Gouvernement du Canada | Government of Canada

Rapport annuel du Centre de la sécurité des télécommunications 2019-20

ISSN 2564-0488

▸ Table des matières

Il peut sembler remarquable que le Centre de la sécurité des télécommunications (CST) se prépare à publier son premier rapport public en même temps qu'il se prépare à célébrer son 75e anniversaire. L'évolution du CST, de sa mise sur pied jusqu'à aujourd'hui, est un récit qui vaut la peine d'être raconté.

Nous sommes le CST, un organisme uni, reconnu et fiable.

Notre effectif inspiré et notre innovation de pointe aident à sécuriser le Canada numérique, à fournir un avantage en matière d'information au Canada et à obtenir un impact stratégique grâce aux cyberopérations.

Le mandat du CST a toujours été important, mais il est graduellement devenu de plus en plus pertinent au fil de ces 75 années passées à recueillir du renseignement étranger et à protéger les systèmes d'information. Les priorités du gouvernement du Canada, ainsi que l'environnement

technique mondial, ont beaucoup changé au cours de ces décennies. Aujourd'hui, en 2020, le monde est plus polarisé et complexe que jamais sur le plan géopolitique. De nouvelles technologies avancées, interconnectées et perturbatrices font leur apparition à un rythme sans précédent.

À la jonction de ces deux tendances se trouve le mandat actuel de cybersécurité du CST.

Bien que nous ayons toujours trouvé des moyens de nous adapter à notre environnement opérationnel en constante évolution, deux développements récents ont été importants pour mettre le CST en position de relever les défis de la prochaine décennie. Premièrement, la *Loi sur le CST* est entrée en vigueur à la mi-2019; cette loi reconnaît la pertinence sans cesse croissante du mandat, du savoir-faire et des capacités du CST. La *Loi* accroît les pouvoirs actuels du CST et confère de nouveaux mandats à l'organisme pour qu'il soit en mesure de faire appel à son expertise pour aider les victimes de cybercrimes qui ne font pas partie du gouvernement du Canada, pour prendre des cybermesures à l'extérieur du Canada lorsque cela est nécessaire et pour offrir de l'assistance aux Forces armées canadiennes dans l'exécution de leur mandat, au besoin. Cette *Loi* — qui fera l'objet d'un examen dans trois ans — a donné au CST un ensemble modernisé de pouvoirs et a accru le cadre de reddition de comptes de l'organisme à l'aide de nouvelles fonctions de surveillance et d'examen.

Deuxièmement, le Centre canadien pour la cybersécurité a été mis sur pied. Cet organisme qui relève du CST s'appuie sur les fondements de notre mission de longue date en matière de sécurité des technologies de l'information et sur l'expertise en cybersécurité d'autres ministères du gouvernement du Canada. Le Centre pour la cybersécurité est tourné vers le public et joue le rôle de source unifiée au Canada fournissant des avis,

des conseils, des services et du soutien spécialisés en matière de cybersécurité. Les équipes de cyberdéfense et de renseignement étranger du CST fournissent les informations et l'expertise nécessaires pour atténuer les risques envers notre cybersécurité nationale. La période du présent rapport marque la première année complète de fonctionnement du Centre pour la cybersécurité.

Cette puissante collaboration entre les deux missions du CST a été mise en évidence plus que jamais lors de notre travail visant à protéger le déroulement des élections générales du Canada en 2019. Le mandat du CST nous a placé au cœur de la surveillance des menaces étrangères ciblant le Canada avant les élections et de la mise en place d'une infrastructure canadienne pour y faire face. Avec ses partenaires, le CST a joué un rôle important, notamment en partageant ses connaissances uniques plus largement avec les Canadiens et les partis politiques du Canada sous la forme d'évaluations des menaces et de prestations d'avis et de conseils conçus sur mesure.

Un exemple plus récent est le soutien que nous avons offert au gouvernement du Canada dans la gestion de la crise de la COVID-19. Depuis le début de 2020, le CST a fourni du renseignement à ses clients du gouvernement, a alerté les Canadiens au sujet de la forte augmentation des arnaques en ligne liées à la COVID-19 et a conseillé le secteur canadien de la santé et de la recherche médicale au sujet de divers auteurs de cybermenaces déterminés. Des conseils, de l'orientation et des services sur mesure ont été conçus pour aider à protéger les Canadiens et les responsables de la recherche d'une solution à la pandémie.

Dans notre monde moderne, la cybersécurité doit être prise au sérieux et intégrée à chaque étape de l'évolution numérique du Canada : pour les propriétaires et exploitants d'infrastructures essentielles, pour les petites

et moyennes entreprises, pour les organismes de recherche et pour les Canadiens. Les réseaux numériques sous-tendent tous les aspects de la société, de l'économie et de la sécurité du Canada. En adoptant des pratiques de cybersécurité, même basiques, tous les Canadiens et tous les organismes canadiens peuvent jouer un rôle dans la cybersécurité nationale du Canada. Il est de notre devoir de fournir aux Canadiens les informations et les outils appropriés pour les aider à jouer leur rôle de défenseurs de premières lignes de la cybersécurité du Canada. Nous avons déployé de grands efforts en 2019-2020 pour sensibiliser le public et ce travail doit se poursuivre.

Depuis ses débuts en temps de guerre, le CST a favorisé une culture d'innovation qui lui est à la fois naturelle et nécessaire et qui est soutenue par son effectif exceptionnel qui fait preuve d'une expertise hors pair, d'engagement envers la collaboration et d'un ensemble robuste de valeurs communes. Certains considèrent encore le CST comme un « organisme secret », mais il serait plus exact de parler d'un « organisme qui a des secrets ». Il est nécessaire que certaines de nos activités restent hors du domaine public et cela, il va sans dire, a des effets sur le contenu que nous pouvons publier dans le présent rapport. Toutefois, toutes nos activités peuvent faire l'objet d'examens par des tierces parties externes et indépendantes qui agissent au nom du public en faisant savoir aux Canadiens que le CST fait un excellent travail et quels éléments notre organisme peut améliorer.

J'espère que grâce à la publication de ce rapport et des rapports à venir au fil des prochaines années, le CST pourra mieux se faire connaître et que le public comprendra mieux le rôle joué par le CST sur le plan national et la contribution importante de notre organisme envers la protection du Canada et des Canadiens contre ceux qui veulent nuire à notre sécurité, à notre prospérité et à notre compétitivité.

Ne manquez pas nos célébrations du 75e anniversaire du CST au cours de la prochaine année afin de découvrir comment notre histoire représente les fondations de notre avenir.

Shelly Bruce
Chef du CST

DÉFINIR LA PERSPECTIVE STRATÉGIQUE DU CST

Le **CST en 2025** est un document qui donne un aperçu de l'horizon stratégique des cinq prochaines années afin d'orienter les investissements et les opérations de manière à concentrer notre attention pour obtenir des résultats sur le plan national et atténuer les risques de niveau national. Voici les objectifs définis au début de 2020 :

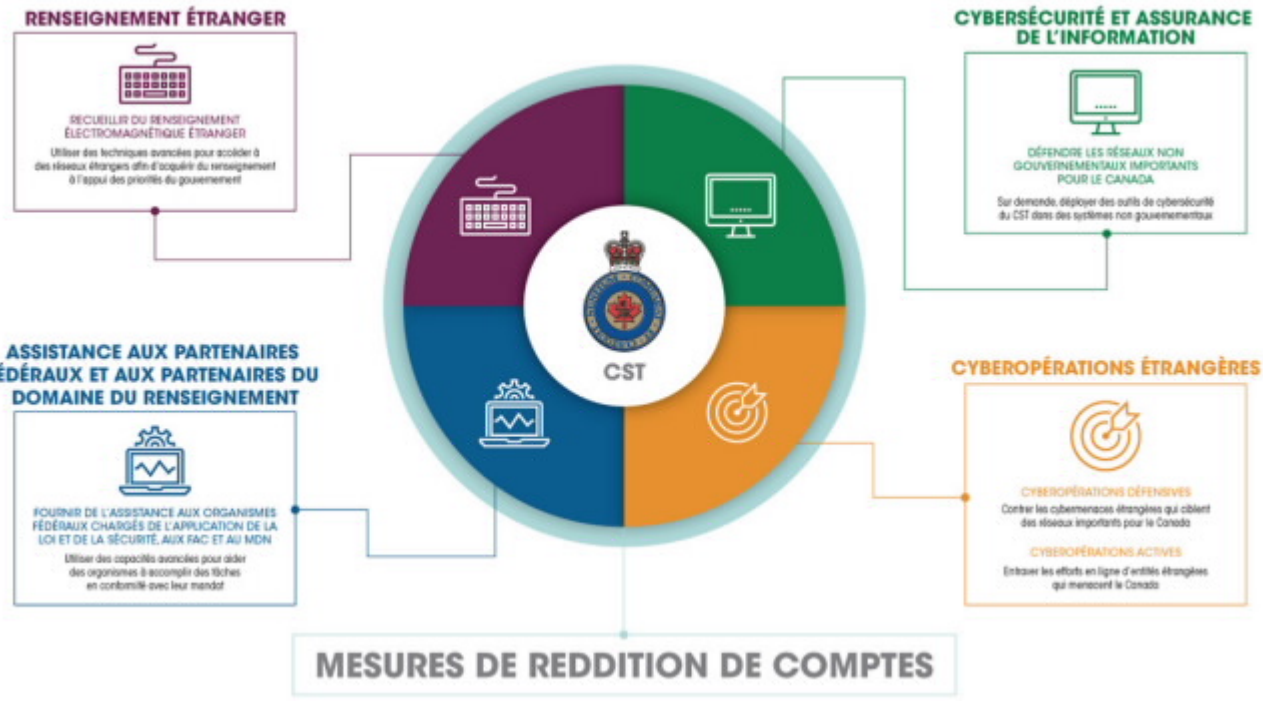
- **Un Canada numérique sécuritaire :** Le CST améliore la résilience numérique du Canada à l'aide d'une culture nationale de cybersécurité, de collaboration et de pratiques exemplaires.
- **Avantage informationnel pour les responsables canadiens des prises de décisions :** Le CST fournit un avantage stratégique en matière d'information pour assurer la sécurité, la prospérité et la compétitivité du Canada.
- **Leadership en matière de cyberopérations :** Le CST est le centre national des cyberopérations qui visent à défendre le Canada et à faire progresser les intérêts nationaux.
- **Innovations de pointe :** Le CST est le pionnier de confiance pour trouver des solutions sécurisées dans le contexte numérique en constante évolution.

POUVOIRS MIS À JOUR ET MODERNISÉS COMPTANT DES MESURES ACCRUES DE REDDITION DE COMPTES

En août 2019, la *Loi sur le CST*, un jalon capital pour le Centre de la sécurité des télécommunications, est entrée en vigueur. Cette nouvelle *Loi* définit les rôles joués par le CST comme autorité nationale en matière de

renseignement étranger (renseignement électromagnétique, ou SIGINT) et comme autorité technique nationale en matière de cybersécurité et d'assurance de l'information. La *Loi* exprime en détail le mandat accru du CST :

- Aider à protéger et défendre les infrastructures d'information importantes pour le Canada;
- Acquérir du renseignement étranger à l'appui des priorités du Canada en matière de renseignement;
- Effectuer des cyberopérations à l'étranger, tant actives que défensives, pour protéger les intérêts du Canada; et,
- Utiliser notre expertise pour offrir de l'assistance aux organismes fédéraux responsables de l'application de la loi et de la sécurité, aux Forces armées canadiennes et au ministère de la Défense nationale pour les aider à exécuter leurs mandats prévus par la loi.



▶ Description détaillée - Mesures de reddition de comptes

De plus, la *Loi sur le CST* explique la place du CST dans le nouveau cadre de reddition de comptes de la collectivité canadienne de la sécurité et du renseignement. Les opérations du CST se déroulent en vertu d'une série d'autorisations du ministre de la Défense nationale et la *Loi sur le CST* vient ajouter à cela un poste de commissaire au renseignement pour assurer une surveillance quasi judiciaire des autorisations du CST en matière de renseignement étranger et de cybersécurité.

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a été mis sur pied à la mi-2019 en vue de faire l'examen des activités de la collectivité canadienne de la sécurité et du renseignement dont le CST fait partie. Simultanément, le Bureau du commissaire du CST, créé en 1996, a été supprimé et les examens en cours ont été confiés à l'OSSNR. En outre, le CST peut faire l'objet d'examens de la part du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) et d'autres agents du Parlement, comme le Vérificateur général et les commissaires à l'information et à la protection de la vie privée.

LA SÉCURITÉ, LA PROSPÉRITÉ ET LA COMPÉTITIVITÉ DU CANADA

Voici un aperçu des activités clés du CST en 2019-2020 visant à illustrer comment notre effectif, nos plans, notre expertise et nos partenariats se combinent pour nous aider à réaliser notre mission à l'appui de la sécurité, de la prospérité et de la compétitivité du Canada.

Protéger le .gc.ca

En 2019-2020, le Centre pour la cybersécurité du CST a continué de fournir une défense dynamique de calibre mondial des réseaux du gouvernement du Canada, en bloquant quotidiennement plus d'un milliard d'actions malveillantes visant les systèmes, bases de données et sites Web du gouvernement fédéral. Le gouvernement du Canada a dû rapidement effectuer la transition de ses systèmes et de ses informations vers des environnements dans le nuage et le CST a été un acteur de premier plan dans la conception de solutions de sécurité visant à protéger ces environnements. Les ministères et organismes fédéraux qui se trouvent à l'intérieur du périmètre de sécurité exploité par le CST et Services partagés Canada tirent parti de moyens sophistiqués de cyberdéfense et du renseignement sur les menaces recueillis par des partenaires de confiance et le CST en vertu de son mandat. Cela renforce la protection des programmes et réseaux fédéraux du Canada et des renseignements personnels des Canadiens.

Certains auteurs de cybermenaces tentent de faire passer leurs sites Web malveillants pour des sites du gouvernement du Canada ou utilisent des adresses courriel qui usurpent l'identité d'entités du GC. Lorsque ces supercheries ont été découvertes, le personnel du Centre pour la cybersécurité a travaillé sans relâche pour découvrir ces domaines et a collaboré avec des partenaires commerciaux et internationaux de confiance pour les supprimer. En 2019-2020, les sites Web les plus souvent usurpés ont été les sites de l'Agence du revenu du Canada, de l'Agence de la santé publique du Canada et de l'Agence des services frontaliers du Canada. Grâce à notre vigilance, les Canadiens sont moins susceptibles d'être victimes de fraudes et de vols de renseignements personnels causés par des auteurs de cybermenaces.

Protéger le .ca

Les tentatives d'hameçonnage sont causées par des auteurs de cybermenaces, appartenant souvent à des réseaux criminels, pour frauder les Canadiens, voler leurs renseignements personnels ou avoir accès à des réseaux d'intérêt. En vertu du rôle du CST d'autorité nationale en matière de cybersécurité, le Centre pour la cybersécurité

travaille en partenariat avec l'Autorité canadienne pour les enregistrements Internet (ACEI), un organisme sans but lucratif qui gère le domaine Internet « .ca ». Dans le cadre de ce partenariat, le Centre pour la cybersécurité et l'ACEI échangent des renseignements sur les menaces afin d'accroître l'efficacité du Bouclier canadien, un service de système de noms de domaine (DNS) protégé offert gratuitement. Ce service bloque la connexion aux sites malveillants qui risquent d'infecter les appareils électroniques des utilisateurs et de voler leurs renseignements personnels.

La sécurité grâce à la collaboration avec l'industrie canadienne

En 2019-2020 le Centre pour la cybersécurité a concentré ses efforts sur la sensibilisation des fournisseurs d'infrastructures essentielles du secteur privé aux questions et préoccupations en matière de cybersécurité. Le Centre pour la cybersécurité a communiqué des renseignements sur les cybermenaces avec des entreprises, notamment des renseignements provenant de nos activités de défense du gouvernement du Canada et de notre programme de renseignement étranger. Le Centre pour la cybersécurité fournit à ces intervenants des flux de nouvelles automatisés, des cyberalertes (des avis de sécurité qui nécessitent une intervention dans les 24 heures) et des cyberflashs (des avis de sécurité qui nécessitent l'application immédiate d'une solution) et d'autres produits de conseils et d'orientation.

Le Centre pour la cybersécurité a collaboré avec le secteur financier du Canada, notamment des banques, des organismes de réglementation et des institutions financières, contribuant ainsi à prévenir des pertes potentielles dues à la fraude. De plus, du soutien a été offert au secteur de l'énergie en aidant les entreprises de services publics à faire la surveillance

des signes liés aux cybermenaces. Ce ne sont là que quelques exemples des nombreuses activités de partenariats qui se sont déroulées durant la période couverte par ce rapport et qui continueront de se poursuivre et de se multiplier afin de renforcer la cybersécurité des systèmes essentiels des différents secteurs de l'industrie canadienne.

Cela est important. Un sondage effectué en 2017 par Statistique Canada a permis de conclure qu'au moins une entreprise canadienne sur cinq croit que ses systèmes ont été ciblés par des auteurs de cybermenaces. Pour aider à protéger ces systèmes, le Centre pour la cybersécurité a élaboré des contrôles de cybersécurité de base pour les petites et moyennes organisations (PMO), car on a reconnu que ces PMO ont des environnements d'exploitation et des ressources qui les distinguent des entités organisationnelles plus vastes, mais qu'elles sont tout autant à risque dans le contexte actuel des cybermenaces.

Publication d'un deuxième rapport sur les cybermenaces ciblant les élections

En 2019, le CST a fait le point sur les cybermenaces contre le processus démocratique du Canada en mettant à jour les évaluations effectuées dans le cadre de son tout premier rapport public sur ce sujet publié en 2017. Ce rapport préélectoral a informé les Canadiens de la tendance à la hausse des cybermenaces contre les processus démocratiques à l'échelle mondiale, en particulier contre les pays de l'OCDE, et a noté que l'électorat, les systèmes d'information et les partis politiques du Canada ne seraient pas à l'abri. Le rapport, de concert avec la perspective opérationnelle en temps réel du CST, a aidé à l'élaboration

d'avis et de conseils du Centre pour la cybersécurité à l'intention des personnes participant au processus démocratique, p. ex. Élections Canada, les partis politiques, les électeurs canadiens.

Suivi des menaces étrangères lors des élections de 2019

Dans les mois qui ont précédé et jusqu'au moment des élections, le CST a travaillé en partenariat avec le Service canadien du renseignement de sécurité (SCRS), Affaires mondiales Canada (AMC) et avec la GRC pour former le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections. Le rôle du CST dans le Groupe était de faire le suivi de l'ingérence et des menaces étrangères dans le processus électoral du Canada. En collaboration avec les représentants officiels du Groupe de travail, le CST a fourni des séances d'information aux responsables du Protocole public en cas d'incident électoral majeur (PPIEM) du gouvernement du Canada qui n'ont observé aucune activité ayant atteint un seuil justifiant une annonce publique ou qui aurait pu nuire à la capacité du Canada à tenir des élections libres et équitables. Le CST a participé, avec d'autres membres du Groupe de travail, à la prestation de séances d'informations à des représentants des différents partis politiques et des médias.

Assurer la sécurité de l'infrastructure des élections canadiennes

Le Centre pour la cybersécurité s'est basé sur l'expérience du CST découlant des élections de 2015 pour assurer que de robustes et efficaces mesures de cyberdéfense soient mises en place pour protéger les systèmes et les réseaux d'Élections Canada. Des conseils et de l'orientation ont aussi été fournis à des institutions provinciales (et autres) qui participent aux processus démocratiques.

Fournir des conseils en cybersécurité aux partis politiques et aux candidats

Le CST a fourni une série de séances d'information et a publié un ensemble de produits conçus sur mesure expliquant les mesures à prendre et présentant des conseils et des pratiques exemplaires à adopter à l'intention des partis politiques, des candidats et de leur effectif pour les aider à se protéger contre les cyberactivités malveillantes tout au long des élections fédérales de 2019, et le CST avait en outre mis en place des protocoles à suivre si de l'assistance en matière de cybersécurité était requise.

Fournir des conseils en cybersécurité aux partis politiques et aux candidats

Le CST a fourni une série de séances d'information et a publié un ensemble de produits conçus sur mesure expliquant les mesures à prendre et présentant des conseils et des pratiques exemplaires à adopter à l'intention des partis politiques, des candidats et de leur effectif pour les aider à se protéger contre les cyberactivités malveillantes tout au long des élections fédérales de 2019, et le CST avait en outre mis en place des protocoles à suivre si de l'assistance en matière de cybersécurité était requise.

Fournir du renseignement étranger aux preneurs de décisions canadiens

Le travail du CST en matière de renseignement étranger ne s'est pas limité au soutien envers le processus démocratique du Canada. Au cours de la dernière année, le CST a fourni des rapports de renseignement étranger à plus de 2100 clients provenant de plus de vingt-cinq ministères et organismes du gouvernement du Canada en réponse à toute une gamme de priorités liées aux affaires internationales, à la défense et à la sécurité. Par exemple, les rapports de renseignement du CST ont aidé à contrecarrer des cybermenaces étrangères, ils ont appuyé des opérations militaires du Canada et ont servi à protéger les forces déployées; ces rapports ont servi à identifier des activités d'États hostiles et ont fourni des connaissances sur les crises et événements mondiaux en vue d'éclairer l'élaboration de politiques et les prises de décisions du gouvernement.

Protéger les communications canadiennes de nature sensible

Le CST a continué de faire fonctionner le Réseau canadien Très secret (RCTS) pour le gouvernement du Canada, a aidé à l'intégration de nouveaux ministères et organismes et a accru les capacités de télécommunication et les fonctionnalités du RCTS tout en assurant la prestation d'autres solutions de télécommunications sécurisées. De plus, le CST a aidé la Chambre des communes à développer des outils pour organiser des réunions virtuelles du Parlement et des comités.

Développer l'avantage quantique du Canada

Les responsables du CST en matière de recherche, en partenariat avec d'autres ministères et des sommités du milieu universitaire, ont poursuivi leurs travaux sur une solution cryptographique nationale à résistante à l'informatique quantique. Les résultats de ces travaux permettront de sécuriser les informations les plus sensibles du gouvernement du Canada avant la production d'un ordinateur quantique suffisamment puissant pour

déchiffrer la cryptographie que nous utilisons actuellement. La conception d'une solution est en cours et on prévoit la déployer dans certains ministères du gouvernement du Canada dès 2021.

Promouvoir l'expérimentation et l'innovation dans le domaine de la cybersécurité

La cybersécurité est un impératif d'équipe. Au printemps 2019, le CST a organisé « La Grande exploration », la dixième édition de son événement classifié d'une semaine qui rassemble des intervenants du gouvernement, de l'industrie, du milieu universitaire et d'organismes alliés pour tenter de résoudre des problèmes particuliers en matière de cybersécurité. Plus tard au cours de la même année, le CST a organisé la sixième édition de la « GeekWeek », un événement similaire, mais non classifié, qui réunit des praticiens de la cybersécurité de partout dans le monde pour cogiter afin de trouver des solutions à des problèmes cruciaux du domaine de la cybersécurité. Ces séances d'expérimentations nous ont aidés à définir d'importants nouveaux savoir-faire afin de mieux sécuriser les réseaux contre les menaces communes et de trouver de nouveaux moyens d'atténuer les risques.

Promotion des domaines STIM auprès de la jeunesse canadienne

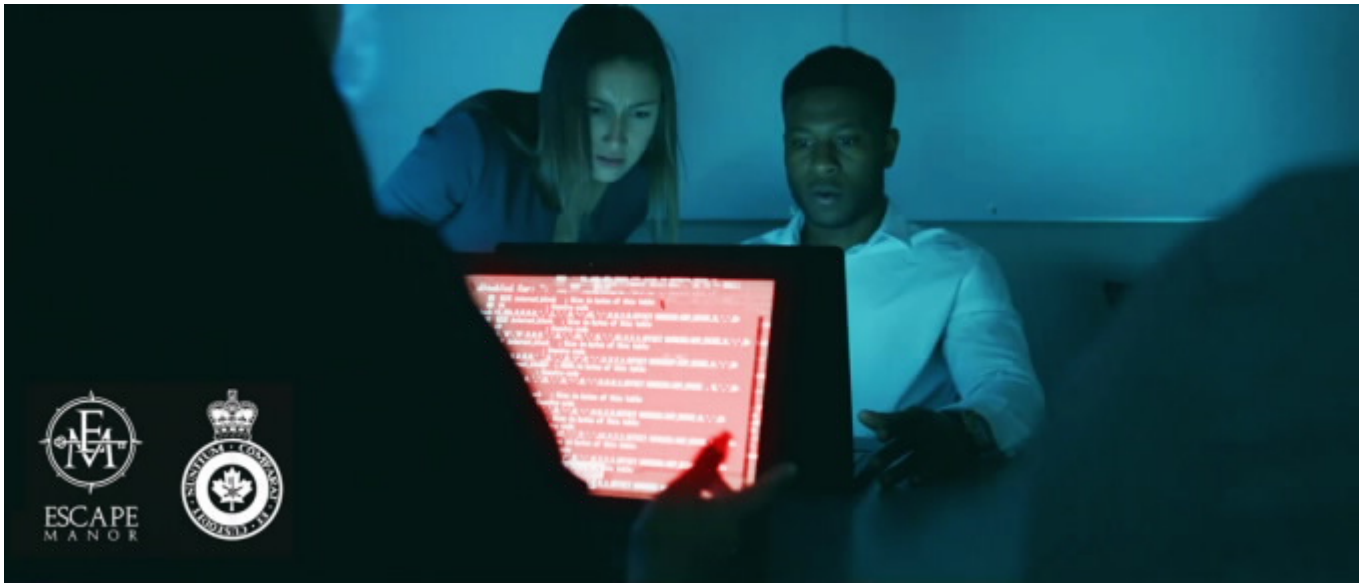
Le CST a un programme d'approche communautaire qui comprend notamment du soutien et du mentorat sur le plan national auprès d'organismes sans but lucratif, comme Hackergal et CyberTitan. Ces partenariats favorisent le développement des compétences des jeunes du Canada dans les domaines des STIM et attisent l'intérêt des jeunes envers

les études et les carrières dans les domaines des STIM. Ils motivent et engagent également les employés du CST qui sont toujours prêts à partager leur passion pour les domaines des STIM dans des organisations nationales, communautaires et des écoles locales.

Présenter des concepts de cybersécurité aux enfants canadiens

Pour inspirer les jeunes qui deviendront les adultes qui nous aideront à répondre aux besoins futurs du gouvernement du Canada en matière de cybersécurité, le CST s'est associé à Ingenium, le réseau de musées canadiens des sciences et de l'innovation, pour créer Chiffrer | Déchiffrer, une exposition itinérante qui explore des concepts de chiffrement et de cybersécurité et spécialement conçue pour les enfants d'âge scolaire. L'exposition Chiffrer | Déchiffrer a connu un grand succès dans les musées qui l'ont présentée, elle a entre autres attiré plus de 22 000 visiteurs au Musée des sciences et de la technologie du Canada. L'exposition sera présentée dans d'autres villes canadiennes au cours de 2021.

Trouver de nouveaux moyens de recruter les meilleurs talents

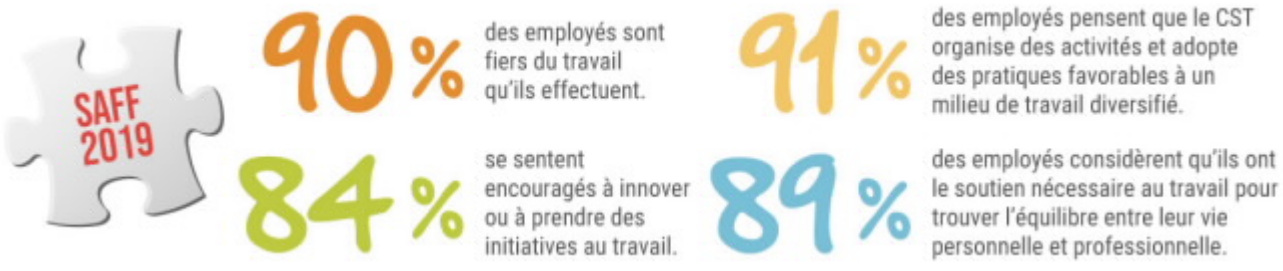


En 2019-2020, le CST a mis en place de nouveaux partenariats visant à promouvoir notre organisme et à appuyer les efforts essentiels de recrutement, afin de s'assurer que le CST soit en mesure de recruter les personnes les plus compétentes. Parmi ces initiatives, on compte « La Recrue », un jeu d'évasion immersif créé en partenariat avec l'Escape Manor d'Ottawa. Les participants qui ont réussi à résoudre l'énigme ont ensuite eu l'occasion de rencontrer des recruteurs du CST et ont été invités à postuler à un emploi au CST.

Les réalisations du CST en 2019-2020 ont été rendues possibles par son effectif constitué de gens brillants et dévoués. Les valeurs, l'éthique et la culture du CST se combinent pour créer un milieu de travail qui promeut la diversité, l'inclusion et le sens de la communauté. Cela ouvre la voie à des

expérimentations qui favorisent l'innovation dans l'ensemble de l'organisme, ce qui nous a permis de décrocher encore une fois le titre de « Meilleur employeur » en 2019 et en 2020.

Les résultats du Sondage auprès des fonctionnaires fédéraux (SAFF) de 2019 révèlent ce qui suit :



▶ Description détaillée - Les résultats du CST au SAFF

Les résultats du CST au SAFF sont positifs depuis plusieurs années, cela dit, nous savons que nous pouvons toujours faire mieux! Le CST prend à cœur l'amélioration continue et communique régulièrement avec les employés sur la façon d'améliorer leur expérience en milieu de travail pour s'assurer que l'effectif de l'organisme soit inspiré et muni de ce dont il a besoin pour réussir sur les plans individuels et collectifs, afin d'accomplir une mission importante pour le Canada et les Canadiens. Notre rapport présenté au greffier du Conseil privé dans le cadre de l'initiative du GC « Au-delà de 2020 » démontre comment notre effectif s'engage à servir notre pays.

Voici quelques dates clés et chiffres importants dans l'histoire du CST...

▶ Description détaillée - Dates clés et chiffres importants dans l'histoire du CST

- Aujourd'hui, le CST est un organisme autonome qui effectue des opérations 24/7 afin de recueillir du renseignement étranger vital (renseignement électromagnétique), pour protéger les systèmes importants pour le Canada; le CST effectue des cyberopérations et offre de l'assistance à ses partenaires fédéraux pour les aider à exécuter leurs mandats.
- La chef du CST, Shelly Bruce, relève du ministre de la Défense nationale, l'honorable Harjit S. Sajjan.
- Le CST a un budget de 786,6 million et son effectif compte 2900 employés.

Cherchez dans nos événements, ressources et notre information

Mission

Découvrez la mission impressionnante du CST

Carrières

Joignez-vous à notre équipe et aidez à assurer la sécurité des Canadiens

Culture et communauté

Découvrez comment nous soutenons nos employés et notre communauté

Date de modification :

2021-06-28