche de l'organisme à participer au groupe de travail sur l'analyse prospective qui a été mis sur pied en septembre 2020. L'objectif du CNRC est de cerner les principaux enjeux auxquels le Canada sera confronté au cours des dix à quinze prochaines années, ainsi que les possibles occasions qui pourraient se présenter. Le groupe de travail a relevé plusieurs priorités en ce qui concerne la cybersécurité et le respect de la vie privée au Canada, dont les suivantes :

- le renforcement de la cyberrésilience de l'infrastructure numérique;
- la protection de la vie privée et de la sécurité des données dans le nuage;
- la promotion du Canada en tant que plateforme de stockage et de transit fiable pour les données internationales.

Le CNRC publiera son rapport d'analyse prospective avant la fin de l'année.

Atténuer la menace que représente l'informatique quantique

Les techniques standards que nous utilisons aujourd'hui pour chiffrer les données ne seront plus efficaces après l'arrivée de l'informatique quantique. Une technologie capable de percer les mécanismes cryptographiques que nous employons de nos jours pourrait être disponible dès les années 2030. Le Centre pour la cybersécurité du CST s'efforce donc de préparer dès à présent le Canada pour l'avenir.

Au cours de la dernière année, nous avons tenu des séances d'information avec nos clients du gouvernement et de l'industrie, tant au niveau technique que de la direction, et publié des ouvrages sur les sujets suivants

:

- Faire face à la menace que l'informatique quantique fait peser sur la cryptographie;
- Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie;
- Blogue sur les normes de la cryptographie post-quantique.



Nous avons également travaillé avec l'industrie et les organismes de normalisation à faire avancer la recherche de pointe sur la post-quantique et collaboré avec les ministères du gouvernement du Canada à la mise à niveau de leur équipement. Conjointement, ces initiatives permettront de s'assurer que le Canada demeure un chef de file dans le domaine de la cybersécurité post-quantique.

Un effectif motivé



La stratégie CST 2025 repose sur la capacité de l'organisme à pouvoir miser sur un effectif motivé. C'est ce qui lui permet de mener à bien tous les autres aspects de son mandat. Nous sommes fiers d'annoncer que le CST a

été reconnu comme un des meilleurs employeurs en 2020 et en 2021.

Mettre les gens au premier plan

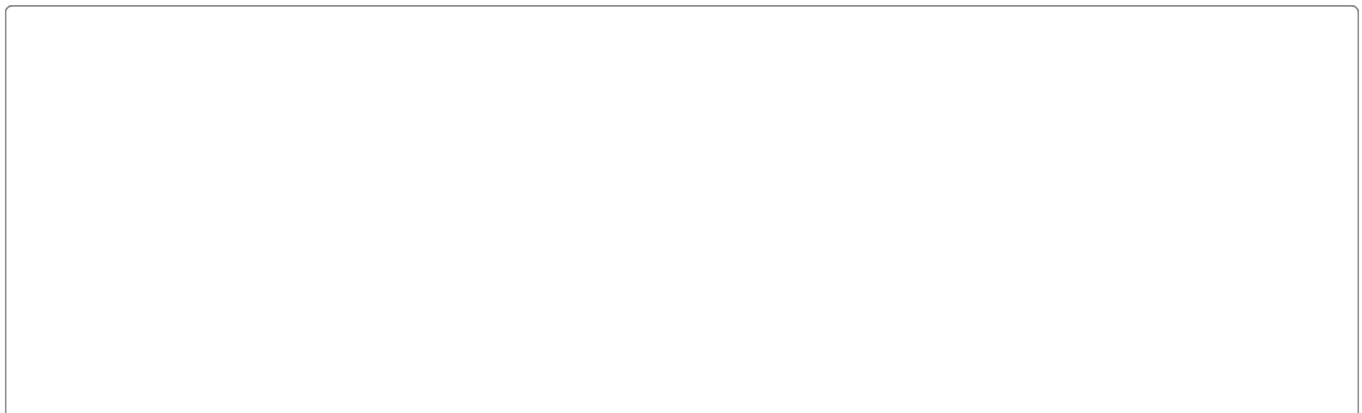
La ressource la plus importante du CST est son effectif.

En mars 2021, le CST a ajouté le Comité des personnes à sa structure de gouvernance pour veiller à ce que les employés continuent d'être à l'avant-plan des décisions prises par la direction de l'organisme. Présidé par Shelly Bruce, chef du CST, le comité a pour mandat de s'assurer que le CST :

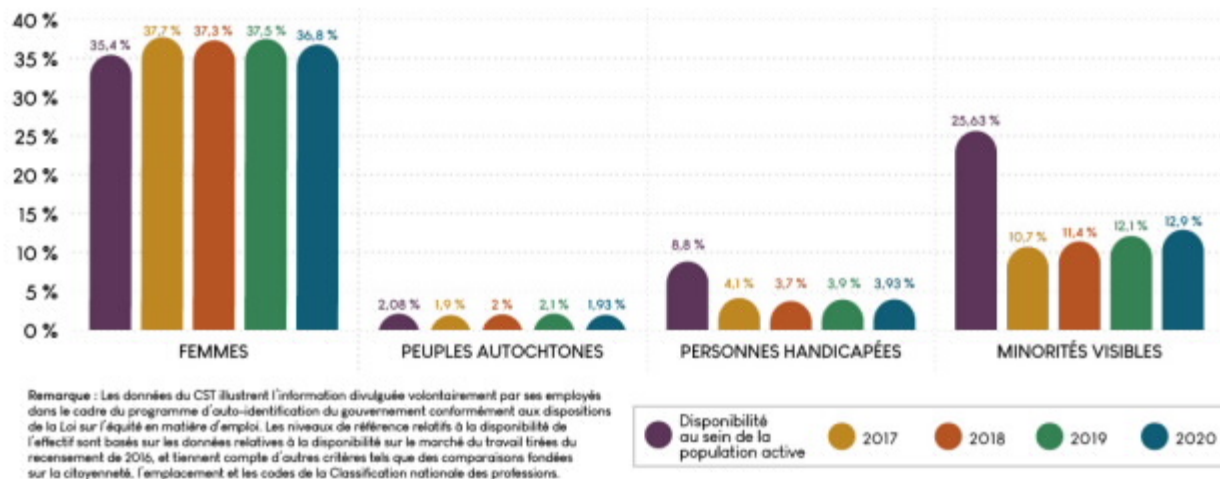
- favorise le bien-être en milieu de travail et la santé mentale;
- respecte la loi sur les langues officielles et soutient la dualité linguistique;
- favorise l'accessibilité en milieu de travail;
- identifie et élimine les obstacles systémiques à la participation;
- met fin au harcèlement et à la discrimination;
- incorpore la diversité et l'inclusion à ses processus et à ses pratiques;
- a recours à l'analyse comparative entre les sexes plus (ACS+) pour éclairer ses politiques et la conduite de ses activités.

Diversité et inclusion

Exception faite des femmes, les membres des groupes visés par l'équité en matière d'emploi à l'échelle du gouvernement fédéral sont toujours sous-représentés au CST.



REPRÉSENTATION DE L'ÉQUITÉ EN MATIÈRE D'EMPLOI AU CST ENTRE 2017 ET 2020



► Description longue - Représentation de l'équité en matière d'emploi au CST entre 2017 et 2020

Une des principales tâches du nouveau Comité des personnes du CST est de veiller à ce que l'organisme réexamine ses politiques internes du point de vue de l'équité, de la diversité et de l'inclusion. Cela comprend les politiques de recrutement et de maintien de l'effectif, ainsi que la formation de sensibilisation, ainsi que l'élaboration et la mise en œuvre de programmes.

Un groupe consultatif composé d'employés de milieux divers soutient le comité et s'assure que les groupes sous-représentés soient pris en compte lors de la prise de décision. Le groupe consultatif collaborera avec les responsables clés des ressources humaines pour traduire ces perspectives en une politique fondée sur des principes et des résultats tangibles.

Nouvelle formation

Cette année, le CST s'efforce d'éliminer les obstacles systémiques dont sont victimes les personnes transgenres et non binaires en offrant de la formation aux collègues prenant part au processus de recrutement. Nous

nous sommes également penchés sur les autres politiques et pratiques pour éradiquer toute pratique discriminatoire basée sur l'identité et l'expression de genre.

En février 2021, deux employés du CST ont fait une présentation en ligne intitulée « Être Noir(e) au Canada » à deux cents collègues et membres de la direction. Les présentateurs ont offert des exemples éclairants de discrimination tirés de leurs propres vies. Ils ont de plus animé une discussion sur le privilège et mentionné des ressources sur la lutte contre le racisme. Le CST prépare une version de la présentation qu'il incorporera à la formation obligatoire de ses nouveaux employés.

Célébrations

Nous
avons
dû
adapter
nos



célébrations sur la diversité qui devaient se tenir en personne ou les remettre à l'an prochain. Par exemple, la communauté LGBTQ2+ du CST, des alliés et des membres de la direction participent généralement au

défilé de la fierté d'Ottawa. Cette année, le CST a plutôt décoré ses installations aux couleurs de l'arc-en-ciel et célébré la Semaine de la fierté sur les médias sociaux.

Conversations cruciales

En janvier 2021, le conférencier et psychologue international John Amaechi OBE a tenu un événement à l'échelle du CST qui visait à discuter de racisme, de discrimination et de l'importance de favoriser une culture organisationnelle respectueuse et inclusive.

En mars 2021, le CST a organisé une discussion virtuelle en groupe dans le cadre de laquelle six employés ont parlé avec franchise de l'incidence disproportionnée de la COVID-19 selon le genre.

Ce même mois, les employés du CST ont invité un dirigeant autochtone possédant de l'expérience du renseignement électromagnétique pour tenter de mieux comprendre cette culture et discuter des façons dont le CST peut promouvoir la réconciliation.

Tout au long de la pandémie, le canal de discussion en ligne du CST sur la diversité et l'inclusion a offert une tribune aux employés désireux de partager leurs expériences personnelles et de mentionner des ressources sur la façon d'appuyer efficacement les communautés marginalisées. Le canal compte plus de 900 membres (plus du quart de l'organisation).

Le CST a déjà amorcé ces conversations importantes dans le but de renforcer sa culture organisationnelle. Nous sommes résolus à les transformer en mesures concrètes au cours des prochains mois.

Bien-être des employés

Reconnaissant les conséquences de la pandémie sur la santé mentale, le CST a offert des cours de formation et des conférences sur des sujets tels que l'autocompassion, la gestion de l'anxiété et le parentage au cours de la pandémie.

Notre équipe des Communications internes a envoyé des rappels réguliers concernant le soutien qui avait été mis à la disposition des employés.

Le Programme de consultation et d'orientation du CST a adapté ses services en ligne de manière à offrir :

- de la formation;
- des consultations individuelles;
- des services de gestion des conflits;
- du soutien aux équipes dispersées (nouveau);
- des séances hebdomadaires de médiation guidée en français et en anglais (nouveau).

La transition vers le télétravail

Avant la pandémie, la majorité du personnel du CST travaillant à partir de ses installations sécurisées ne pouvait pas accéder à leurs courriels professionnels non classifiés à l'extérieur de l'édifice. La transition vers le télétravail n'a donc pas été chose facile.

Le Centre pour la cybersécurité était déjà prêt à travailler dans un environnement en nuage sécurisé et le



CST avait prévu dans son plan à long terme d'offrir ces capacités au reste de l'organisme. Lorsque la pandémie a frappé, ce plan à long terme s'est rapidement transformé en un besoin urgent.

En l'espace de deux semaines, en mars 2020, les équipes du CST ont :

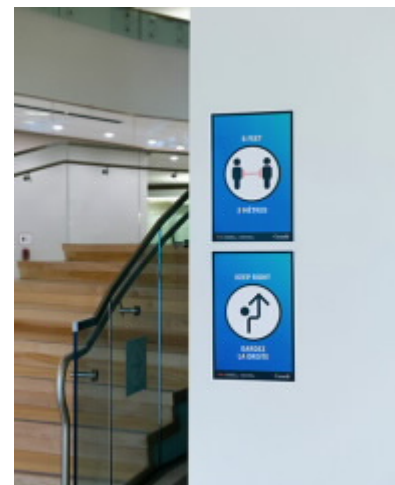
- fourni des dispositifs mobiles sécurisés aux employés;
- migré les charges de travail dans un environnement en nuage sécurisé;
- offert de nouvelles capacités afin que les employés puissent travailler et communiquer à distance.

Grâce à ces efforts extraordinaires, le CST a été en mesure de maintenir ses activités quotidiennes et de produire des résultats importants pour le Canada tout au long de la dernière année, malgré le fait que plusieurs de ses employés travaillaient essentiellement de la maison.

Assurer la sécurité dans les installations

Comme nos activités de nature classifiée ne peuvent être menées qu'à partir de notre environnement classifié, nous avons pris les mesures nécessaires pour faire en sorte que nos installations soient aussi sécuritaires que possible. Nous avons entre autres :

- réaménagé les espaces de travail et les aires communes;
- adapté les horaires de travail;
- imposé le port du masque;
- mis en application les directives de santé publique, dont la consigne de rester à la maison en cas de symptômes.



Notre équipe de nettoyage mérite d'ailleurs une mention spéciale pour avoir réussi à maintenir des normes plus rigoureuses tout au long de l'année.

Nous n'avons enregistré aucun cas de transmission de la COVID-19 dans nos environnements de travail au cours de la période faisant l'objet d'un présent rapport.

Résultats du sondage auprès des fonctionnaires fédéraux

Le Sondage auprès des fonctionnaires fédéraux (SAFF) de 2020 comprenait de nouvelles questions sur la santé mentale, le racisme et le travail durant la pandémie. Les résultats du SAFF du CST ont révélé ce qui suit.

- Quatre-vingt-onze pour cent (91 %) des membres du personnel considèrent que le CST les a clairement informés des services et des ressources en santé mentale qui leur étaient accessibles.
- Quatre-vingt-sept pour cent (87 %) se sentiraient libres de parler du racisme en milieu de travail sans crainte de représailles.
- Quatre-vingt-quatre pour cent (84 %) sont satisfaits des mesures prises par le CST pour protéger leur santé et leur sécurité physique pendant la pandémie.

Bien que ces résultats soient au-dessus de la moyenne de la fonction publique (84 %, 79 % et 81 % respectivement), il est toujours possible de faire mieux.

Naturellement, le pourcentage d'employés indiquant avoir ressenti du stress au travail a augmenté pendant la pandémie, passant de 9 % en 2019 à 15 % en 2020.

89 %
des membres du personnel du CST
sont fiers du travail qu'ils font.



86 %
sentent qu'on les encourage
à innover ou à prendre des
initiatives dans leur travail.

90 %
affirment que les personnes avec
lesquelles ils travaillent valorisent
leurs idées et opinions.



92 %
affirment que le CST
les traite avec respect.

► Description longue - Statistiques choisies provenant des résultats du CST au sondage auprès des fonctionnaires fédéraux.

À partir de ces résultats, le CST a dégagé trois priorités sur lesquelles il souhaite se pencher en 2021 :

- assurer une meilleure gestion du stress, de la santé mentale et de l'équilibre entre la vie professionnelle et la vie privée;
- tenir des discussions et prendre des mesures pour favoriser l'équité, la diversité et l'inclusion;
- aider la direction et les employés à s'adapter à la nouvelle réalité de « l'avenir du travail ».

Le CST continuera de s'assurer que ses employés ont tout ce dont ils ont besoin pour mener à bien leur mission dans l'intérêt du Canada et des Canadiens.

Sensibilisation

Les restrictions imposées par la pandémie nous ont forcés à repousser à l'an prochain les activités de notre programme d'approche communautaire comme les ateliers de codage dans les écoles primaires de la région. Les volontaires du CST ont toutefois trouvé des façons de partager virtuellement leurs compétences avec la nouvelle génération de talents en technologie.

De novembre 2020 à mars 2021, les volontaires du CST ont animé neuf présentations sur la cybersécurité auxquelles ont participé près de 220 élèves du secondaire dans la région de la capitale nationale.

Nous avons maintenu notre partenariat avec **Hackergal** (disponible en anglais seulement), un organisme à but non lucratif qui a pour objectif d'initier les jeunes filles, ainsi que les étudiantes trans et non binaires, au codage. Cette année, les volontaires du CST ont pris part aux activités suivantes :



- mentorat des étudiants;
- évaluation des soumissions au programmation;
- participation aux groupes de discussion virtuels;
- prononciation de discours;
- rédaction de blogues;
- création de vidéos d'apprentissage;
- contribution au contenu du mois sur l'histoire des Noirs;
- conquête des médias sociaux.

Nous avons poursuivi notre partenariat avec **Cyber Titan** (disponible en anglais seulement), et fourni le contenu pour leur concours en ligne sur la cyberdéfense auquel ont participé de jeunes Canadiens de la 7^e à la 12^e année.

En juillet 2020, les volontaires du CST ont commencé à collaborer avec **Black Boys Code**, un organisme qui inspire les jeunes hommes noirs à devenir les créateurs de contenu numérique et les innovateurs technologiques de demain.

Un organisme de confiance reconnu



Parce que la majorité du travail du CST est classifié, il est essentiel que nous utilisions des systèmes robustes de surveillance et de reddition de compte pour que les Canadiens aient confiance que le CST respecte la loi et protège la vie privée.

De la Loi sur le CST, qui est entrée en vigueur en août 2019, a découlé la création de trois nouveaux organes d'examen externes indépendants pour renforcer la surveillance des activités du CST :

- Le Bureau du commissaire au renseignement (BCR)
- L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR)
- Le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)

Le CST valorise les examens importants et indépendants que ces organes effectuent ainsi que les recommandations qu'ils lui offrent pour améliorer ses pratiques et ses politiques.

Le commissaire au renseignement

Le Bureau du commissaire au renseignement fournit une surveillance quasi judiciaire des autorisations du CST en matière de renseignement étranger et de cybersécurité avant qu'elles n'entrent en vigueur.

Le 27 janvier 2021, le commissaire au renseignement, l'honorable Jean-Pierre Plouffe, a présenté son premier rapport annuel (2019).

Dans ce dernier, le commissaire a examiné cinq autorisations ministérielles qu'a reçues le CST entre juillet 2019 (lors de la création du bureau du commissaire) et la fin de cette même année. Le commissaire a statué que les conclusions sur lesquelles le ministre de la Défense nationale avait basé ces autorisations étaient toutes raisonnables et justifiées.

Le commissaire a également formulé plusieurs recommandations à des fins d'amélioration, que le CST a acceptées et mises en œuvre.

Le commissaire a d'ailleurs fait remarquer ces améliorations dans son rapport annuel de 2020, qui a été présenté le 30 avril 2021.

Le commissaire reconnaît également que le CST a « fait preuve d'un engagement continu quant à l'amélioration de [ses] procédures et de [ses] demandes, malgré les difficultés et le fardeau que représente la pandémie. » (p. 3)

« Bien que le nouveau cadre de surveillance n'en soit qu'à sa deuxième année, les développements positifs de la dernière année sont de bon augure. »

- L'honorable Jean-Pierre Plouffe, commissaire au renseignement,
Rapport annuel de 2020

Le rapport de 2020 fait état de l'examen de quatre autorisations ministérielles accordées au CST en 2020, qui ont toutes été trouvées raisonnables et justifiées.

Le commissaire a offert d'autres suggestions pour améliorer la clarté des dossiers de demande et pour s'assurer qu'ils soient complets. Il a également noté toutefois que « ces enjeux n'ont pas influé sur le caractère raisonnable des conclusions du ministre ni empêché le [commissaire au renseignement] d'approuver les autorisations » (p. 17). Le CST accueille la perspective du commissaire sur la façon d'améliorer le processus associé aux autorisations ministérielles.

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR)

L'OSSNR est un organisme indépendant dont le mandat est d'examiner minutieusement toutes les activités relatives à la sécurité et au renseignement au sein du gouvernement fédéral.

L'OSSNR a présenté au Parlement son premier rapport annuel le 11 décembre 2020.

En ce qui concerne le CST, il est indiqué dans le rapport que :

- Le CST a élaboré et diffusé des ensembles complets de politiques pour encadrer ses activités d'échange d'information avec des partenaires

étrangers (p. 49);

- Le CST a pris des mesures de conformité en temps utile et conformément à sa politique (p. 72);
- Le CST s'est conformé à la loi lors d'un incident relatif à la protection des renseignements personnels concernant une activité d'analyse de métadonnées qu'il a réalisée (p. 85).

Le 4 mars 2021, l'OSSNR a publié son premier examen d'un incident autosignalé par le CST lié à la vie privée. L'OSSNR a fait cinq recommandations au CST et ce dernier les a toutes acceptées.

Le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)

Le CPSNR est composé de membres de la Chambre des communes et du Sénat qui ont une habilitation de sécurité TRÈS SECRÈTE. Le Comité a le vaste mandat d'examiner les activités des organismes de sécurité nationale et du renseignement du Canada, dont le CST fait partie.

Le rapport annuel de 2020 du CPSNR a été présenté au Parlement le 12 avril 2021. Environ un cinquième du rapport a été consacré aux cyberactivités malveillantes et le CPSNR a indiqué que « Les cybermenaces présentent un risque grave et croissant pour la sécurité nationale du Canada » (p.48).

Le rapport visait principalement à présenter une mise à jour de l'évaluation des menaces qui avait été entreprise par le Comité en 2018. N'étant pas un examen à proprement dit, il ne présentait aucune conclusion ou recommandation quant aux activités du CST. Dans la conclusion du rapport, le Comité a toutefois reconnu « les efforts des organisations de la sécurité et du renseignement d'avoir fourni des documents en réponse aux demandes du Comité même si elles étaient également aux prises avec leurs propres défis liés à la pandémie » (p. 45).

Le CST continuera de soutenir tous ces organes d'examen et de leur fournir les renseignements dont ils ont besoin pour examiner ses activités au nom des Canadiens.

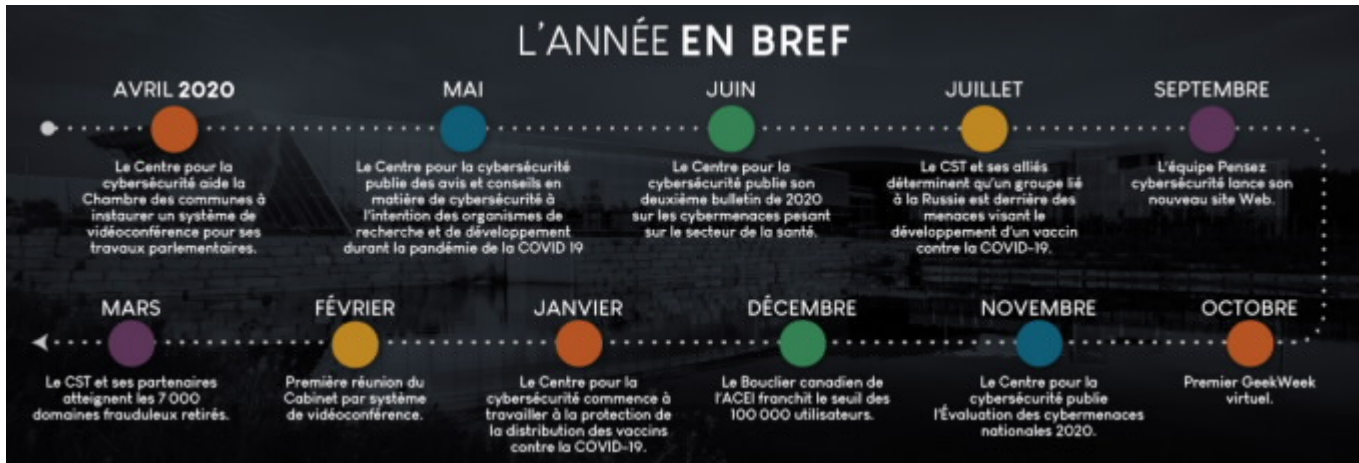
Faits saillants



L'année en bref



- Avril 2020 : Le Centre pour la cybersécurité aide la Chambre des communes à instaurer un système de vidéoconférence pour ses travaux parlementaires.
- Mai : Le Centre pour la cybersécurité publie des avis et conseils en matière de cybersécurité à l'intention des organismes de recherche et de développement durant la pandémie de la COVID 19.
- Juin : Le Centre pour la cybersécurité publie son deuxième bulletin de 2020 sur les cybermenaces pesant sur le secteur de la santé.
- Juillet : Le CST et ses alliés déterminent qu'un groupe lié à la Russie est derrière des menaces visant le développement d'un vaccin contre la COVID-19.
- Septembre : L'équipe Pensez cybersécurité lance son nouveau site Web.
- Octobre : Premier GeekWeek virtuel.
- Novembre : Le Centre pour la cybersécurité publie l'Évaluation des cybermenaces nationales 2020.
- Décembre : Le Bouclier canadien de l'ACEI franchit le seuil des 100 000 utilisateurs.

- Janvier : Le Centre pour la cybersécurité commence à travailler à la protection de la distribution des vaccins contre la COVID-19.
- Février : Première réunion du Cabinet par système de vidéoconférence.
- Mars : Le CST et ses partenaires atteignent les 7 000 domaines frauduleux retirés.



Le CST en bref

- Le CST a été fondé en 1946 sous le nom de Direction des télécommunications du Conseil national de recherches.
- En 1975, la Direction est renommée Centre de la sécurité des télécommunications et fait désormais partie du programme de la Défense nationale.
- En novembre 2011, le CST devient un organisme autonome sous la responsabilité du ministre de la Défense nationale.
- La chef actuelle du CST, Shelly Bruce, a été nommée en juin 2018.
- Le Centre canadien pour la cybersécurité est lancé en octobre 2018 et regroupe les expertises du gouvernement fédéral sous un même toit. Le Centre pour la cybersécurité fait partie du CST.
- La loi régissant le CST, appelée Loi du CST entre en vigueur en août 2019.

- Le budget annuel du CST pour l'année 2020-2021 s'élève à 794 millions de dollars. 
- Notre effectif s'élève à près de 3 000 employés. 
- Le 1^{er} septembre 2021, le CST célèbrera son 75^e anniversaire.

Note de bas de page



dont on a un plein pouvoir



En date du 31 mars 2021, nous comptons 2 992 employés à temps plein. Nous ne comptons pas les employés à temps partiel, les entrepreneurs et les étudiants.

Date de modification :

2021-06-29