Centre de la sécurité des télécommunications
Communications Security Establishment

ISSN 2564-0488
CAT D95-11F-PDF

Centre de la sécurité des télécommunications

RAPPORT ANNUEL

2021–2022

Canada

Centre de la sécurité des télécommunications
1929, chemin Ogilvie
Ottawa, ON K1J 8K6
cse-cst.gc.ca

ISSN 2564-0488
CAT D95-11F-PDF

Table des **matières**

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 technique en matière de cybersécurité et d'assurance de l'information.

Le Centre canadien pour la cybersécurité[1] (Centre pour la cybersécurité), qui sert d'autorité opérationnelle en matière de cybersécurité pour le gouvernement fédéral, relève du CST.

Le mandat du CST est détaillé dans la *Loi sur le CST*[2] et présente les cinq volets suivants :

- le renseignement électromagnétique étranger;
- la cybersécurité;
- les cyberopérations actives;
- les cyberopérations défensives;
- l'assistance technique et opérationnelle offerte à des partenaires fédéraux.

Le présent rapport est un sommaire non classifié des activités qu'a menées le CST du 1er avril 2021 au 31 mars 2022.

À moins d'indication contraire, « cette année » fait référence à l'année financière et non à l'année civile.

Avant-propos de la **ministre de la Défense nationale**

Les événements mondiaux qui se sont déroulés cette année ont souligné l'importance que revêt le mandat du CST.

Les comportements de certaines puissances mondiales s'avèrent de plus en plus hostiles et irresponsables, y compris dans le cyberespace. Comme en témoigne l'invasion scandaleuse en Ukraine par la Russie, les deux vont souvent de pair.

Des intervenants étrangers font la promotion de fausses informations pour masquer la vérité, semer la discorde et justifier l'injustifiable. Pour être en mesure de naviguer en eaux troubles, le gouvernement du Canada doit se baser sur des faits concrets quant aux actions, aux plans et aux capacités de ses adversaires. Grâce au renseignement électromagnétique étranger que le CST recueille, le Canada dispose de ces faits.

Des incidents hautement médiatisés aux quatre coins du monde ont montré à quel point une cyberintrusion pouvait facilement perturber des services essentiels dont dépend la population. Le Centre pour la cybersécurité du CST défend les institutions fédérales contre ces menaces. Il travaille parallèlement avec des fournisseurs d'infrastructures essentielles et offre des ressources uniques aux Canadiens dans le but d'améliorer la résilience globale du Canada dans le cyberespace.

À la lumière de l'importance croissante du mandat du CST, le gouvernement du Canada investit massivement pour appuyer les activités du CST.

Il investit entre autres dans la capacité du CST à mener des cyberopérations étrangères visant à prévenir et à contrer les cyberattaques. Il subventionne aussi la recherche classifiée dans le domaine des technologies de pointe, comme l'informatique quantique et l'intelligence artificielle.

Étant donné que les menaces qui nous guettent continuent d'évoluer et de se multiplier, ces investissements permettront d'offrir au CST les ressources dont il a besoin pour contribuer à la protection des Canadiens et pour favoriser l'atteinte des priorités stratégiques du Canada pendant longtemps encore.

- L'honorable Anita Anand,
  ministre de la Défense nationale

> « Superviser le Centre de la sécurité des télécommunications, afin qu'il soit en mesure de mener la réponse du Canada face à l'évolution rapide des cyberrisques et des cybermenaces, notamment grâce à des ressources adéquates et à une coopération étroite avec nos alliés. »
>
> **Premier ministre Justin Trudeau**
> *Lettre de mandat[3] à l'intention de la ministre de la Défense nationale, le 16 décembre 2021*

Message de la **chef et du chef associé**

Quelle année nous avons vécue!

En effet, depuis le dernier rapport annuel du CST, le volume et la variété des cybermenaces n'ont pas cessé de croître. L'habitude de vivre et de travailler en ligne a persisté parallèlement à la pandémie. De plus, les événements qui se sont déroulés à l'échelle planétaire ont changé les priorités en matière de renseignement et ont introduit de nouveaux scénarios de cybermenace.

Ainsi, la mission du CST[4] ne s'est jamais avérée aussi pertinente, car elle permet :

- de recueillir du renseignement électromagnétique étranger indispensable;
- de protéger les systèmes importants du Canada;
- de mener des cyberopérations défensives et actives;
- de faire part de notre expertise à des partenaires fédéraux de la défense, de la sécurité nationale et des services de police.

Dans le présent rapport, nous fournissons des détails sur les activités qu'a menées le personnel du CST durant l'année en vue de réaliser la mission de l'organisme. Pas tous les détails, bien entendu. Il faut savoir que certains aspects de notre travail (savoir-faire, techniques et renseignement) doivent demeurer secrets pour être efficaces. Un rapport annuel n'a néanmoins jamais présenté autant d'information sur les activités de l'organisme et sur les techniques employées pour les réaliser. En effet, cette année, le CST a pris des mesures sans précédent afin de rehausser son niveau d'ouverture et de transparence.

Dans les derniers mois, nous avons déclassifié du renseignement sur les campagnes de désinformation éhontées de la Russie pour pouvoir en informer les Canadiens sur les médias sociaux. Il n'y a pas si longtemps, rare sont ceux qui auraient pu s'imaginer que nous aurions déclassifié du renseignement. Nous avons aussi averti des organisations canadiennes au sujet d'outils et de techniques employés par les auteurs de cybermenace parrainés par la Russie. De plus, nous avons continué de communiquer aux intervenants pertinents des indicateurs de cybermenace expurgés tirés du renseignement classifié recueilli. Nous avons en outre continué d'insérer de l'information provenant de sources classifiées dans des évaluations publiques sur les menaces.

La collaboration entre le Centre pour la cybersécurité du CST et les industries et les partenaires liés aux infrastructures essentielles s'est également poursuivie dans le but d'accroître la résilience numérique du Canada. Par l'intermédiaire de nos comptes de médias sociaux, de la campagne Pensez cybersécurité et du Mois de la sensibilisation à la cybersécurité, nous avons aussi pu présenter aux Canadiens des mesures de cybersécurité pratiques. Un nombre sans précédent de cadres du CST a aussi participé à des événements publics, à des comités rassemblant les industries, à des conférences universitaires, à des comités parlementaires et à des entrevues médiatiques. Bien que nous ne puissions présenter publiquement aucun détail classifié, sachez que le CST se prête aux examens et à la surveillance des organismes externes compétents. Les Canadiens peuvent ainsi être assurés que toutes les activités du CST sont réalisées conformément à la loi et que leur vie privée est protégée en tout temps.

Le présent rapport décrit donc en détail les mesures concrètes que notre collectivité a adoptées pour abattre les inégalités systémiques ainsi que les façons que nous avons célébré la diversité et l'inclusion, car il s'agit d'impératifs non négociables de la mission du CST. Des conversations franches ont d'ailleurs été tenues concernant des erreurs qui ont été commises dans le passé. Nous nous sommes efforcés d'éliminer les obstacles à l'équité dans nos programmes et nos processus, et nous avons partagé de nombreuses expériences positives en tant que collectivité.

Les groupes d'affinité au travail (représentant par exemple la communauté noire, les Autochtones, les personnes neurodivergentes, la communauté 2SLGBTQIA+, la communauté juive et les femmes) ont donné de la rétroaction qui a changé la donne et proposé des façons d'améliorer le milieu de travail pour l'ensemble des employés. Leur leadership et leurs expériences ont permis d'orienter la création du cadre sur l'équité, la diversité et l'inclusion[5] du CST, qui a été approuvé par le Comité exécutif du CST en mars 2022. Le rôle de leader et de partenaire qu'a adopté le CST au sein de la collectivité de la sécurité et du renseignement du Canada et des pays alliés nous remplit de fierté.

Par ailleurs, en 2021, le CST a également célébré ses 75 ans d'existence en tant qu'organisme cryptologique national du Canada. Nous en avons profité pour souligner le travail de nos prédécesseurs à qui nous devons beaucoup, notamment les neuf chefs précédents qui ont été à la tête du CST depuis 1946. Aujourd'hui, une page se tourne sur cet anniversaire important et il ne fait aucun doute que la pertinence de notre travail grandira d'année en année.

- Shelly Bruce, 10e chef du CST
- Dan Rogers, chef associé du CST


STAND
WITH
UKRAINE

Invasion de l'**Ukraine** par la Russie

Le 24 février 2022, les forces russes ont envahi l'Ukraine.

Le CST a appuyé les mesures qu'a prises le Canada en réaction à cette invasion illégale. Pour ce faire, il a mis à profit les volets de son mandat touchant la cybersécurité et le renseignement électromagnétique étranger (SIGINT).

Mesures prises contre les cybermenaces russes

Dans les semaines précédant l'invasion, le Centre pour la cybersécurité a publié deux avis publics qui demandaient aux organisations liées aux infrastructures essentielles canadiennes de renforcer leurs mesures de défense pour contrer des activités de cybermenace connues parrainées par la Russie[6].

Ces avis étaient fondés sur les connaissances opérationnelles du Centre pour la cybersécurité et du secteur SIGINT du CST ainsi que sur les antécédents de la Russie par rapport à l'utilisation irresponsable de cybercapacités, par exemple dans les cas suivants :

- la cybercompromission de SolarWinds[7];
- les activités ciblant la recherche sur le vaccin contre la COVID-19[8];
- les activités ciblant le processus démocratique de la Géorgie[9];
- les attaques ciblant des gouvernements ou des infrastructures essentielles commises partout dans le monde au moyen du maliciel NotPetya[10].

> Nous savons que la Russie dispose de capacités sophistiquées lui permettant de mener des cyberattaques. Nous ne parlons pas ici uniquement de mésinformation et de désinformation, mais bien d'attaques qui ciblent les infrastructures, les systèmes, les personnes et les entreprises et qui peuvent causer de graves perturbations. Heureusement, dans les dernières années, nous avons investi dans le CST, qui détient des cybercapacités extraordinaires et à la fine pointe de la technologie. Il s'agit d'ailleurs de l'un des éléments nous permettant de nous défendre contre les cyberattaques russes ou les cyberattaques étrangères de manière générale.
>
> **Premier ministre Justin Trudeau**
> *Conférence de presse du gouvernement du Canada, le 3 mars 2022*

Avant et durant l'invasion, le Centre pour la cybersécurité a continué de suivre de près les activités de cybermenace au Canada et à l'étranger, et de communiquer l'information pertinente aux partenaires liés aux infrastructures essentielles du Canada. Ce flux de renseignements sur les menaces comprend ce qui suit :

- des indicateurs de compromission (des détails numériques sur des activités malveillantes);
- des conseils sur l'atténuation des risques;
- des alertes confidentielles sur :
  - → de nouvelles formes de maliciels;
  - → des tactiques utilisées pour cibler des victimes.

Nous avons également continué de communiquer de l'information sur les cybermenaces à des partenaires importants en Ukraine.

Appui des mesures prises par le Canada en réaction à l'invasion en Ukraine

En appui aux mesures prises par le Canada en réaction à l'invasion injustifiable en Ukraine par la Russie, le CST a fourni au bon moment des rapports de renseignement électromagnétique étranger pertinents permettant de répondre aux besoins de plusieurs clients différents.

Par exemple, il a participé aux efforts de rapatriement du personnel diplomatique canadien déployé en Ukraine en donnant du renseignement sur les risques qu'il courait.

Le CST a continué à offrir une assistance technique et opérationnelle à l'opération UNIFIER, qui est la mission des Forces armées canadiennes (FAC) en soutien à l'Ukraine. Il a notamment communiqué du renseignement et apporté de l'appui en matière de cybersécurité.

Mesures visant à contrer la désinformation russe

Le CST a surveillé les campagnes de désinformation liées à la guerre en Ukraine qui sont parrainées par la Russie, dont ce qui suit :

- la fausse information selon laquelle seules des cibles militaires sont attaquées;
- les théories du complot antisémites, anti-LGBTQ+, anti-immigration et anti-mondialisation;
- les fausses histoires sur des crimes de guerre commis par les FAC;
- la désinformation sur les alliés de l'OTAN;
- les fausses allégations selon lesquelles les États-Unis ont établi des laboratoires d'armement biologique en Ukraine.

Le CST a déclassifié des observations importantes provenant de ses rapports de renseignement afin d'exposer publiquement ces fausses assertions. En avril 2022, le CST a dévoilé aux Canadiens ces exemples sur les médias sociaux et a fourni des ressources permettant de détecter toute désinformation.

Attributions

Le CST collabore avec Affaires mondiales Canada (AMC) et d'autres partenaires fédéraux et internationaux pour dénoncer des comportements irresponsables dans le cyberespace. Le CST prend part à ces attributions en se fondant sur son expertise en cybersécurité et son analyse du renseignement.

En avril 2021, le Canada s'est joint à ses alliés pour attribuer la responsabilité de la cybercompromission de SolarWinds[11] à un auteur de menace parrainé par la Russie. L'auteur de menace a compromis des milliers de réseaux dans le monde en installant un maliciel par l'intermédiaire de mises à jour de programme. Il a par la suite ciblé certaines de ces victimes à des fins de cyberespionnage.

En juillet 2021, le Canada s'est joint à ses alliés pour attribuer la responsabilité de l'exploitation « sans précédent et sans discernement » des serveurs de Microsoft Exchange[12] à des auteurs de menace parrainés par la République populaire de Chine. Cette compromission a touché environ 400 000 serveurs dans le monde et a permis aux auteurs de menace de voler de la propriété intellectuelle et une grande quantité de renseignements personnels.

Tel que mentionné précédemment, en janvier et en février 2022, le Centre pour la cybersécurité a uni sa voix à celles des alliés américains et britanniques, et lancé un avis[13] et un rappel[14] aux organisations canadiennes au sujet des cybermenaces connues parrainées par la Russie qui ciblaient les infrastructures essentielles.

Renseignement électromagnétique étranger

À titre d'organisme de renseignement électromagnétique étranger du Canada, le CST intercepte et analyse des communications électroniques et d'autres types de transmissions étrangères afin d'informer le gouvernement du Canada sur les activités d'entités étrangères qui cherchent à compromettre la prospérité et la sécurité nationale du Canada. (La loi interdit au CST de cibler les communications des Canadiens, peu importe où ils se trouvent, ainsi que des personnes se trouvant au Canada.) Le SIGINT du CST contribue également à l'établissement de politiques gouvernementales dans les domaines de la défense, de la sécurité et des affaires internationales.

Menaces basées à l'étranger

Cette année, le CST a produit des rapports concernant une variété de menaces basées à l'étranger, entre autres :

- des activités menées par des États hostiles, dont des cybermenaces;
- la cybercriminalité;
- l'espionnage ciblant le Canada, dont l'espionnage économique;
- les campagnes de désinformation et d'ingérence étrangère;
- l'enlèvement de Canadiens à l'étranger;
- le terrorisme et l'extrémisme, dont l'extrémisme violent à caractère idéologique (EVCI);
- les menaces ciblant des Canadiens et des forces canadiennes à l'étranger.

Cette année, le CST a contribué à des opérations militaires canadiennes à l'étranger, dont les opérations IMPACT, UNIFIER et REASSURANCE, et a fourni du renseignement et de l'assistance afin d'aider les forces canadiennes déployées à l'étranger.

Le renseignement électromagnétique étranger du CST a aussi permis à AMC et aux FAC d'évacuer par pont aérien des Canadiens de Kaboul après la reprise de l'Afghanistan par les talibans en août 2021.

Rapports de renseignement étranger du CST pour l'année 2021-2022

3202
rapports

1686
clients

27
ministères et organismes

Assistance offerte à des partenaires fédéraux et dans le cadre d'opérations militaires

Cette année, le CST a continué de remplir le volet de son mandat qui consiste à offrir une assistance technique et opérationnelle aux partenaires fédéraux responsables de la sécurité, de la défense et de l'application de la loi, c'est-à-dire :

- la Gendarmerie royale du Canada (GRC);
- le Service canadien du renseignement de sécurité (SCRS);
- l'Agence des services frontaliers du Canada (ASFC);
- les Forces armées canadiennes (FAC) et le ministère de la Défense nationale (MDN).

Collaboration avec des partenaires internationaux

Le Canada fait partie de la collectivité des cinq, qui comprend aussi les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. Le Canada tire de grands avantages de cette alliance stratégique qui perdure depuis des décennies. Elle permet une coopération et des échanges de renseignement portant sur des intérêts communs très importants. Le CST collabore très étroitement avec les autres organismes de la collectivité des cinq pour répondre à une grande variété de priorités concernant la défense, la sécurité et les affaires étrangères, et le renseignement obtenu grâce à ces partenariats profite grandement au gouvernement du Canada. Le CST maintient en outre des relations de collaboration avec d'autres organismes SIGINT et de cyberdéfense dans le monde.

Le CST, en collaboration avec ses alliés, promeut et respecte les normes concernant les comportements responsables à adopter dans le cyberespace, et a dénoncé des intervenants qui ont violé ces normes (consulter la section Attributions).

> La Russie, la Chine et l'Iran sont fort probablement responsables de la plupart des activités de cybermenace parrainées par des États et menées contre des processus démocratiques partout dans le monde.
>
> **Centre canadien pour la cybersécurité**
> *Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021*[15]

Surveillance des menaces ciblant les processus démocratiques du Canada

Le secteur du renseignement électromagnétique du CST a contribué à des évaluations des menaces, dont la mise à jour de juillet 2021 de l'évaluation des cybermenaces contre le processus démocratique du Canada publiée par le Centre pour la cybersécurité.

Selon le rapport, bien que le Canada constitue une cible de priorité moindre par rapport à d'autres pays, il est toujours « très probable que les électeurs canadiens soient victimes de cyberingérence étrangère » à l'approche des élections fédérales de 2021 et durant les élections.

À titre de membre du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (MSRE), le CST a surveillé les menaces visant les élections générales de 2021, en collaboration avec ses partenaires du Groupe de travail sur les MSRE, c'est-à-dire le SCRS, la GRC et AMC. Durant cet effort, le CST a remis du renseignement sur les intentions, les activités et les capacités d'auteurs de menace étrangers.

De plus, grâce aux pouvoirs liés aux cyberopérations qu'il détenait, le CST avait la possibilité d'interrompre toute cyberactivité malveillante ciblant l'infrastructure d'Élections Canada, au besoin (consulter la section Protection de la démocratie).

Parallèlement, le Centre pour la cybersécurité a collaboré avec Élections Canada et les partis politiques enregistrés afin de mettre à leur disposition un service d'assistance en cybersécurité (consulter la section Protection des institutions démocratiques).

Cyberopérations **étrangères**

Le volet touchant les cyberopérations étrangères a nouvellement été ajouté au mandat du CST, plus précisément lors de l'adoption de la *Loi sur le CST* en 2019. Grâce à ces pouvoirs, le Canada peut contrer toute cyberactivité que mène un adversaire étranger et qui se rapporte aux affaires internationales, à la défense ou à la sécurité du Canada.

Ces pouvoirs concernent les cyberopérations défensives (COD) et les cyberopérations actives (COA), et permettent au Canada d'agir en fonction de ce que le CST apprend dans le cadre de ses missions SIGINT et de cybersécurité.

Il est à noter que la *Loi sur le CST* interdit à l'organisme de faire ce qui suit :

- cibler des Canadiens ou des personnes se trouvant au Canada;
- causer la mort ou une lésion corporelle;
- contrecarrer le cours de la justice;
- contrecarrer le cours de la démocratie.

Le ministre de la Défense nationale peut uniquement autoriser une COD ou une COA s'il conclut ce qui suit :

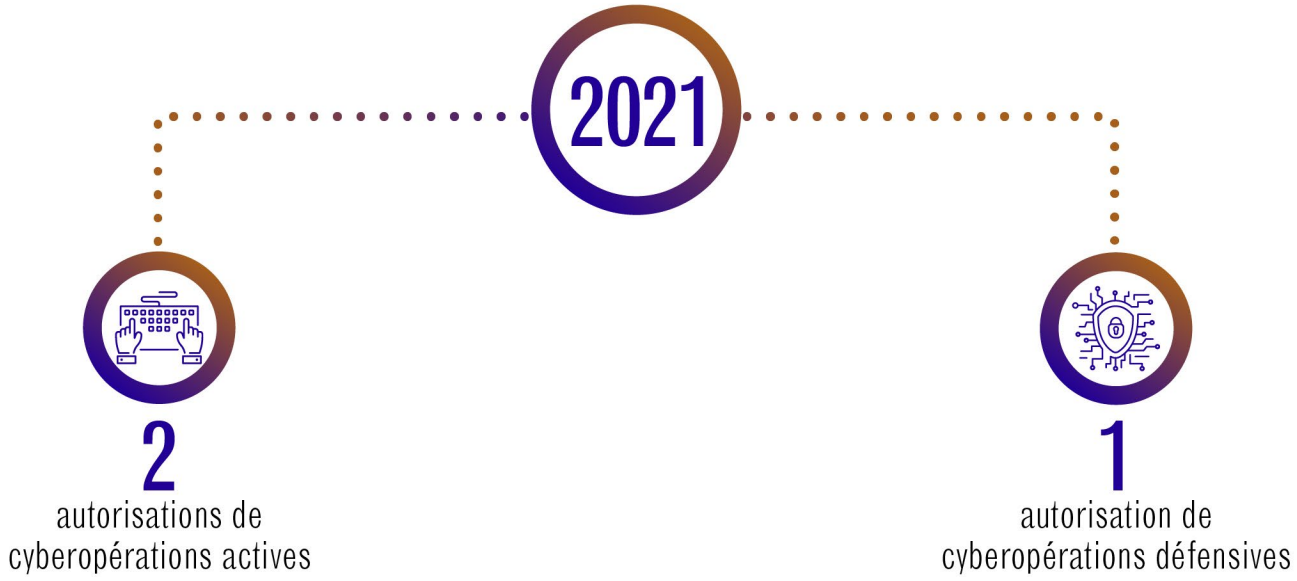
- l'activité est raisonnable;
- l'activité est proportionnelle;
- l'objectif ne pourrait pas raisonnablement être atteint d'une autre manière;
- aucune information ne sera acquise.

Le ministre d'AMC doit consentir aux cyberopérations actives et doit être consulté concernant les cyberopérations défensives.

À l'instar de toute activité réalisée par le CST, les cyberopérations étrangères sont examinées au nom des Canadiens par des organes de surveillance externes et indépendants. Ces derniers produisent des rapports publics et non classifiés faisant état de leurs conclusions. Pour en savoir plus sur la coopération entre le CST et ces organes de surveillance, consultez la section Redditions de comptes du présent rapport.

Autorisations de cyberopérations étrangères

En 2021, le ministre de la Défense nationale a délivré trois autorisations de cyberopérations étrangères.[16]



Chaque autorisation est valide pour une durée maximale d'un an. Plusieurs opérations étrangères peuvent être réalisées dans le cadre d'une seule autorisation. Or, dans certains cas, une autorisation peut être de nature préventive et n'engendrer finalement aucune opération. L'autorisation de COD qui a pour objectif de protéger les élections fédérales canadiennes en est un exemple (voir ci-dessous).

Exemples de cyberopérations étrangères

Un rapport non classifié permet uniquement de fournir de l'information limitée concernant les cyberopérations étrangères que mène le CST. Toutefois, dans un souci de transparence, nous avons expurgé des exemples de cyberopérations étrangères réalisées par le CST ou ayant été autorisées dans le passé. Comme il est délicat de discuter d'opérations en cours, ces exemples ne concernent pas nécessairement la présente année financière.

Perturbation d'activités extrémistes étrangères

Le CST s'est servi de ses capacités de COA pour perturber les efforts d'extrémistes basés à l'étranger qui visaient les objectifs suivants :

- recruter des ressortissants canadiens;
- mener des opérations en ligne;
- diffuser du matériel extrémiste violent.

Mesures visant à contrer la cybercriminalité

L'utilisation de rançongiciels et le vol de renseignements personnels par des cybercriminels sont néfastes pour le Canada et les Canadiens. Ainsi, le CST a entrepris une campagne à long terme pour réduire la capacité des groupes cybercriminels à cibler des Canadiens ainsi que des institutions et des entreprises canadiennes.

Grâce à sa collaboration avec des partenaires canadiens et alliés, le CST a contribué à réduire la capacité des cybercriminels à lancer des attaques par rançongiciel et à bénéficier de la vente de renseignements volés.

> Nous estimons que les attaques par rançongiciel continueront de poser une menace pour la sécurité nationale et la prospérité économique du Canada et de ses alliés tout au long de 2022, car il s'agit d'activités lucratives pour les cybercriminels.
>
> **Centre canadien pour la cybersécurité**
> *La menace des rançongiciels en 2021*[17], *décembre 2021*

Protection de la démocratie

Le CST dispose de capacités et d'un mandat juridique lui permettant d'interrompre des cyberactivités malveillantes qui menacent les processus démocratiques du Canada. À l'approche des élections fédérales canadiennes de 2021, le CST disposait de pouvoirs de cyberopérations défensives lui donnant les moyens de protéger l'infrastructure électronique employée par Élections Canada. En cas de cyberactivités malveillantes ciblant le processus électoral, le CST aurait ainsi été prêt à intervenir immédiatement.

Assistance offerte aux FAC

Le CST a également eu recours à ses capacités de cyberopérations actives pour aider les FAC dans le cadre de leur mission.

Sécurité des communications (COMSEC)

Le CST a le mandat de sécuriser les communications sensibles du gouvernement du Canada.

Il met par exemple à la disposition des ministres et des hauts fonctionnaires des dispositifs leur permettant de sécuriser leurs communications partout où ils se trouvent. Cette fonction s'est avérée plus importante que jamais durant la pandémie. En février 2021, le CST a établi un partenariat avec le Bureau du Conseil privé (BCP) et Services partagés Canada (SPC) pour sécuriser la fonction vidéo et ainsi répondre au besoin qu'avaient les intervenants de tenir des rencontres virtuelles de niveau classifié.

La demande pour ce type de services a continué d'augmenter cette année. Le CST a poursuivi sa collaboration avec ses partenaires afin de soutenir et d'accroître la fonctionnalité de ces services essentiels, ce qui comprend la mise à niveau du matériel et l'accroissement de l'accès aux systèmes.

Il a également continué de gérer le Réseau canadien Très secret (RCTS). Comme en témoigne le nom, il s'agit d'un réseau qui permet aux ministères, aux organismes et aux entrepreneurs autorisés du gouvernement du Canada de stocker et de transmettre de l'information classifiée Très secret. Cette année, le CST a piloté l'initiative des trousses déployables du RCTS qu'il a remises à un nombre limité de ministères clients. Ces trousses facilitent le déploiement de la connectivité du RCTS sur le terrain lorsqu'une installation temporaire est requise par un ministère.

La sécurisation des communications repose sur une cryptographie forte permettant de protéger l'information et de mettre les systèmes à l'abri des cybermenaces.

Dans la dernière année, le CST a contribué à sécuriser les données du gouvernement du Canada en prenant les mesures suivantes :

- offrir des outils, des dispositifs et une expertise cryptographiques;
- mettre en œuvre de nouvelles procédures cryptographiques;
- conseiller le gouvernement et les industries sur l'utilisation de la cryptographie et de nouvelles techniques cryptographiques, par exemple :
  - → les algorithmes post-quantiques (consulter la section Préparation à l'avenir post-quantique);
  - → le chiffrement homomorphe.

Le CST a contribué à renforcer l'assurance par rapport aux produits de TI employés par les organisations canadiennes en faisant ce qui suit :

- certifier les produits de TI commerciaux conformément aux normes internationales en :
  - → cryptographie (Programme de validation des modules cryptographiques)[18];
  - → cybersécurité (Critères communs)[19].
- participer à des organismes de normalisation internationaux.

Il a en outre publié de l'orientation sur le chiffrement à l'intention des Canadiens et des organisations canadiennes :

- Utiliser le chiffrement pour assurer la sécurité des données sensibles[20].

Cybersécurité : **institutions fédérales**

Le Centre pour la cybersécurité du CST est chargé des opérations visant à protéger le gouvernement du Canada contre les cybermenaces, comme les rançongiciels et le cyberespionnage. Il travaille de concert avec des partenaires fédéraux, dont SPC et le Secrétariat du Conseil du Trésor (SCT), pour défendre les réseaux et l'information des institutions fédérales, dont les ministères et les organismes gouvernementaux et les sociétés d'État. Dans le présent rapport, le terme *ministères* englobe les ministères et les organismes.

Défense par couches

Le Centre pour la cybersécurité fait appel à des capteurs autonomes pour détecter toute cyberactivité malveillante sur les réseaux, les systèmes et les infrastructures infonuagiques du gouvernement. Les trois types de capteurs suivants sont déployés : les capteurs au niveau du réseau, les capteurs au niveau du nuage et les capteurs au niveau de l'hôte[21] (sur les ordinateurs portatifs, les ordinateurs de bureau et les serveurs).

Ces capteurs recueillent en toute sécurité des données système et les transmettent au Centre pour la cybersécurité aux fins d'analyse. Des partenaires liés aux infrastructures essentielles, dont des provinces et des territoires, nous envoient également des données techniques tirées de journaux de sécurité de système. Nous pouvons ainsi les protéger et améliorer nos analyses pour le gouvernement du Canada et d'autres partenaires. Des contrôles de protection de la vie privée stricts encadrent ces processus.

Nos outils automatisés et nos analystes spécialisés recherchent des données inhabituelles. Si des activités malveillantes sont détectées, des mesures sont prises pour les contrecarrer. On peut par exemple diriger les capteurs pour qu'ils les bloquent automatiquement.

Les mesures de défense automatisées protègent le gouvernement du Canada contre des activités malveillantes, plus précisément entre trois et cinq milliards d'activités chaque jour; ce chiffre a même déjà atteint sept milliards. Ces activités comptent ce qui suit :

- des tentatives de mappage des systèmes et des réseaux;
- des tentatives d'extraction de l'information de bases de données;
- des domaines malveillants (noms de sites Web et adresses de courriel);
- des adresses IP malveillantes (le code unique identifiant un ordinateur ou un dispositif sur Internet).

Tous les ministères faisant partie du périmètre réseau des services Internet d'entreprise de SPC profitent de cette protection. Cette année, le Centre pour la cybersécurité a aussi déployé des capteurs au niveau de l'hôte afin de fournir un soutien en matière de cyberincidents aux exploitants d'infrastructures essentielles du Canada.

En mars 2022 :

- 70 institutions fédérales avaient déployé nos capteurs au niveau du nuage;
- 79 institutions fédérales avaient déployé des capteurs au niveau de l'hôte sur plus de 730 000 hôtes.

Protection des sociétés d'État

Les sociétés d'État font partie des institutions fédérales et sont donc comprises dans le volet du mandat du CST touchant la cybersécurité. Toutefois, elles fonctionnent indépendamment du gouvernement du Canada et sont responsables de la gestion de leurs propres infrastructures de TI. Chaque société d'État est libre de choisir le niveau de soutien qu'elle souhaite obtenir par rapport aux services offerts aux partenaires des infrastructures essentielles (consulter la section Services de cybersécurité). Certaines sont admissibles à l'ensemble des services auxquels ont droit les ministères principaux du gouvernement.

En février 2022, le Comité des parlementaires sur la sécurité nationale et le renseignement a publié un rapport sur les mesures de cyberdéfense du gouvernement du Canada. Bien que le Comité ait reconnu que le Canada représentait « un chef de file mondial en défense de ses réseaux contre les cyberattaques »[22], il a noté que bon nombre des sociétés d'État n'avaient pas choisi de se prévaloir des services de cyberdéfense offerts par le gouvernement du Canada, ce qui posait un risque élevé pour leurs données. Le rapport recommandait donc que le gouvernement étende ses services de cyberdéfense avancés, y compris les capteurs de cyberdéfense du CST, à l'ensemble des organismes fédéraux. Le gouvernement du Canada s'est dit en accord avec la recommandation et le CST explore les options à mettre en œuvre.

> Pour le Comité, les conséquences de ce choix sont claires : refuser les services de cyberdéfense du gouvernement équivaut à choisir de rendre les données et l'intégrité des systèmes vulnérables aux cybermenaces les plus avancées du monde.
>
> **Comité des parlementaires sur la sécurité nationale et le renseignement**
> *Rapport spécial portant sur le cadre de travail et les activités du gouvernement du Canada visant à défendre ses systèmes et ses réseaux contre les cyberattaques*[23], *février 2022*

Ces services s'ajoutent aux services de cybersécurité qu'offre le Centre pour la cybersécurité aux partenaires liés aux infrastructures essentielles, dont les sociétés d'État. En avril 2021, le Centre pour la cybersécurité a établi un point de contact dédié aux sociétés d'État. Durant l'année, nous avons communiqué avec toutes les sociétés d'État pour nous assurer qu'elles étaient au courant de la grande variété de services à leur disposition ainsi que des avantages potentiels sur le plan de leur cybersécurité. À la suite de cette communication, des dizaines d'autres organisations se sont inscrites aux services du Centre pour la cybersécurité. Des sociétés d'État ont haussé leur niveau de service cette année pour qu'il équivaille à celui des ministères gouvernementaux principaux.

Gestion des incidents

La nature de la cybersécurité veut que même les meilleures défenses n'empêchent pas les cyberincidents.

Le Centre pour la cybersécurité fournit un soutien en permanence pour contenir la menace et atténuer les dommages lorsque des cyberincidents touchent des institutions fédérales ou des systèmes d'importance pour le gouvernement du Canada.

Cette année, le Centre pour la cybersécurité a ouvert 2023 cas concernant des incidents de cybersécurité. Ce nombre représente une moyenne de 5,5 incidents par jour. Parmi ces cas, 1154 incidents visaient des institutions fédérales et 869 ciblaient des infrastructures essentielles.

Ces types d'incidents comprennent ce qui suit :

- les activités de reconnaissance menées par des auteurs de menace dotés de techniques sophistiquées;
- les incidents d'hameçonnage (courriels contenant des maliciels);
- les accès non autorisés à des environnements de TI organisationnels;
- les attaques imminentes par rançongiciel;
- les exploits de jour zéro (exploitation de vulnérabilités critiques dans des logiciels n'ayant pas fait l'objet de correctifs).

Selon la nature et la gravité des cas, l'équipe responsable de la gestion des incidents offre les services suivants :

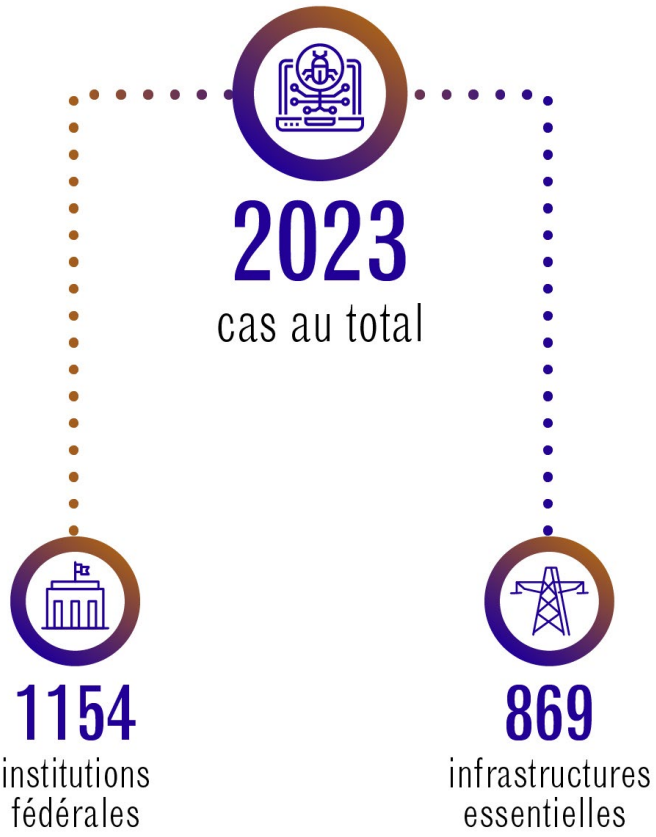
- des messages d'alerte aux victimes;
- des conseils et de l'orientation adaptés;
- une assistance aux fins de reprise des activités;
- des rapports d'analyse;
- des services de criminalistique numérique.

Ces services sont offerts en tout temps. Cette année, le Centre pour la cybersécurité a également proposé un service d'assistance et de coordination pour les interventions en cas d'incidents en vue d'événements importants prévus, dont les suivants :

- les élections fédérales canadiennes de 2021;
- le recensement canadien de 2021;
- la vaccination contre la COVID-19.

> **Cyberincident :** Toute tentative non autorisée, réussie ou non, d'avoir accès à une ressource informatique ou à un réseau, de le modifier, de le détruire, de le supprimer ou de le rendre inutilisable.
>
> **Centre canadien pour la cybersécurité**
> *Glossaire*[24]

Cas concernant des incidents de cybersécurité pour l'année 2021-2022



Étude de cas : Vulnérabilité Apache Log4j

En décembre 2021, une vulnérabilité de jour zéro dans un produit logiciel utilisé à grande échelle a permis la compromission d'organisations partout dans le monde. Il s'agit de la vulnérabilité Apache Log4j.

Des auteurs de menace pouvaient donc accéder à des dispositifs vulnérables à distance pour voler de l'information, dont des mots de passe et des justificatifs d'identité, ou pour infecter des réseaux au moyen de codes malveillants.

Les équipes du Centre pour la cybersécurité sont rapidement intervenues pour en aviser les partenaires gouvernementaux et les organisations canadiennes. Huit alertes ont été publiées au total.

Le Centre pour la cybersécurité a coordonné la réponse fédérale pour s'assurer que les autres ministères gouvernementaux et les exploitants d'infrastructures essentielles étaient au courant de la menace et savaient comment l'atténuer.

Grâce aux données provenant de nos capteurs au niveau de l'hôte, nous avons pu cerner les dispositifs vulnérables et aider rapidement les équipes de TI des ministères dans leurs efforts pour rétablir leurs activités.

Des analystes du Centre pour la cybersécurité ont déterminé les domaines et les adresses IP associés à la vulnérabilité et les ont bloqués au périmètre réseau.

Cette cybervulnérabilité aurait pu avoir de graves conséquences. Grâce à nos outils de défense automatisés, à nos spécialistes qualifiés ainsi qu'à notre étroite collaboration avec les équipes de TI de SPC, du SCT et de nombreux autres ministères du gouvernement du Canada, la menace a été contenue et neutralisée avant que des dommages importants soient causés.

Collaboration avec des partenaires

Le Centre pour la cybersécurité n'agit jamais seul. Il coordonne ses activités avec des partenaires fédéraux, internationaux et des industries.

À titre d'équipe nationale d'intervention en cas d'incident lié à la sécurité informatique (CSIRT), le Centre pour la cybersécurité met en commun de l'information et de l'expertise avec d'autres CSIRT nationales partout dans le monde. Les CSIRT de chaque pays peuvent ainsi aviser les victimes et résoudre les incidents rapidement.

À l'automne 2021, le Centre pour la cybersécurité et ses partenaires fédéraux ont officialisé la formation d'un groupe opérationnel pour accroître la coordination des interventions en cas de cyberincidents qui pourraient engendrer des répercussions sur le plan de la sécurité nationale. L'Unité de cyberincident nationale se compose d'équipes :

- du CST;
- des FAC;
- du SCRS;
- de la GRC;
  - → de l'Unité nationale de coordination contre la cybercriminalité (NC3);
  - → de services de police fédéraux.

Retrait d'éléments d'usurpation

Des cybercriminels créent de faux sites Web, domaines de courrier informatique et profils de médias sociaux pour essayer de piéger des Canadiens afin qu'ils donnent leurs renseignements personnels ou cliquent sur des liens compromis.

Lorsque ces éléments se font passer pour des ministères ou des représentants du gouvernement, cela a pour effet de miner la confiance du public dans les vraies sources et d'exposer des Canadiens à des arnaques potentielles.

Du début de la pandémie au 31 mars 2022, le Centre pour la cybersécurité a coopéré avec des partenaires de l'industrie de confiance et des alliés internationaux pour retirer plus de 11 500 faux domaines.

Cybersécurité : **infrastructures essentielles**

Le CST a pour mandat de contribuer à l'amélioration de la cyberrésilience des infrastructures essentielles canadiennes. Il s'agit d'une priorité pour le Centre pour la cybersécurité, et la majeure partie de ses efforts cette année ont d'ailleurs visé l'approfondissement et l'élargissement des partenariats avec les exploitants des infrastructures essentielles.

On entend par *infrastructures essentielles* les services qui sont absolument nécessaires, comme les soins de santé, l'énergie, les finances et les communications. Elles constituent des cibles lucratives pour les groupes criminels misant sur les rançongiciels.

Les infrastructures essentielles sont également ciblées par des auteurs de cybermenace parrainés par des États qui peuvent s'intéresser à des actifs d'infrastructures essentielles dans le but de disposer d'un levier géopolitique. Au début de 2022, le Centre pour la cybersécurité a publié deux avis sur les cybermenaces[25] pour informer les exploitants d'infrastructures essentielles d'activités de cybermenace connues parrainées par la Russie.

Si le CST est au courant d'une cybermenace, par l'intermédiaire du renseignement électromagnétique étranger qu'il recueille ou des activités de cyberdéfense du gouvernement, il transmet l'information au plus grand nombre de fournisseurs d'infrastructures essentielles de confiance possible.

> **En 2021, on a signalé au Centre pour la cybersécurité 304 incidents liés à des rançongiciels ciblant des Canadiens, dont la moitié des victimes avaient un lien avec des infrastructures essentielles. Nous savons toutefois que les cyberincidents sont très peu déclarés et que le nombre réel de victimes est de beaucoup supérieur.**
>
> **Sami Khoury**
> *Dirigeant principal du Centre canadien pour la cybersécurité*

Étude de cas : Soutien offert à la province de Terre-Neuve-et-Labrador

À l'automne 2021, le système de soins de santé de Terre-Neuve-et-Labrador a fait l'objet d'un grave cyberincident. Des milliers d'interventions médicales ont dû être annulées et il y a eu compromission de milliers de dossiers de patients[26].

Le Centre pour la cybersécurité a travaillé étroitement avec la province et ses partenaires fédéraux pour coordonner la portion TI des mesures à prendre. Il a par exemple déployé une équipe sur place pour qu'elle offre un soutien concret en cybersécurité. Dans les derniers mois, le Centre pour la cybersécurité a conféré les services suivants :

- offrir du soutien sur place (trois semaines);
- fournir de l'assistance à distance;
- donner des avis et des conseils adaptés;
- offrir des services de criminalistique numérique;
- offrir de l'assistance aux fins d'atténuation (reprise des activités);
- communiquer de l'information;
- produire des rapports d'analyse;
- donner des conseils sur la reconstruction de l'infrastructure.

Grâce au financement prévu dans le Budget 2022, le Centre pour la cybersécurité sera plus à même d'apporter ce type d'aide en cas de cyberincidents engendrant de grandes répercussions sur les infrastructures essentielles du Canada.

Secteurs clés

Cette année, le Centre pour la cybersécurité a coopéré avec environ 1000 partenaires liés aux infrastructures essentielles provenant de différents secteurs, dont les suivants :

- le milieu universitaire;
- des sociétés d'État;
- des institutions démocratiques;
- le secteur de l'énergie;
- le secteur des finances;
- le secteur de la santé;
- le secteur des technologies de l'information et des communications;
- des provinces, des territoires et des municipalités;
- de petites et moyennes entreprises;
- le secteur des transports.

*Remarque : Le terme « municipalités » comprend certains services municipaux, dont les services de police et d'incendie et les services d'approvisionnement en eau.

Services de cybersécurité

Le Centre pour la cybersécurité encourage les partenaires liés aux infrastructures essentielles admissibles à se prévaloir des services de cybersécurité gratuits et confidentiels qu'il offre, notamment les suivants :

- la gestion des incidents;
- la prestation de renseignement sur les menaces;
  - → des alertes en cas de cybermenaces (et les mesures d'atténuation connexes);
  - → des résumés hebdomadaires sur les incidents;
  - → des informations régulières sur les cybermenaces;
  - → des avertissements concernant des activités malveillantes sur leur espace IP;
- un accès à sa plateforme d'analyse de maliciels;
- un accès à son flux automatisé de renseignements sur les menaces;
- un service de coopération et de sensibilisation de la collectivité propre à chaque secteur;
- un point de contact désigné au Centre pour la cybersécurité.

Nos services ne remplacent pas les solutions commerciales, mais les informations fiables et les conseils spécialisés que nous offrons aident les fournisseurs des infrastructures essentielles à personnaliser les mesures de cyberdéfense qu'ils adoptent. Les partenaires peuvent choisir le niveau de service qui répond le plus à leurs besoins ou peuvent communiquer avec le Centre pour la cybersécurité afin d'obtenir des avis et des conseils, au besoin.

Plateforme d'analyse de maliciels

Assemblyline[27] est la plateforme de détection et d'analyse de maliciels du Centre pour la cybersécurité. Des analystes y soumettent des fichiers suspects et Assemblyline les vérifie en se fondant sur la base de données unique sur les cybermenaces du Centre pour la cybersécurité. Si un élément est malveillant, Assemblyline présente des détails sur le type de maliciel afin de guider les mesures à prendre.

Au départ, Assemblyline pouvait uniquement être utilisé dans l'enceinte du CST sur le réseau classifié et servait à défendre le gouvernement du Canada contre les cybermenaces. Or, avec les années, il a été possible d'offrir cet outil à l'externe pour que d'autres défenseurs de la cybersécurité puissent en tirer profit.

La première version du logiciel pour Assemblyline du CST date de 2017; d'autres intervenants ont pu construire leurs propres plateformes en se basant sur le code fourni. Plus de 3000 organisations ont téléchargé ces versions d'Assembly à créer soi-même. Le Centre pour la cybersécurité a depuis recréé Assemblyline de toutes pièces.

Assemblyline 4[28], qui est la plus récente version, est compatible avec le nuage. Il présente une nouvelle base de données, une nouvelle interface utilisateur et de nouvelles capacités de détection de maliciels. Il est accessible en tant que logiciel de source ouverte depuis janvier 2020 et sa mise en œuvre sur notre réseau classifié est terminée depuis février 2022.

Entretemps, nous avons créé deux nouvelles plateformes Assemblyline pouvant être utilisées gratuitement par nos partenaires externes : une pour la clientèle gouvernementale et l'autre pour les partenaires liés aux infrastructures essentielles. Ces deux plateformes sont le fruit d'investissements importants réalisés dans notre infrastructure TI durant la pandémie. Grâce au travail préparatoire mené dans le cadre de ces efforts, nous pouvons maintenant offrir un nombre accru de services au niveau non classifié et au niveau Protégé B (une classification de sécurité[29] intermédiaire).

Désormais, plutôt que de transmettre par courriel des fichiers au Centre pour la cybersécurité et attendre plusieurs jours pour obtenir une analyse manuelle, les partenaires externes se connectent simplement à leur compte, soumettent des fichiers suspects aux fins d'analyse et obtiennent un résultat en quelques minutes.

Sommaire d'Assemblyline 4

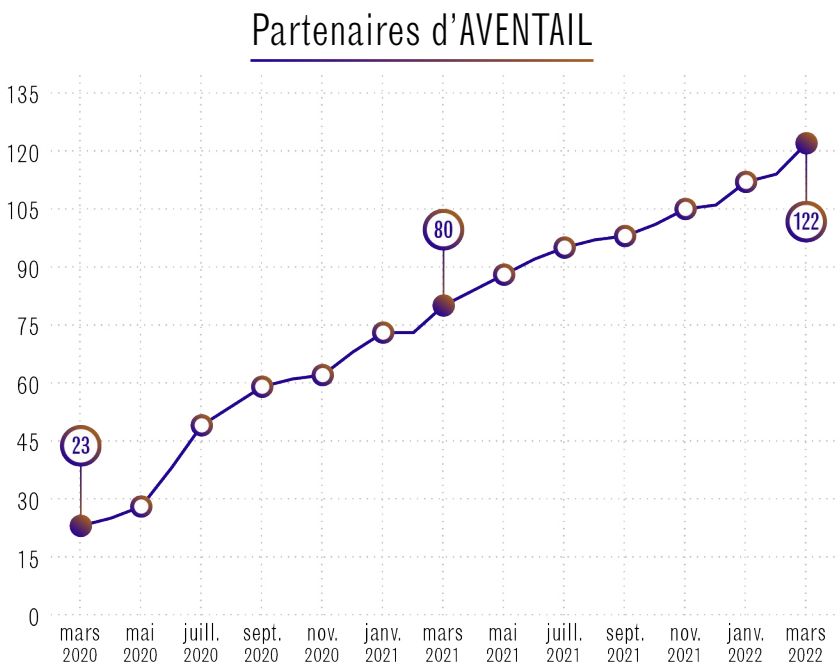
Date	Format	Auditoire	Classification	Nombre d'organisations
Janvier 2020	Logiciel de source ouverte	Pour tout le monde	Non classifié	Aucun suivi
Juillet 2020	Plateforme externe	Clientèle gouvernementale	Protégé B	32 ministères
Mars 2021	Plateforme externe	Infrastructures essentielles	Non classifié	133 organisations
Février 2022	Mise à niveau – plateforme interne	Défenseurs de la cybersécurité du CST	Classifié	Aucun client externe

Flux automatisé de renseignements sur les menaces

Aventail est le service de diffusion automatisée de renseignements sur les menaces du Centre pour la cybersécurité. Il met à la disposition des partenaires liés aux infrastructures essentielles de l'information pertinente et vérifiée sur les indicateurs de compromission extrêmement rapidement. Les indicateurs de compromission sont des détails sur les cybermenaces, par exemple :

- les domaines et les URL (éléments d'adresses Web);
- les adresses IP (codes numériques qui identifient les dispositifs sur Internet).

Des défenseurs de la cybersécurité ont recours aux indicateurs de compromission pour prévenir et atténuer toute activité malveillante sur leurs réseaux. Cette année, Aventail a transmis 46 965 indicateurs de compromission uniques. Il s'agit d'une moyenne quotidienne de 129 indicateurs de compromission.



Depuis 2017, le CST transmet son flux de renseignements sur les menaces aux ministères du gouvernement du Canada et à ses partenaires de la collectivité des cinq. En mars 2020, le Centre pour la cybersécurité a lancé Aventail pour pouvoir transmettre directement l'information à ses partenaires liés aux infrastructures essentielles. Cette année, la clientèle d'Aventail est passée de 80 à 122 partenaires liés aux infrastructures essentielles.

Le Centre pour la cybersécurité met aussi Aventail à la disposition de CIRA (l'Autorité canadienne pour les enregistrements Internet) afin d'améliorer le Bouclier canadien, dont l'objectif est de bloquer les menaces.

Aventail s'inscrit dans la stratégie du Centre pour la cybersécurité qui vise à créer des outils et à établir des partenariats qui améliorent la cybersécurité au Canada.

Protection de l'infrastructure énergétique du Canada

En février 2021, le premier ministre du Canada et le président des États-Unis ont annoncé une feuille de route pour un partenariat renouvelé États-Unis–Canada[30], comportant un engagement à accroître la cyberrésilience de l'infrastructure énergétique transfrontalière conjointe. Cette année, le Centre pour la cybersécurité a poursuivi sa collaboration avec ses partenaires américains et canadiens en vue de répondre à cette priorité stratégique conjointe.

Par exemple, en août 2021, Ressources naturelles Canada a annoncé le financement fédéral du Programme de la flamme bleue[31]. Il s'agit d'un partenariat bilatéral d'échange d'information entre le Centre pour la cybersécurité et l'Association canadienne du gaz (ACG).

Les organisations participantes ont la possibilité de transmettre les données de leur réseau au Centre pour la cybersécurité aux fins d'analyse. Le Centre peut ainsi brosser un tableau précis des menaces qui guettent le secteur du gaz naturel. En retour, le Centre pour la cybersécurité peut transmettre des renseignements sur les menaces selon les besoins de chacun des membres de l'ACG.

Le partenariat avec l'ACG suit un modèle établi entre le Centre pour la cybersécurité et la Société indépendante d'exploitation du réseau d'électricité (SIERE) de l'Ontario, qui s'inscrit dans l'initiative Lighthouse[32] (en anglais seulement) de la SIERE. Les deux collaborations se poursuivent en 2022.

> **(La) probabilité qu'une cyberattaque puisse avoir un impact sur le secteur canadien de l'électricité est plus élevée qu'elle aurait pu l'être autrement en raison des liens qui existent entre les réseaux électriques américains et canadiens.**
>
> **Centre canadien pour la cybersécurité**
> *Cybermenaces contre le processus démocratique du Canada*[33], *novembre 2020*

Protection du secteur de la santé

Comme le mentionnait le rapport annuel du CST l'an dernier[34], les cybermenaces ciblant le secteur de la santé du Canada se sont accrues durant la pandémie, poussant même le Centre pour la cybersécurité à inscrire à ses services de cybersécurité plus de 100 nouveaux organismes de santé entre 2020 et 2021. La participation est demeurée forte cette année; environ 140 organismes ont régulièrement assisté aux séances virtuelles destinées à la collectivité de la santé.

En mars 2021, le Centre pour la cybersécurité a commencé un programme d'urgence visant à amplifier la cybersécurité entourant la vaccination contre la COVID-19 et la réponse à la pandémie. Le programme appelé Armure canadienne était ouvert à tous les organismes canadiens participant au développement ou à la livraison des vaccins contre la COVID-19.

Le Centre pour la cybersécurité a conclu un contrat avec CIRA afin d'offrir des licences à son service de pare-feu DNS. L'acronyme DNS signifie *Domain Name System* (système de noms de domaine). Ce système sert de répertoire Internet et permet de convertir les adresses Web lisibles pour un humain en adresses IP lisibles pour les machines. Ainsi, un pare-feu DNS protège les utilisateurs en les empêchant de se connecter à des sites Web malveillants connus.

Outre cette protection grâce au pare-feu DNS, les organismes de santé ont bénéficié des analyses du Centre pour la cybersécurité. En analysant le trafic DNS, le Centre pour la cybersécurité a détecté des domaines potentiellement malveillants qui étaient inconnus auparavant. Il en a avisé les organismes pour enquêter sur ces possibles compromissions et les atténuer, le cas échéant.

Neuf organismes ont pris part au programme, dont des hôpitaux, des autorités sanitaires et des fabricants biopharmaceutiques. La partie du programme relative aux licences a pris fin à la fin de mars 2022, mais les analyses du Centre pour la cybersécurité se poursuivent pour les organismes participants.

Protection des institutions démocratiques

Les élections fédérales canadiennes de 2021 ont eu lieu le 20 septembre 2021. S'appuyant sur l'expérience acquise par le CST lors d'élections antérieures, le Centre pour la cybersécurité a collaboré avec Élections Canada pour :

- veiller à la mise en place de mesures de cyberdéfense rigoureuses et efficaces afin de protéger les systèmes et les réseaux d'Élections Canada;
- préparer et mener des exercices de simulation basés sur la cybersécurité pour mettre à l'essai les processus de prise de décision et de coordination;
- assurer une gestion et une surveillance des cyberincidents durant la période électorale.

Le Centre pour la cybersécurité a communiqué avec les partis politiques fédéraux enregistrés pour déterminer leurs préoccupations principales en matière de cybersécurité. Il s'est fondé sur l'information obtenue pour leur présenter des conseils et de l'information sur les menaces qui répondent à leurs priorités.

Il a aussi travaillé de concert avec la Commission des débats des chefs et le Musée canadien de l'histoire (où se tenaient les débats des chefs) pour examiner leurs infrastructures TI et les conseiller sur le plan de la cybersécurité.

En dehors des périodes d'élections fédérales, le Centre a continué de coopérer avec le BCP pour renforcer les institutions démocratiques du Canada, dont :

- Élections Canada;
- les partis politiques fédéraux enregistrés;
- les autorités électorales provinciales et territoriales.

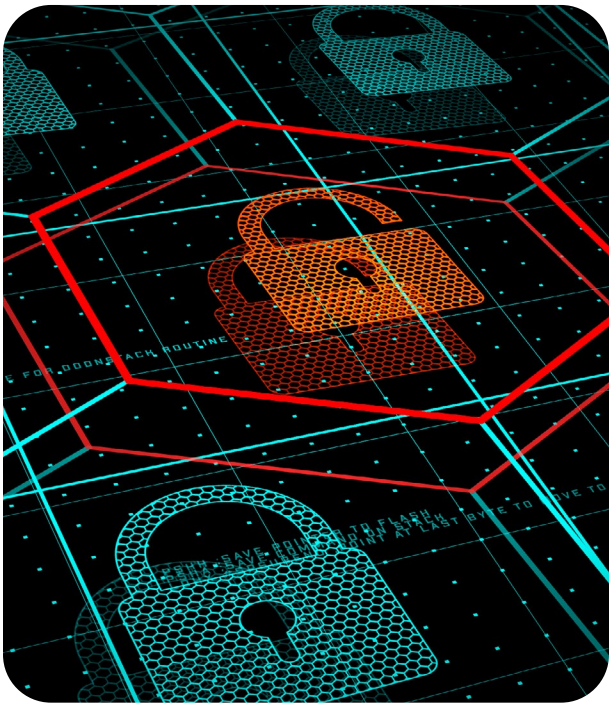
Le Centre a produit des conseils sur des sujets qui intéressent le secteur visé, y compris des documents d'orientation et un nouveau cours du Carrefour de l'apprentissage portant sur la cybersécurité pour les partis politiques[35].

Protection des Canadiens contre l'hameçonnage

Les tentatives d'hameçonnage se produisent malheureusement très souvent. Il s'agit en fait de messages non sollicités qu'envoient des cybercriminels pour tenter d'arnaquer des victimes par l'intermédiaire d'appels téléphoniques, de courriels, de messages directs sur les médias sociaux ou de messages textes (hameçonnage par message texte).

Le Centre pour la cybersécurité collabore avec certains partenaires des secteurs des télécommunications et des finances afin de protéger les Canadiens contre les activités d'hameçonnage et d'hameçonnage par message texte. Les partenaires concernés informent les autres partenaires des sites qui sont potentiellement malveillants. Chaque partenaire peut ensuite examiner et utiliser l'information en fonction de son mandat respectif. À titre d'exemple, le Centre pour la cybersécurité peut ajouter un site Web à sa liste de sites bloqués ou aviser les partenaires de l'industrie de confiance pour qu'ils retirent le site en question.

En septembre 2021, le Centre pour la cybersécurité a mis en œuvre un nouveau centre de mise en commun permettant de vérifier et de consigner automatiquement ces cybermenaces. Ainsi, les partenaires peuvent désormais atténuer ces cybermenaces extrêmement rapidement afin de protéger les Canadiens contre l'hameçonnage.



Sondage auprès de petites et moyennes organisations

À l'automne 2021, le Centre pour la cybersécurité et la Chambre de commerce de la Colombie-Britannique ont mené un sondage sur la cybersécurité auprès de petites et moyennes organisations canadiennes.[36] Selon les résultats :

- la plupart des entreprises (61 %) ont été victimes d'un incident de cybersécurité;
- seul le quart de ces victimes (26 %) ont signalé l'incident aux forces de l'ordre;
- la majorité des propriétaires d'entreprise (85 %) ne savaient pas que le gouvernement du Canada offrait une assistance en matière de cybersécurité aux petites et moyennes entreprises;
- plus de la moitié (52 %) des propriétaires d'entreprise ne savaient pas à qui s'adresser pour signaler un cybercrime.

À la suite du sondage, le Centre pour la cybersécurité a collaboré avec des partenaires fédéraux pour rédiger un document de sensibilisation concernant les ressources en matière de cybersécurité auxquelles ont accès les petites et moyennes entreprises[37]. Le Centre est aussi en voie de concevoir « Les cinq outils essentiels », un ensemble d'outils de base à l'intention des entreprises qui contient les mesures de cybersécurité minimales à adopter, lesquelles sont présentées sous forme d'aide-mémoire pratique.

Nouveau portail de signalement des cyberincidents

Depuis mai 2021, le Centre pour la cybersécurité offre une nouvelle fonction sur son site Web afin de faciliter le signalement de cyberincidents[38].

Le signalement de cyberincidents permet au Centre pour la cybersécurité d'assurer la sécurité des activités du Canada et des Canadiens en ligne, car il peut dresser un tableau précis du contexte de cybersécurité. Il se base sur cette information pour aiguiller ses avis, ses conseils et ses services.

Grâce au portail, les ministères du gouvernement, les exploitants d'infrastructures essentielles et les praticiens en TI peuvent signaler des incidents directement au Centre pour la cybersécurité. Selon les circonstances, il peut leur offrir des avis et des conseils.

Le portail dirige les Canadiens ainsi que les petites et moyennes organisations vers le partenaire compétent en fonction des différents types d'incidents. Par exemple, la GRC ou le service de police local mène des enquêtes sur les cybercrimes, alors que le Centre de notification des pourriels est chargé de recueillir les plaintes relatives aux courriels et aux messages textes non sollicités.

Renforcement de la **résilience numérique du Canada**

Le CST travaille à améliorer la résilience numérique générale du Canada en misant sur l'échange d'information ainsi que la prestation de conseils et de formation.

Transmission du flux de renseignements sur les menaces pour donner un avantage aux Canadiens

Le Centre pour la cybersécurité coopère avec des partenaires de confiance pour accroître la cybersécurité des Canadiens dans leur vie quotidienne. Le partenariat entre CIRA et le Centre pour la cybersécurité en est un excellent exemple.

Le Bouclier canadien[39] de CIRA est un service gratuit qui sert à protéger la vie privée des Canadiens lorsqu'ils mènent des activités sur leurs réseaux domestiques et leurs dispositifs personnels. Il offre en outre une option qui permet de bloquer les menaces en empêchant les utilisateurs de se connecter par inadvertance à des sites malveillants connus. Le Centre pour la cybersécurité communique son flux automatisé de renseignements sur les menaces à CIRA; toute menace détectée par le Centre sera ainsi bloquée par le Bouclier canadien.

Le 31 mars 2022, plus de 177 000 utilisateurs s'étaient inscrits aux services de blocage des menaces du Bouclier canadien, qui ont permis de bloquer plus de 88 millions d'activités cette année.

Rapports et conseils

Le Centre pour la cybersécurité renforce la cyberrésilience et sensibilise la population à cet égard en rédigeant des rapports et des documents d'orientation publics.

Rapports et évaluations

Cette année, le Centre pour la cybersécurité a publié les trois rapports approfondis qui suivent :

- Cybermenaces contre le processus démocratique du Canada : mise à jour de juillet 2021[40];
- Les cybermenaces visant les technologies opérationnelles[41];
- La menace des rançongiciels en 2021[42].

Il a également publié deux courts bulletins sur les activités de cybermenace parrainées par la Russie[43]. Ses rapports sur les cybermenaces sont basés sur une combinaison de sources classifiées et de sources publiques, dont les suivantes :

- les rapports de source ouverte des industries;
- les connaissances opérationnelles découlant des activités de cyberdéfense du CST;
- du renseignement classifié découlant du programme de renseignement électromagnétique étranger du CST;
- du renseignement provenant des partenaires de la collectivité des cinq (États-Unis, Royaume-Uni, Australie et Nouvelle-Zélande).

Documents d'orientation

Cette année, le Centre pour la cybersécurité a publié 30 publications présentant des avis et des conseils[44]. Il a aussi ajouté une fonction de filtrage à son site Web pour faciliter la recherche de ressources pour les Canadiens.

Compte tenu de l'augmentation marquée des incidents par rançongiciel dans les deux dernières années, le Centre pour la cybersécurité a créé une page consacrée aux rançongiciels[45] sur son site Web en décembre 2021. La page contient des rapports sur les menaces, des documents d'orientation et une lettre ouverte destinée aux organisations canadiennes signée par quatre ministres du gouvernement canadien. Le nouveau Guide sur les rançongiciels[46] présente des avis détaillés sur les mesures à prendre pour se défendre contre les rançongiciels et pour assurer la reprise des activités en cas d'incident.

Cette année, les documents d'orientation du Centre pour la cybersécurité qui sont présentés ci-dessous ont porté sur les « maillons faibles » les plus couramment exploités par les pirates recourant aux rançongiciels :

- Empreinte numérique[47];
- Facteurs à considérer en matière de cybersécurité pour votre site Web[48];
- Reconnaître les courriels malveillants[49];
- Stratégies pour protéger les systèmes d'application Web contre les attaques par bourrage d'identifiants[50].

Plusieurs documents d'orientation sont axés sur les menaces visant les infrastructures essentielles :

- Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels[51];
- Protéger le matériel de recherche médicale contre les cybermenaces[52];
- La cybersécurité et les dispositifs médicaux connectés[53].

Le Centre a aussi élaboré des guides sur des sujets prioritaires pour les institutions démocratiques, dont les suivants :

- Repérer les cas de mésinformation, désinformation et malinformation[54];
- L'organisation bénévole et l'accès sécurisé[55];
- Facteurs à considérer en matière de sécurité pour les systèmes de registre électronique du scrutin[56];
- Facteurs à considérer lors de l'utilisation des médias sociaux dans votre organisation[57].

Avis et alertes

Le Centre pour la cybersécurité a publié des avis et des alertes à l'intention des professionnels des TI. Ils présentent des mesures recommandées pour contrer certaines cybermenaces, comme l'application régulière de mises à jour logicielles (avis), et pour atténuer des vulnérabilités critiques (alertes).

Par exemple, en décembre 2021, le Centre pour la cybersécurité a publié un avis conjoint[58] et huit alertes[59] portant sur la vulnérabilité Apache Log4j.

Ces avis et alertes sont publiés sur notre site Web et nos comptes de médias sociaux. Les clients du Centre pour la cybersécurité les reçoivent également par courriel. Le 31 mars 2022, 2701 personnes provenant de 832 organisations s'étaient inscrites à ce service.

Les rapports publics du Centre pour la cybersécurité en chiffres

679 avis

46 alertes

30 documents contenant des avis et de l'orientation

5 rapports sur les cybermenaces

Pensez cybersécurité

La campagne nationale de sensibilisation publique appelée Pensez cybersécurité a pour objectif d'offrir aux Canadiens des conseils simples en matière de cybersécurité qu'ils peuvent appliquer dans leur vie quotidienne. Le mois de novembre 2021 a marqué les dix ans[60] de la campagne Pensez cybersécurité, qui aide les Canadiens à mener leurs activités en ligne en toute sécurité.

Ressources liées à la campagne Pensez cybersécurité

Cette année, les rançongiciels ont été le thème central de la campagne :

- Soyez préparé : comment votre entreprise peut se protéger contre les attaques par rançongiciels[61];
- Rançongiciel 101 : Comment assurer votre cybersécurité?[62];
- Vidéo : Maliciels et rançongiciels[63];
- Rançongiciels : Sauvegardez vos données, sinon…[64].

Dans le cadre de la campagne de cette année, différentes ressources ont été créées à l'intention des aînés canadiens, dont les documents suivants :

- Liste de vérification de cybersécurité[65];
- Comment les adultes âgés peuvent se protéger contre les principales cybermenaces[66];
- De vrais exemples de faux courriels[67];
- Pensez cybersécurité pour vous protéger en ligne[68].

Les responsables de la campagne ont également rédigé du contenu ciblant les jeunes et les familles, par exemple les documents suivants :

- Les menaces à la cybersécurité que toute la famille doit surveiller[69];
- Qu'y a-t-il dans ton sac à dos cybersécuritaire?[70];
- Comment éviter de partager trop de renseignements en ligne[71];
- Cahier d'exercices pour enfants[72] (il contient des jeux et des questionnaires sur la « formation pour devenir un cyberagent »).

En décembre 2021, la campagne Pensez cybersécurité a répandu la joie des Fêtes et a sensibilisé la population à la cybersécurité en publiant ce qui suit :

- le Guide cadeau Pensez cybersécurité de 2021[73];
- le vidéo Coupe-feu de foyer festif[74];
- les ensembles de réseau domestique en pain d'épices[75].

Le vidéo Coupe-feu de foyer festif présente des chants de Noël en anglais et en français dont la thématique est la cybersécurité. Les ensembles en pain d'épices comprennent des conseils pour sécuriser les routeurs domestiques et les ordinateurs portables à même les directives de décoration. Le CST a transmis de véritables ensembles en pain d'épices à 27 partenaires externes, dont 18 ont fait résonner nos conseils en partageant leurs créations sur les médias sociaux.

Mois de la sensibilisation à la cybersécurité

Octobre est le Mois de la sensibilisation à la cybersécurité[76] (MSC) au Canada. Cette année, le thème « La vie en ligne » a été choisi pour refléter à quel point Internet nous a permis de rester connectés durant la pandémie. Les responsables de la campagne Pensez cybersécurité sont les organisateurs principaux du MSC au Canada. Ils travaillent avec des partenaires externes pour promouvoir la cybersécurité par l'intermédiaire de ce qui suit :

- des ressources accessibles[77];
- des conférences.

Cette année, la liste des partenaires du MSC comptait plus de 300 organisations (une augmentation de 35 %) et les demandes reçues concernant les conférences ont doublé. Nous avons co-créé du contenu avec les intervenants suivants :

- l'Association des banquiers canadiens;
- CIRA;
- MediaSmarts;
- Microsoft.

Au moins 247 partenaires ont partagé le contenu du MSC, dont :

- des institutions fédérales;
- des provinces, territoires et municipalités;
- des partenaires de l'industrie.

Médias sociaux

Notre équipe des médias sociaux publie quotidiennement du contenu pour les comptes du CST, du Centre pour la cybersécurité et de la campagne Pensez cybersécurité. Cette année, nos comptes de médias sociaux ont partagé ce qui suit :

- des alertes et des avis en matière de cybersécurité;
- des conseils et des ressources en matière de cybersécurité;
- des rapports publics;
- des possibilités d'emploi et des activités de recrutement;
- le mandat et l'histoire du CST;
- des initiatives en matière d'équité, de diversité et d'inclusion au CST;
- des initiatives de sensibilisation;
- des collaborations avec des partenaires internationaux.

Les médias sociaux en chiffres

Le CST détient 17 comptes de médias sociaux sur cinq plateformes différentes : Twitter, Facebook, LinkedIn, Instagram et YouTube. Ces comptes représentent le CST, le Centre pour la cybersécurité et la campagne Pensez cybersécurité dans les deux langues officielles. Combinées, les publications de l'ensemble des comptes du CST du 1er avril 2021 au 31 mars 2022 ont été vues 6,6 millions de fois.

Totalisant environ 55 000 abonnés, le compte de la campagne Pensez cybersécurité constitue notre plus grande présence sur Twitter; sa présence équivaut en fait à celles du CST et du Centre pour la cybersécurité ensemble. Cette année, le nombre d'abonnés du compte Twitter de la campagne Pensez cybersécurité est demeuré stable, alors que le nombre d'abonnés du compte Facebook a quelque peu chuté. Chacun des autres comptes a enregistré une augmentation du nombre d'abonnés se chiffrant à entre 13 et 43 %.

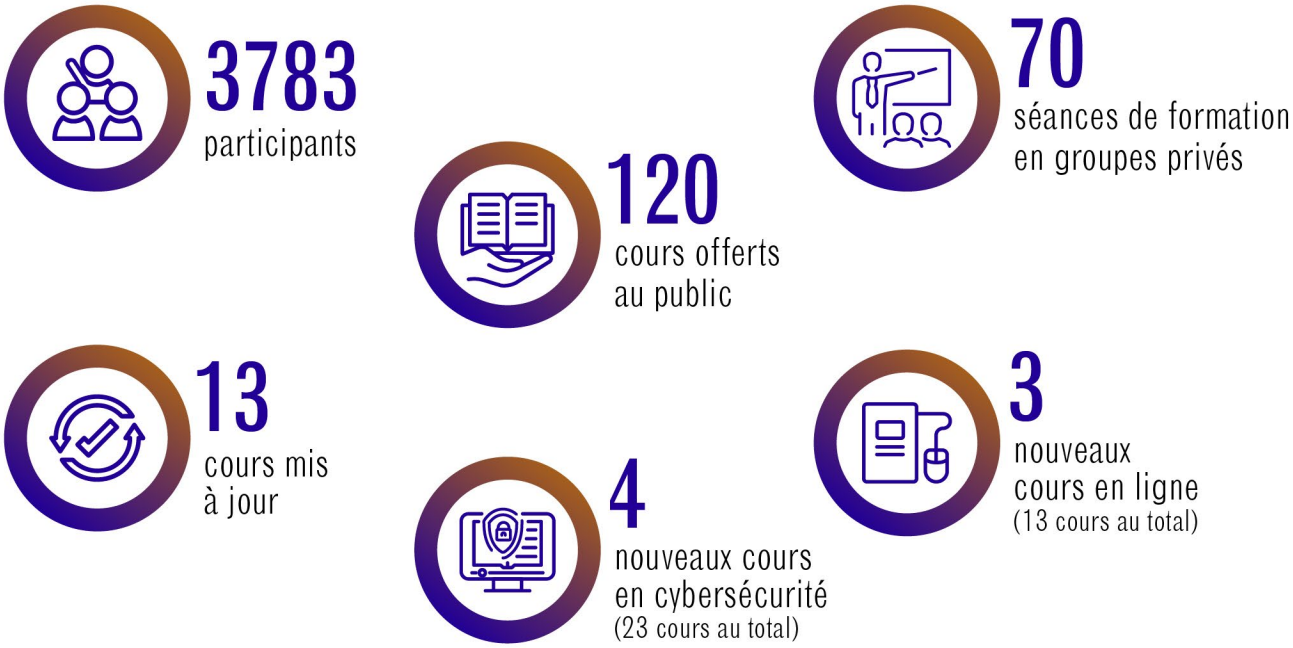
Le tableau ci-dessous présente le nombre d'abonnés francophones et anglophones combinés de nos comptes de médias sociaux en date du 31 mars 2022. Les chiffres sont arrondis au millier le plus près. Les changements de pourcentage sont pour une année à l'autre.

Plateforme	Compte	Abonnés	Changement
Twitter	CST	21 000	13 %
	Centre pour la cybersécurité	27 000	38 %
	Pensez cybersécurité	55 000	0,4 %
Facebook	Pensez cybersécurité	52 000	- 1,4 %
LinkedIn	CST	10 000	43 %
	Pensez cybersécurité	2 000	38 %
Instagram	CST	2 000	-
	Pensez cybersécurité	3 000	28 %
YouTube	CST	500	43 %

Carrefour de l'apprentissage

Le Carrefour de l'apprentissage est établi au Centre pour la cybersécurité et offre de la formation en vue d'améliorer la cybersécurité du gouvernement du Canada et des organisations liées aux infrastructures essentielles.

Le Carrefour de l'apprentissage de 2021 à 2022

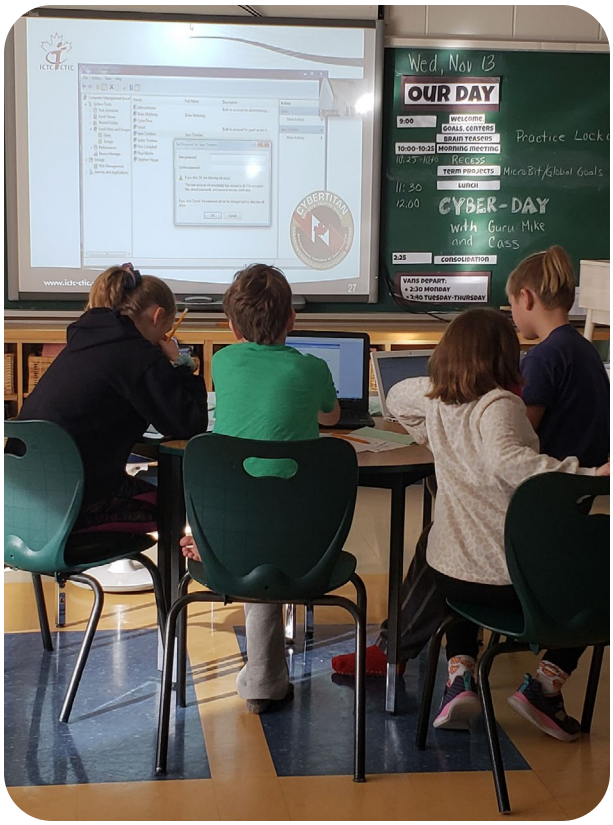


Formation pour les petites et moyennes organisations

Le Carrefour de l'apprentissage collabore avec Innovation, Sciences et Développement économique Canada (ISDE) pour élaborer des cours gratuits en cybersécurité à l'intention des petites et moyennes organisations. La série d'apprentissage en ligne[78] d'ISDE comporte 14 modules que les apprenants peuvent réaliser à leur propre rythme. Ces modules ont été conçus pour des apprenants qui ont des connaissances techniques minimales. Ils peuvent être réalisés dans le cadre du processus de certification de CyberSécuritaire Canada ou simplement pour améliorer ses cyberconnaissances et sa cyberrésilience.

Formation à l'intention des fonctionnaires

Cette année, le Carrefour de l'apprentissage a renouvelé sa collaboration avec l'École de la fonction publique du Canada (EFPC) et offrira un programme normalisé en cybersécurité pour tous les fonctionnaires fédéraux. Par exemple, le Carrefour de l'apprentissage et l'EFPC ont créé ensemble un cours en ligne visant à offrir des connaissances de base sur l'informatique en nuage aux fonctionnaires ne travaillant pas dans le domaine technique. Il s'agit d'un sujet prioritaire pour la fonction publique, car la migration de l'infrastructure TI des ministères vers le nuage se poursuit.



Relations avec le milieu universitaire

Il est nécessaire pour le Canada de disposer d'un effectif doté de compétences en cybersécurité; cette nécessité ne fera que s'accroître. Le Centre pour la cybersécurité coopère avec des établissements d'enseignement pour constituer un bassin de talents canadiens en cybersécurité. Cette année, l'équipe Relations et collaboration avec le milieu universitaire :

- a conseillé des établissements d'enseignement sur le contenu de leur programme d'enseignement;
- a tenu à jour des ressources sur les carrières possibles en cybersécurité, dont ce qui suit :
  → les certifications[79];
  → les programmes post-secondaires[80].

Engagement communautaire

Le CST mène des activités d'engagement communautaire[81] pour conscientiser la population et inspirer la prochaine génération de défenseurs de la cybersécurité.

Les mesures découlant de la pandémie ont bien sûr continué de limiter la tenue d'activités en personne en 2021, mais des employés du CST se sont portés volontaires pour offrir six présentations virtuelles à quelque 200 élèves de l'Ontario afin qu'ils sachent comment sécuriser leurs dispositifs et leurs comptes. Des volontaires du CST ont aussi offert des séances virtuelles liées à Raspberry Pi dans des écoles francophones de la région de la capitale nationale.

Le CST a renouvelé son partenariat avec Hackergal, un organisme sans but lucratif canadien qui enseigne aux filles, aux filles trans et aux élèves non binaires à coder. Nous avons fourni du contenu dans le cadre des campagnes de médias sociaux de Hackergal, notamment pour la Journée de la protection des données et le Mois de l'histoire des Noirs. Des employés du CST se sont également porté volontaire pour mener les activités suivantes :

- offrir du mentorat à des étudiants;
- évaluer des soumissions au programmathon;
- participer à des groupes de discussion virtuels;
- prononcer des discours;
- rédiger des blogues;
- créer des vidéos d'apprentissage.

Nous avons aussi poursuivi notre partenariat avec Cyber Titan; nous leur avons remis du contenu et offert les services d'un conférencier principal dans le cadre de leur concours en ligne sur la cyberdéfense, auquel ont participé de jeunes Canadiens de la 7e à la 12e année.

> **Grâce au soutien du CST, Hackergal a permis à plus de 25 000 filles et personnes s'identifiant comme des filles du Canada d'acquérir des compétences en codage et en littératie numérique depuis 2017. Nous sommes fiers du partenariat que nous avons établi avec le CST; il nous permet de surmonter les obstacles auxquels sont confrontées les filles et de réduire l'écart entre les sexes dans le domaine des technologies au Canada.**
>
> **Lucy Ho**
> *Directrice générale d'Hackergal*

Innovation

Les technologies ne cessent d'évoluer. Le CST consacre du temps, de l'énergie et de l'expertise pour trouver de nouvelles solutions afin de surmonter les défis actuels et futurs.

Recherches universitaires

L'Institut Tutte pour les mathématiques et le calcul[82] (ITMC) est un institut de recherche basé au CST. Ses chercheurs collaborent avec les universités et l'industrie pour relever des défis scientifiques entourant la mission du CST.

Dans la dernière année, les chercheurs de l'ITMC ont collaboré avec des partenaires à l'interne et à l'externe sur des problèmes de recherche, dont :

- la détection de faux profils de médias sociaux par l'intermédiaire de l'apprentissage machine;
- la réduction du nombre de faux positifs dans la détection de maliciels;
- le traitement de données chiffrées sans les avoir d'abord déchiffrées;
- l'accélération de la détection des pourriels et des courriels d'hameçonnage en regroupant le trafic similaire en grappes;
- le recours à l'intelligence artificielle pour séparer les activités de réseau malveillantes des activités inhabituelles mais anodines.

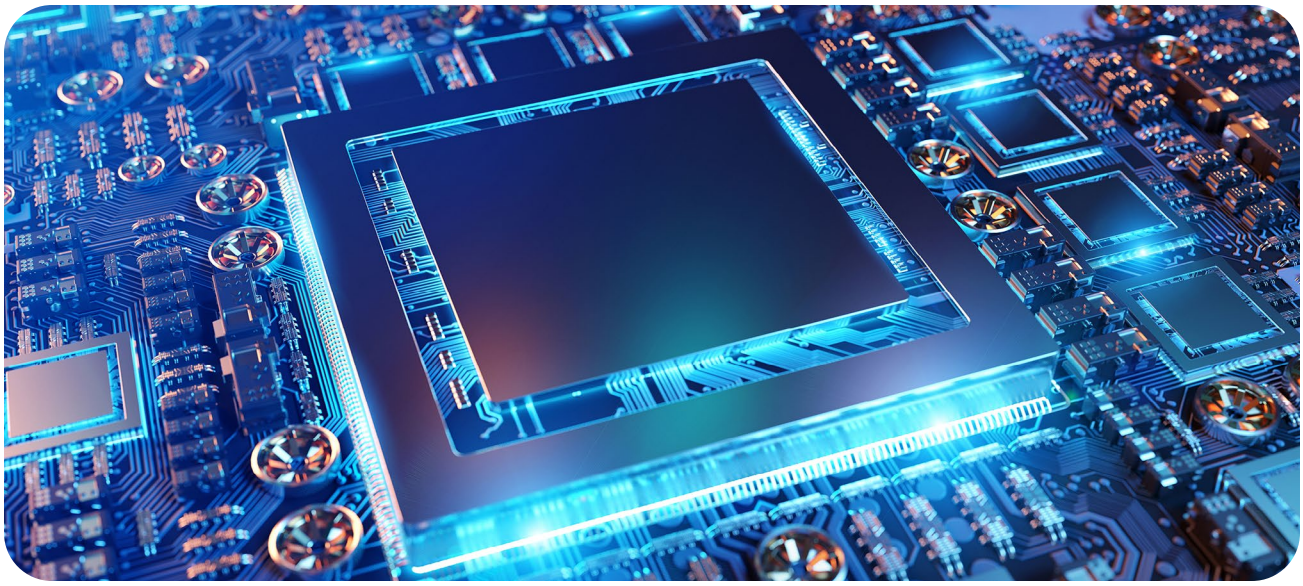
L'ITMC a également fait de la recherche sur la cryptographie et la cryptographie post-quantique (voir la prochaine section).

Bien que certains aspects du travail que réalise l'ITMC soient classifiés, l'Institut publie ses recherches originales lorsqu'il le peut; les collectivités de recherche et de source ouverte externes peuvent ainsi en profiter. Dans la dernière année, les chercheurs de l'ITMC ont publié ce qui suit :

- des articles dans des revues avec comité de lecture;
- des documents de conférence;
- des versions de code de source ouverte;
- un manuel.

Les chercheurs de l'ITMC ont organisé sept conférences virtuelles et ont participé à des dizaines d'autres conférences. Plus de 2,5 millions de téléchargements s'effectuent chaque mois à partir des librairies logicielles de l'ITMC.

En décembre 2021, l'ITMC a célébré ses dix ans d'existence.



Préparation à l'avenir post-quantique

Nous recourons à la cryptographie tous les jours pour stocker et transmettre en toute sécurité des données, par exemple lorsque nous effectuons des transactions bancaires ou échangeons des courriels et des messages instantanés. Toutefois, les experts ont prédit qu'au début des années 2030, les ordinateurs quantiques[83] pourraient être suffisamment forts pour déchiffrer la cryptographie employée de nos jours.

C'est d'ailleurs la raison pour laquelle le CST s'efforce de préparer le Canada à l'avenir post-quantique.

Il collabore avec des partenaires de l'industrie, du milieu universitaire et du Conseil national de recherches Canada pour mieux prédire le moment où les ordinateurs quantiques réaliseront cette percée. Ces efforts visent à guider l'orientation du Centre pour la cybersécurité par rapport au risque qui guette le gouvernement et les infrastructures essentielles.

La cryptographie repose sur des techniques spécialisées (chiffrement et authentification) et a pour objectif de garantir la confidentialité de l'information et de protéger les systèmes contre les cybermenaces. Le personnel du Centre pour la cybersécurité et de l'ITMC du CST se penche sur de nouvelles techniques cryptographiques et sur les mathématiques sur lesquelles elles sont fondées pour trouver des solutions post-quantiques.

La National Institute of Standards and Technology (NIST) des États-Unis a piloté un processus de sélection international de quatre ans dans le but de normaliser l'utilisation de la cryptographie post-quantique à grande échelle. Le Centre pour la cybersécurité a analysé ces technologies afin de s'assurer que les Canadiens puissent y recourir pour protéger leur information encore longtemps.

La NIST devrait annoncer cette année la sélection de la toute première cryptographie post-quantique pour usage général à être normalisée. Ce sera une étape importante vers la mise en œuvre d'applications post-quantiques fiables.

Résolution collaborative de problèmes

Le CST a tenu différents événements collaboratifs pour favoriser l'innovation en cybersécurité.

La Grande exploration

La Grande exploration est un événement classifié de deux semaines qui est organisé chaque année par le Centre pour la cybersécurité afin de relever des défis de cybersécurité de priorité élevée. Les participants proviennent de différents ministères du gouvernement du Canada, des organismes de la collectivité des cinq et de certaines industries canadiennes partenaires. Ils doivent détenir une habilitation de sécurité valide pour pouvoir utiliser des ressources classifiées du CST.

En novembre et en décembre 2021, les participants de la Grande exploration ont entre autres fait des avancées dans les domaines suivants :

- la détection d'incidents;
- l'analyse de maliciels;
- les capacités liées aux cyberopérations défensives;
- la sécurisation de l'Internet des objets.

GeekWeek

La GeekWeek est l'atelier de cybersécurité annuel non classifié du Centre pour la cybersécurité. Cet événement rassemble des participants du gouvernement, de l'industrie et du milieu universitaire. Chaque année, les participants à la GeekWeek travaillent sur plus de 30 projets différents dans le but de résoudre des problèmes difficiles en matière de cybersécurité.

Les derniers événements de la GeekWeek ont eu lieu à l'automne, mais les prochains seront plutôt organisés au printemps. Compte tenu de ce changement, il n'y a donc pas eu de GeekWeek cette année. Toutefois, les efforts entamés lors d'événements de la GeekWeek se poursuivent toute l'année, car le personnel du CST trouve des façons de concrétiser la mise en œuvre d'idées qui sont à l'étape de la validation de principe.

Par exemple, Chameleon est un logiciel configurable pouvant être utilisé hors ligne comme simulateur réseau ou en ligne comme piège à pirates réseau. Un piège à pirates sert de leurre pour attirer les pirates; on peut ainsi étudier les activités de cybermenace qu'ils mènent pour apprendre à les contrer. Chameleon a été développé par plus de 50 participants de différentes organisations lors de quatre événements de la GeekWeek. Pour l'instant, il peut reproduire plus de 154 vulnérabilités en matière de cybersécurité.

En mars 2022, le Centre pour la cybersécurité a finalisé le code pour Chameleon et l'a diffusé à la collectivité de la GeekWeek pour qu'il ait un effet important sur le Canada.

Les innovations qui ont été rendues possibles grâce à la GeekWeek ont contribué à bon nombre d'outils du Centre pour la cybersécurité, dont plusieurs des outils mentionnés dans le présent rapport :

- Assemblyline;
- Aventail;
- Suivi;
- le centre de mise en commun visant à aider à protéger les Canadiens contre l'hameçonnage.

GeekPeek

Nouveauté cette année : l'événement GeekPeek est un programmathon non classifié pour les étudiants canadiens de premier cycle et de cycle supérieur dans des domaines liés à la cybersécurité.

En décembre 2021, à l'occasion de la première édition du GeekPeek, le Centre pour la cybersécurité a accueilli 26 étudiants provenant de sept universités canadiennes. Pendant cinq jours, ils ont travaillé de concert avec des professionnels du Centre pour la cybersécurité sur des problèmes portant sur les sujets suivants :

- l'apprentissage machine;
- l'analyse de trafic réseau;
- la recherche de cybermenaces;
- la rétroingénierie de maliciels

De janvier à mars 2022, le Centre pour la cybersécurité a organisé une « édition cadre » de l'événement GeekPeek en collaboration avec l'Université Queen's. Des employés du Centre pour la cybersécurité ont encadré 25 étudiants qui se sont concentrés sur leurs projets cadres (recherche appliquée durant leur dernière année d'études). Des juges du Centre pour la cybersécurité ont évalué les projets à la fin de mars et les meilleures présentations ont été données lors de la GeekWeek de 2022.

Développement et amélioration d'outils de cybersécurité

Le Centre pour la cybersécurité conçoit et diffuse des outils afin que les ministères du gouvernement puissent évaluer leur propre cybersécurité avec efficacité. Vous trouverez ci-dessous des exemples des technologies que nous avons améliorées cette année.

Application « ObservationDeck »

Le Centre pour la cybersécurité offre l'application Web ObservationDeck aux ministères dans le cadre de son programme de capteur au niveau de l'hôte. Grâce à l'application, les utilisateurs peuvent consulter les données des capteurs sur l'infrastructure de TI de leur ministère afin de prendre des décisions éclairées concernant leur cybersécurité.

En tout, plus de 40 ministères ont adopté ObservationDeck depuis son lancement en 2020. Depuis novembre 2021, le Centre pour la cybersécurité offre une nouvelle version de l'application dont les modifications sont fondées sur les observations des utilisateurs. Elle offre une fonction de recherche améliorée et de nouveaux affichages de rapport. Elle permet aussi aux utilisateurs de générer et d'exporter des ensembles de données, y compris des graphiques sur mesure.

Au cours de la dernière année, le Centre pour la cybersécurité a eu recours à ObservationDeck pour aider ses partenaires à prendre des mesures contre de nombreux événements de cybersécurité, dont Log4j et #PrintNightmare.

ASTRA (Logiciel d'analyse aux fins d'évaluation de la menace)

Le Centre pour la cybersécurité a créé ASTRA, un outil d'évaluation des menaces et des risques, pour aider les ministères du gouvernement du Canada à évaluer le niveau de risque pour la cybersécurité qui pèse sur leurs biens de TI. Par exemple, ASTRA pourrait être utilisé dès le début d'un projet pour évaluer la cybersécurité de différentes architectures de réseau.

L'interface guide les utilisateurs à chaque étape du processus d'évaluation des risques, un peu comme les logiciels d'impôts aident les utilisateurs à produire leur déclaration de revenus.

Les utilisateurs d'ASTRA peuvent :

- cerner les risques plus préoccupants;
- recommander des solutions;
- surveiller les niveaux de risque tout au long d'un projet.

ASTRA était auparavant une plateforme autonome hébergée par le Centre pour la cybersécurité. Puis, en mars 2022, le Centre pour la cybersécurité a lancé une version entreprise de l'outil que les ministères clients peuvent télécharger directement sur leurs réseaux. Des équipes entières disposent ainsi de la même information, ce qui améliore grandement la convivialité du processus. À la fin de l'année, 53 ministères avaient téléchargé ASTRA pour les aider à évaluer les risques pour la cybersécurité.

Suivi

Suivi est un outil d'auto-évaluation automatisé qui est à la disposition des ministères du gouvernement du Canada. Les utilisateurs peuvent consulter la plateforme interactive pour prendre connaissance de la configuration de sécurité de leurs sites Web et de leurs services de courriel publics. Cet outil permet :

- d'empêcher des cybercriminels d'usurper des domaines de messagerie du gouvernement;
- de sécuriser les services en ligne sur lesquels comptent les Canadiens;
- de protéger la réputation du gouvernement du Canada.

Suivi est le fruit d'un partenariat entre le Centre pour la cybersécurité et le Secrétariat du Conseil du Trésor (SCT) du Canada et a été inspiré de l'outil HTTPS-partout[84] du SCT. Grâce à la version améliorée de l'outil, il est désormais plus facile pour les ministères de vérifier si leurs sites Web et leurs services de courriel sont conformes aux politiques du SCT et aux conseils du Centre pour la cybersécurité. Lancé en octobre 2021, l'outil est utilisé par près d'une centaine d'organismes du gouvernement du Canada.

Reddition de **comptes**

Le CST met tout en œuvre pour être aussi transparent que possible, de sorte que les Canadiens sachent qu'il mène ses activités dans le respect de la loi et qu'il protège leur vie privée.

Transparence

Dans le cadre de l'Engagement de transparence en matière de sécurité nationale[85], le CST s'efforce de renseigner ses clients, ses partenaires, les organismes d'examen et l'ensemble de la population canadienne sur qui il est et sur ce qu'il fait sans pour autant compromettre les renseignements personnels et la sécurité.

Au cours de l'année, le CST a publié de l'information sur ses activités par l'entremise des moyens suivants :

- rapports publics[86];
- témoignages parlementaires;
- divulgations proactives[87];
- demandes d'accès à l'information[88];
- publications sur le portail du gouvernement ouvert[89].

Il ne faut pas oublier les outils de communication externe suivants :

- communiqués de presse;
- entrevues dans les médias;
- contenu des médias sociaux;
- discours publics;
- contenu des sites Web.

Conformité interne

La *Loi sur le CST* dicte au CST ce qu'il peut faire et ce qu'il ne peut pas faire. L'ensemble des politiques relatives à la mission décrit en détail **la façon** dont le CST met ces pouvoirs en application.

La série de politiques opérationnelles, élaborées en consultation avec le ministère de la Justice, reposent sur les lois et les valeurs canadiennes ainsi que sur les résultats d'examens internes et externes menés sur une période de plus de 10 ans.

Le CST fait tout en son pouvoir pour que ses employés connaissent les obligations qui leur sont conférées par la loi et les politiques et qui sont décrites dans l'ensemble des politiques relatives à la mission. Le CST favorise une culture axée sur la conformité en prenant les moyens suivants :

- il encourage les employés à autosignaler tout éventuel incident de conformité;
- il collabore avec les employés afin de répondre aux préoccupations et de régler les incidents;
- il mène ses propres activités de vérification interne;
- il fixe des obligations de conformité relatives à la formation, aux systèmes, aux outils et aux processus.

Cette année, l'équipe de la conformité interne du CST s'est livrée aux activités suivantes :

- formation annuelle sur la conformité;
- mise à l'épreuve des connaissances;
- suivi de routine;
- initiatives de mobilisation.

Surveillance externe

Le ministre de la Défense nationale oriente et autorise les activités du CST au moyen de directives, d'autorisations et d'arrêtés ministériels qui définissent les paramètres et les attentes relatifs aux opérations du CST.

Le commissaire au renseignement joue également un rôle dans la reddition de compte, c'est-à-dire qu'il assure une surveillance externe indépendante des autorisations de renseignement étranger et de cybersécurité obtenues par le CST. Le ministre doit délivrer de telles autorisations pour toutes les activités qui, par ailleurs :

- contreviendraient aux lois fédérales;
- porteraient atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

Par exemple, le CST doit obtenir une autorisation pour offrir des services de cybersécurité à un ministère fédéral dans les cas où ces services risquent de porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien. Pour délivrer une autorisation, le ministre doit conclure que le CST satisfait aux conditions énoncées dans la *Loi sur le CST*, entre autres que les activités sont raisonnables et proportionnelles et qu'il y a en place des mesures de protection de la vie privée des Canadiens et des personnes se trouvant au Canada.

Le CST transmet ensuite au commissaire au renseignement, à l'oral ou à l'écrit, toute l'information qu'il a fournie au ministre. Sur la foi de cette information, le commissaire détermine si les conclusions du ministre sont raisonnables. Le CST doit attendre que le commissaire approuve l'autorisation avant de mener les activités visées.

En tout, le CST a soumis cinq autorisations ministérielles au commissaire en 2021 :

- trois autorisations de renseignement étranger;
- deux autorisations de cybersécurité.

Le commissaire au renseignement a approuvé quatre autorisations dans leur entièreté.

Il a approuvé en partie une autorisation de renseignement étranger, mais a demandé au CST de lui transmettre davantage d'information sur une activité en particulier qu'elle contenait. Le CST lui transmettra plus de détails sur l'activité en question dans une application subséquente. D'ici là, le CST ne mène que les activités approuvées par le commissaire.

Autorisations ministérielles soumises par le CST au commissaire au renseignement en 2021[90]

Autorisation	Soumise	Approuvée	Non approuvée	Approuvée en partie
Renseignement étranger	3	2	-	1
Cybersécurité	2	2	-	-
Modifications aux autorisations	-	-	-	-
Total	**5**	**4**	**-**	**1**

Examen externe

Les activités des ministères fédéraux sont assujetties aux examens de divers organismes fédéraux et le CST ne fait pas exception à la règle. En effet, ses activités sont examinées par le Commissariat à la protection de la vie privée, le Commissariat à l'information, la Commission canadienne des droits de la personne et le Commissariat aux langues officielles, entre autres.

De plus, le CST doit se soumettre aux examens de deux organes d'examen externe indépendants dont le mandat est axé sur la sécurité nationale et le renseignement, soit :

- 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).

L'OSSNR est chargé de surveiller les activités liées à la sécurité nationale et au renseignement menées à l'échelle du gouvernement du Canada. Pour sa part, le CPSNR est composé de membres des deux Chambres du Parlement de tous les partis politiques principaux et est mandaté d'examiner les organismes du Canada chargés de la sécurité nationale et du renseignement.

Ensemble, les organes d'examen externe veillent à ce que les politiques et les activités du CST :

- soient raisonnables et nécessaires;
- respectent la vie privée des Canadiens et des personnes se trouvant au Canada;
- soient conformes à la *Loi sur le CST* et à toute autre loi canadienne;
- soient efficaces dans l'atteinte du mandat.

Au cours de la dernière année, le CST a contribué à 14 examens externes (12 par l'OSSNR et deux par le CPSNR). De ce nombre, quatre ont été amorcées au cours de l'année et dix sont en cours.

Le CST contribue aux examens en accordant au CPSNR et à l'OSSNR un large accès à l'information, aux documents, aux dossiers et aux experts en la matière.

Au cours de l'année, le CST :

- a consacré des milliers d'heures au soutien des examens externes;
- a répondu à plus de 200 questions détaillées du CPSNR et de l'OSSNR;
- a donné accès à des dizaines de milliers de documents et de dossiers;
- a participé à plus de 20 séances d'information, réunions ou entrevues avec le personnel des organes d'examen;
- a accordé à l'OSSNR un accès à ses installations et lui a donné des espaces de travail aux fins de recherche dans les documents classifiés;
- a fourni à l'OSSNR, de façon proactive, de l'information sur les autorisations ministérielles et les arrêtés ministériels.

Le CST reconnait la valeur des examens importants et indépendants que ces organes effectuent ainsi que des recommandations qu'ils lui présentent pour améliorer ses pratiques et ses politiques.

Amélioration des processus de protection de la vie privée des Canadiens

Le CST cherche toujours des façons d'améliorer ses processus, surtout en ce qui a trait à la protection de la vie privée des Canadiens et des personnes se trouvant au Canada.

Il ne cible pas les Canadiens ou les personnes se trouvant au Canada dans le cadre de ses activités de collecte de renseignement. Lorsqu'il acquiert par inadvertance de l'information nominative sur un Canadien (INC), il s'assure de la supprimer de ses rapports de renseignement afin de protéger la vie privée des personnes visées. Toutefois, les clients qui reçoivent les rapports peuvent demander l'INC pourvu qu'ils soient autorisés légalement à recevoir cette information et qu'ils aient un besoin de la connaître dans le cadre de leurs opérations.

En juin 2021, l'OSSNR a publié l'Examen des divulgations d'informations identifiant un Canadien par le CST[91]. Dans le cadre de cet examen, l'OSSNR a présenté 11 recommandations pour améliorer le traitement de ce genre de demande.

Depuis le début de l'examen, le CST a mis en œuvre 10 de ces recommandations, entre autres les suivantes :

- effectuer deux mises à niveau d'un logiciel de base;
- renforcer la rigueur des processus de divulgation;
- ajouter des exigences pour ce qui est de consigner les décisions et les analyses à l'interne;
- communiquer avec les ministères clients pour vérifier qu'ils sont bien autorisés légalement à recevoir l'information.

De plus, le CST a mené une étude interne distincte sur la divulgation d'INC afin de s'assurer de la robustesse des mesures de protection de la vie privée.

La dernière recommandation de l'OSSNR, soit d'effectuer une évaluation des facteurs relatifs à la vie privée (EFVP), a été lancée. Le CST s'attend à terminer l'EFVP en 2022.

L'examen a aussi soulevé la non-conformité possible de certaines divulgations d'INC effectuées au cours de la période visée.

Après la réalisation d'une analyse approfondie de son programme et des divulgations liées à 2 351 INC mentionnées dans le rapport de l'OSSNR et après la consultation des partenaires gouvernementaux, le CST est persuadé que toutes les divulgations étaient conformes, sauf une. La seule divulgation qui n'était pas conforme à la *Loi sur la protection des renseignements personnels* a été retirée et l'institution qui a reçu la divulgation a supprimé l'information en question de ses dossiers.

Rapports des organes d'examen et de surveillance

Les organes d'examen et de surveillance externes publient des rapports annuels et des examens non classifiés dans lesquels ils font part de leurs observations à la population canadienne, ce qui contribue à renforcer la reddition de comptes et la transparence.

Voici une liste de rapports publiés au cours de l'année qui touchaient le CST :

- Commissaire au renseignement
  - → Rapport annuel de 2021 du Bureau du commissaire au renseignement[92]
- CPSNR
  - → Rapport spécial du Comité des parlementaires sur la sécurité nationale et le renseignement portant sur le cadre de travail et les activités du gouvernement du Canada visant à défendre ses systèmes et ses réseaux contre les cyberattaques[93]
  - → Rapport annuel 2020 du CPSNR[94]
- OSSNR
  - → Examen des divulgations d'informations identifiant un Canadien par le Centre de la sécurité des télécommunications[95]
  - → Examen de la mise en œuvre par les ministères de la Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères en 2019[96]
  - → Rapport annuel 2020 de l'OSSNR[97]

Un effectif **motivé**

La stratégie CST 2025 repose sur la capacité de l'organisme à miser sur un effectif sain et motivé. Lorsque son effectif est épanoui, le CST peut s'acquitter plus efficacement de sa mission.

L'organisme a fait très bonne figure dans le cadre du récent Sondage auprès des fonctionnaires fédéraux[98], mais il a adopté, en 2021, trois priorités pour favoriser le bien-être au travail :

- la prise de mesures en faveur de l'équité, de la diversité et de l'inclusion;
- la gestion de l'équilibre entre la vie professionnelle et la vie privée, du stress et de la santé mentale;
- le soutien à la direction et aux employés pour faciliter l'adaptation à la nouvelle réalité de « l'avenir du travail ».

Équité, diversité et inclusion (EDI)

Le CST s'est donné comme objectif de créer un milieu de travail dans lequel :

- l'effectif reflète la diversité du pays qu'il sert;
- les obstacles structurels discriminatoires envers les groupes marginalisés sont repérés et supprimés;
- l'inclusion est intégrée dans les politiques et les pratiques;
- aucun employé ne subit du harcèlement ou de la discrimination;
- des mesures sont prises en vue de la réconciliation avec les peuples autochtones partout au Canada;
- chaque membre du personnel est valorisé et célébré pour son unicité.

L'organisme n'a pas encore atteint cet objectif, mais il prend des mesures concrètes pour y arriver. Des changements imposés par la direction aux initiatives lancées sur le terrain, voici quelques mesures prises par le CST pour promouvoir l'EDI cette année.

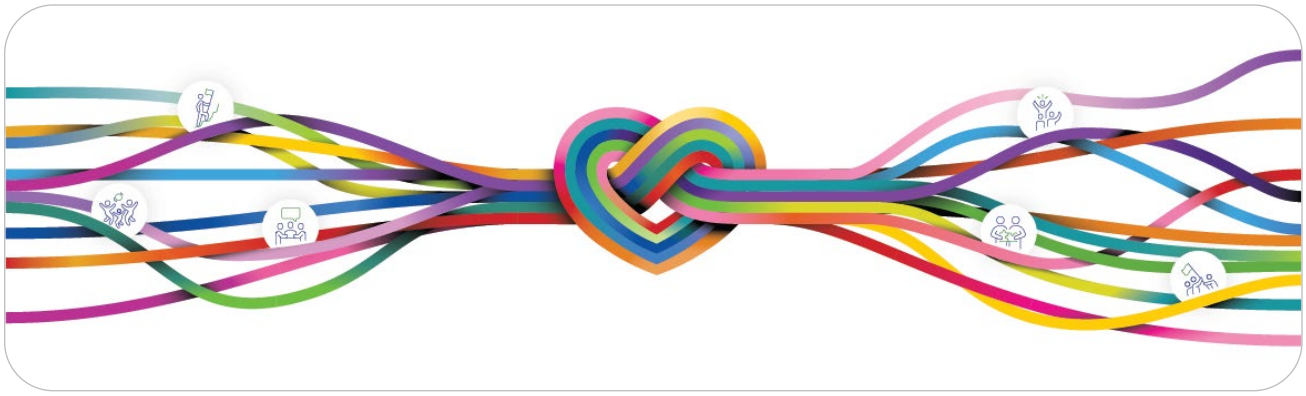
Conseiller supérieur à l'EDI

En mai 2021, le CST a nommé un conseiller supérieur pour les personnes, l'équité, la diversité et l'inclusion. Artur Wilczynski est un défenseur de longue date de l'EDI et, avant cette nomination, il occupait un poste de sous-ministre adjoint au sein du secteur du SIGINT au CST.

Voici quelques-unes des façons dont le conseiller supérieur a laissé sa marque cette année :

- il a conseillé la chef et le chef associé sur les dossiers liés aux personnes;
- il a collaboré avec les secteurs d'activités pour élaborer des stratégies qui favorisent les personnes au niveau des directions;
- il a soutenu les groupes d'affinité du CST (réseaux d'employés);
- il a tissé et maintenu des relations avec :
  → des partenaires à l'échelle du gouvernement;
  → des organisations externes;
  → des dirigeants autochtones;
- il a collaboré avec les Services centraux et les Ressources humaines du CST afin d'intégrer l'EDI dans :
  → le recrutement et le perfectionnement professionnel;
  → le filtrage de sécurité;
  → la formation;
  → la gestion des installations;
  → l'auto-identification aux fins d'équité en matière d'emploi.

> **En tant que personne arrivée au Canada comme réfugié fuyant la persécution ethnique et en tant qu'homme gai, je comprends ce que signifie le fait d'être exclu. Je sais à quel point cela peut saper l'énergie d'une personne. Je veux que nous consacrions toute notre énergie à notre mieux-être et à notre vision commune du CST. Un milieu de travail sain et inclusif nous permettra de maximiser notre capacité à exécuter notre mission.**
>
> **Artur Wilczynski**
> *SMA, conseiller supérieur, Personnes, équité, diversité et inclusion, CST*



Cadre sur l'EDI

En mars 2022, le Comité des personnes a approuvé le tout premier cadre sur l'équité, la diversité et l'inclusion[99] du CST. Le cadre fixe des objectifs ambitieux afin de favoriser l'EDI au CST. Il propose des façons de faire tomber les obstacles systémiques qui empêchent certaines personnes d'atteindre leur potentiel. Il pousse les membres de la direction et du personnel à intégrer la diversité et l'inclusion au niveau de travail pour que le CST réponde aux besoins de tous les Canadiens dans le cadre de sa mission.

Le cadre a été rédigé en collaboration avec des employés des groupes d'affinité du CST. Il comprend des principes, des stratégies et un plan d'action pour rendre le CST un meilleur lieu de travail.

Groupes d'affinité

Il serait impossible d'accomplir des projets comme le cadre sur l'EDI sans la participation et la contribution des groupes d'affinité du CST. Ces groupes sont des réseaux d'employés sur le terrain qui rassemblent des collègues partageant les mêmes préoccupations au sujet de l'EDI. Tous les membres du personnel sont invités à faire partie de ces groupes, en tant que personne ayant vécu des expériences en lien avec le groupe ou en tant qu'allié.

Cette année, les groupes d'affinité du CST ont :

- piloté des initiatives afin de rendre le CST plus inclusif;
- contribué aux nouvelles politiques de l'organisme;
- créé et diffusé des ressources d'orientation;
- offert un lieu sûr pour apporter du soutien mutuel;
- organisé des conférences et des discussions en groupe;
- tenu des célébrations et des événements commémoratifs;
- collaboré avec des groupes de défense dans les organismes partenaires;
- donné des exposés et des séances de sensibilisation.

Trois nouveaux groupes d'affinité ont vu le jour cette année :

- Handicap;
- EmbRACE (un réseau de soutien pour les employés racisés et leurs alliés);
- Neurodiversité.

Ils se sont ajoutés aux réseaux déjà en place, soit :

- le Réseau de la Fierté (pour les personnes bispirituelles, lesbiennes, gaies, bisexuelles, transgenres, queer, intersexuées et asexuelles du CST et leurs alliés);
- Cybersécurité et renseignement au féminin.

> **On constate que l'organisme évolue depuis que nous faisons cette présentation. Il semble qu'il y ait maintenant un véritable désir d'apprendre et de s'exprimer de la part de nos cadres supérieurs.**
>
> **Jonathan Gohidé**
> *Employé du CST, Être Noir(e) au Canada : Une entrevue avec Jonathan et Marie, collègues du CST*[100]

> **La présentation a permis de rassembler les employés racisés et autochtones du CST [...] Les fruits de nos rencontres communautaires nous ont permis de proposer 8 mesures que l'organisme pourrait prendre pour aider son personnel racisé. Ces mesures sont désormais intégrées dans le cadre de l'équité, de la diversité et de l'inclusion. Ainsi ces préoccupations sont soit en voie d'être traitées ou le sont déjà.**
>
> **Marie Calixte-McKenzie**
> *Cadre du CST*

Combattre le racisme anti-Noirs

En février 2021, deux employés du CST, soit Marie Calixte-McKenzie et Jonathan Gohidé, ont présenté leur exposé « Être Noir(e) au Canada » lors d'un événement organisé pour tout le personnel de l'organisme dans le cadre du Mois de l'histoire des Noirs. Ils ont monté cette présentation afin d'exposer ce que les employés Noirs du CST ont vécu depuis le meurtre de George Floyd.

L'exposé a eu un effet retentissant. Le CST a demandé à Marie et à Jonathan de présenter l'exposé aux gestionnaires et aux cadres de l'organisme et a ajouté, en juillet 2021, un enregistrement de la présentation à la liste des formations obligatoires pour les nouveaux employés.

L'exposé a inspiré des employés à former le groupe d'affinité EmbRACE qui a tenu sa première réunion en avril 2021.

En mars 2022, Marie et Jonathan avaient présenté leur exposé dans plus de 36 groupes, rassemblant entre autres :

- des employés, des gestionnaires et des cadres du CST;
- des homologues britanniques du Government Communications Headquarters (GCHQ);
- des membres du programme en leadership de l'Université d'Ottawa destiné aux cadres supérieurs de la fonction publique;
- plus de 2600 fonctionnaires dans le cadre du Forum des conférenciers fédéraux[101] sur la diversité et l'inclusion.

Réconciliation avec les peuples autochtones

La réconciliation avec les peuples autochtones est un des principes fondamentaux du nouveau cadre sur l'EDI du CST.

Les cadres du CST tissent des liens avec les dirigeants autochtones de la région pour prendre connaissance de leurs expériences et veiller à ce que les efforts de réconciliation soient appropriés sur le plan culturel.

De plus, les cadres du Centre pour la cybersécurité discutent avec des organisations autochtones afin de collaborer à des initiatives de mobilisation en matière de cybersécurité.

Le CST participe au Programme d'apprentissage en TI pour les peuples autochtones[102] [document en anglais seulement] et tente de trouver des façons d'inciter davantage d'Autochtones à poser leur candidature au CST.

En juin 2021, pour donner suite à l'appel à l'action lancé par la Commission de vérité et réconciliation du Canada, le CST a convié tous les membres de son personnel à un événement qui visait à les sensibiliser sur l'histoire et les répercussions du régime des pensionnats autochtones.

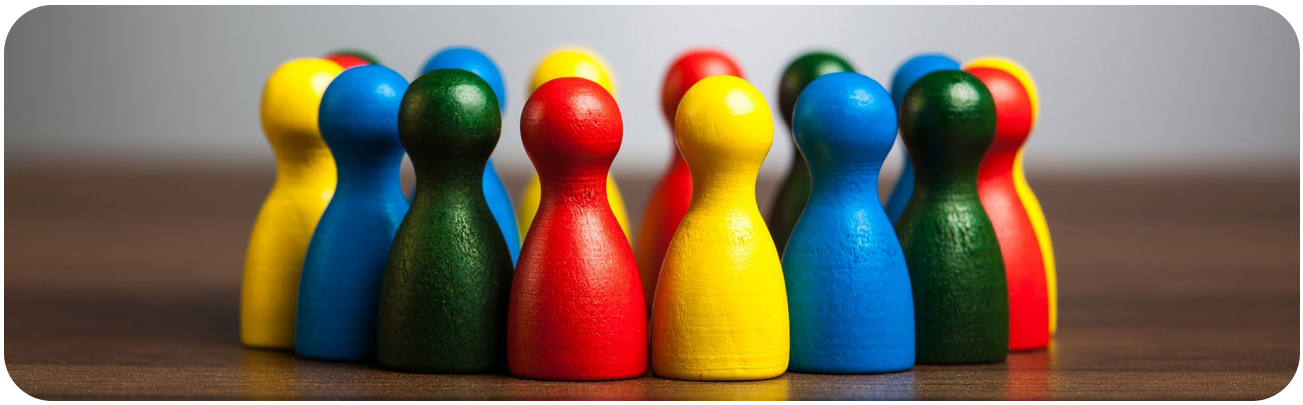
La réconciliation ne se fera pas du jour au lendemain, mais le CST tente de trouver des façons d'y arriver, étape par étape, en collaboration avec les peuples autochtones.

Nouveau guide pour soutenir les droits des personnes transgenres et de diverses identités de genre

En mars 2022, le CST a adopté un nouveau guide : *Soutenir les personnes transgenres et de diverses identités de genre au Centre de la sécurité des télécommunications*[103]. Le document s'adresse entre autres aux membres du personnel qui sont en transition ou qui se questionnent sur leur expression ou leur identité de genre et qui veulent savoir à quoi s'attendre du CST en tant qu'employeur. Il s'adresse aussi aux gestionnaires et aux collègues de ces personnes et leur explique comment les soutenir dans ce processus.

Le guide a été créé en partenariat avec la communauté des personnes bispirituelles, lesbiennes, gaies, bisexuelles, transgenres, queer, intersexuées et asexuelles (2SLGBTQIA+) du CST. Il évoluera avec les lois et les pratiques exemplaires.

> **Comme je suis une personne transgenre plus âgée qui est en voie de transition, je devais savoir dans quelle mesure la direction et le personnel du CST allaient m'accepter. Ce guide fait office de police d'assurance qui me protégera de toute réaction négative éventuelle ou de propos haineux. Ce n'est pas seulement pour moi. C'est pour les jeunes qui suivront ma voie.**
>
> **Toni**
> *Membre du personnel du CST, Changer les choses en appuyant les personnes transgenres et de diverses identités de genre au CST*[104]



Données sur l'équité en matière d'emploi

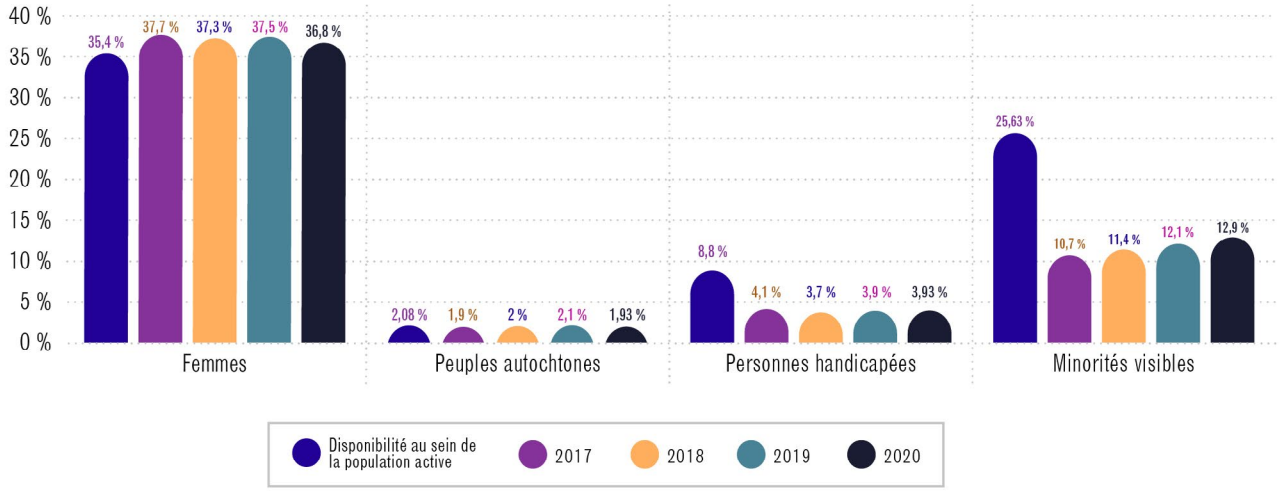
La *Loi sur l'équité en matière d'emploi* dicte à tous les ministères de recueillir des données sur leur effectif. L'objectif est de corriger les désavantages que subissent au travail les personnes qui font partie de quatre groupes désignés, à savoir :

- les femmes;
- les Autochtones;
- les personnes qui font partie des minorités visibles[105];
- les personnes handicapées.

Les dernières données officielles sur l'équité en matière d'emploi montrent une légère augmentation de la diversité au CST (voir le tableau ci-dessous qui montre la tendance sur 4 ans jusqu'en 2020)[106].

Le CST n'a pas pu recueillir de données sur l'équité en matière d'emploi pendant la pandémie étant donné que les employés n'avaient pas accès aux systèmes de ressources humaines (RH). Toutefois, en mars 2022, le CST a lancé un nouveau système de RH qui lui a permis de relancer la collecte d'information issue de l'auto-identification. Les premières statistiques montrent une nette amélioration de la représentativité des personnes handicapées (10 %) et montrent maintenant des données sur le pourcentage de l'effectif du CST qui s'identifie comme faisant partie de la communauté 2SLGBTQIA+ (5 %). Cependant, les membres des minorités visibles et les Autochtones sont encore sous-représentés comparativement à leur disponibilité au sein de la population active. Le CST prend des mesures actives pour que la situation s'améliore et pour augmenter la représentativité des femmes dans les domaines STIM. Le CST sera en mesure de présenter des données à jour dans le rapport annuel de l'an prochain.

Représentation de **l'équité en matière d'emploi** au CST de 2017 à 2020



Campagne d'auto-identification

Pour ce qui est de l'auto-identification, le nouveau système de RH a permis de régler le problème de la logistique, mais il y avait d'autres obstacles. Le CST a consulté des membres des groupes d'affinité qui ont fait part d'inquiétudes par rapport au processus. Certaines personnes avaient des inquiétudes quant à l'utilisation des données. D'autres ont mentionné que le format des cases à cocher ne reflétait pas leurs origines mixtes. Nombreux sont ceux qui ont avoué ne jamais avoir participé à l'auto-identification pour ne pas être accusés d'être un jeton.

Le CST a tenu compte de ces commentaires lorsqu'il a conçu son propre questionnaire d'auto-identification et monté une campagne de communication pour expliquer les fins auxquelles l'utilisation des données est autorisée ou interdite (p. ex., les données ne peuvent pas servir dans des processus de dotation ou de sécurité). La campagne mettait l'accent sur le fait que des données plus précises allaient aider l'organisme à cerner et à combler les lacunes dans la représentativité.

Le CST a lancé le nouveau système de RH le 1er mars 2022. À la fin de l'année, environ les trois quarts de l'effectif avaient rempli le questionnaire d'auto-identification. Grâce aux données ainsi recueillies, le CST pourra édifier des stratégies pour bâtir un effectif plus représentatif du pays qu'il sert.

> **Pour être franche, j'avais des doutes face à l'auto-identification, car je voulais que l'obtention d'un poste soit attribuable à mes compétences et non au fait que je corresponds à un point de données. Maintenant je comprends l'importance du processus et la raison pour laquelle l'organisme a besoin des données recueillies : il peut ainsi mesurer la représentativité actuelle et suivre les progrès vers l'atteinte des objectifs. Chaque point de données compte.**
>
> **Melanie Anderson**
> *Cadre du CST*

L'EDI en ligne

Environ 40 % des employés participent aux forums internes de discussion en ligne consacrés à l'EDI. Le CST a des canaux dédiés aux groupes d'affinité, mais aussi des communautés en ligne sur :

- le patrimoine asiatique;
- les peuples autochtones et la réconciliation;
- la santé mentale;
- les langues officielles.

Compte tenu de l'intérêt pour ces enjeux, le CST a lancé en mars 2022 un espace consacré à l'EDI sur son site Web interne. Il a regroupé en un seul endroit les ressources, les outils, les politiques, l'information sur des événements ainsi que les liens vers les groupes d'affinité.

Langues officielles

Pour le CST, la dualité linguistique au travail est une priorité. Organisme à grande majorité anglophone, il tente de modifier la culture organisationnelle pour faire plus de place au français dans tous les secteurs et à tous les niveaux. Il s'agit d'un engagement à long terme soutenu par la formation et le perfectionnement. Les employés sont invités à parler la langue de leur choix et à aider leurs collègues qui sont en apprentissage linguistique. Toutes les communications officielles, tant à l'interne qu'à l'externe, sont présentées dans les deux langues officielles. Cette année, le CST a souligné la Journée de la dualité linguistique et la Journée internationale de la francophonie.

De plus, l'organisme a lancé en septembre 2021 un outil interne pour aider les membres de la direction à déterminer les exigences linguistiques des postes. L'outil interactif présente une série de questions liées aux fonctions exercées par le titulaire d'un poste et mène à un résultat logique, cohérent et objectif.

Le CST a également produit un Passeport de prises de risques linguistiques offert en français et en anglais. Il contient une liste de défis qui poussent les personnes en apprentissage d'une langue à mettre en pratique leurs compétences linguistiques dans des situations réelles.

Événements pour tout le personnel

Le CST invite régulièrement des conférenciers de l'organisme ou d'ailleurs dans le cadre d'événements (virtuels pour l'instant) ouverts à tout le personnel. Cette année, nombre de ces événements portaient sur des thèmes liés à l'EDI, notamment :

- la lutte contre l'intimidation et le harcèlement;
- les démarches cognitives de la pensée dyslexique;
- l'EDI au CST;
- encourager les jeunes femmes et les filles dans le domaine des technologies;
- l'identité et l'expression de genre;
- la Journée dédiée à la mémoire des victimes de l'Holocauste;
- la Semaine nationale de l'accessibilité;
- la réconciliation avec les peuples autochtones.

Recrutement

Cette dernière année, le CST a modernisé son processus de recrutement pour le rendre plus simple, transparent et interactif. Parmi les moyens pris par l'organisme pour recruter des candidats plus diversifiés, citons entre autres :

- le retrait du langage genré des descriptions de poste;
- la promotion de la diversité et de l'inclusion dans le matériel de recrutement;
- la participation à des activités de recrutement s'adressant à des groupes sous-représentés;
- la prestation de formation sur les techniques d'entrevue aux gestionnaires d'embauche;
- la prise de contact sur les réseaux sociaux professionnels avec des personnes qui pourraient poser leur candidature;
- l'établissement d'une liaison avec :
  - → des groupes autochtones;
  - → des groupes qui font la promotion des femmes dans des domaines techniques.

Bien-être des employés

La pandémie a été difficile pour tout le monde et a laissé des séquelles mentales, physiques et émotionnelles. Voici quelques-unes des mesures prises par le CST pour soutenir son personnel cette année.

Santé mentale

Tous les employés ont accès à un service de consultation professionnelle à l'interne et peuvent donc aborder librement tout ce qui les préoccupe, même des sujets classifiés. Le Programme de mieux-être des employés et de l'organisme comprend :

- le Programme de consultation et d'orientation (PCO);
- le Programme de gestion de l'incapacité (PGI);
- les services de transition de carrière.

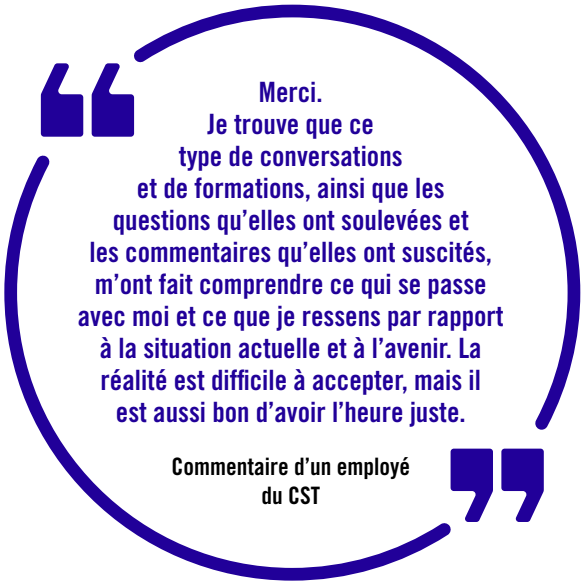
Depuis le début de la pandémie, ces services sont offerts en personne ou en ligne.

Cette année, le PCO a monté et offert des séances de formation destinées à tous les employés, dont les suivantes :

- la gestion de l'anxiété;
- l'art d'être parent en période de pandémie;
- le travail à domicile;
- l'autocompassion;
- le retour au travail au bureau.

Le PCO a également continué d'offrir des séances de méditation en ligne chaque semaine en français et en anglais.

De plus, le CST encourage les membres du personnel à profiter des ressources en santé mentale offertes par l'École de la fonction publique du Canada, notamment des webémissions, des formations et des événements virtuels.



Programme de prévention du harcèlement et de la violence (PPHV)

En janvier 2021, le CST s'est donné les moyens de mieux prévenir et gérer les incidents de harcèlement et de violence au travail, conformément au nouveau règlement fédéral[107].

Le nouveau PPHV est maintenant composé de quatre conseillers (comparativement à un conseiller en 2020).

Le PPHV permet aux employés de signaler des incidents en toute sécurité, mais il comporte aussi un volet de prévention. Le PPHV s'aligne sur le nouveau règlement et offre du soutien aux membres du personnel qui sont victimes de violence familiale.

Cette année, le PPHV a offert :

- du soutien aux parties touchées au moyen du processus de résolution;
- de l'aide avec les évaluations du lieu de travail;
- des mesures d'atténuation des risques;
- des mesures d'urgence;
- du soutien aux membres du personnel victimes de violence familiale;
- des stratégies de prévention;
- des séances d'information;
- des ressources de formation;
- de l'information sur les services de soutien communautaires.

Tous les employés du CST sont maintenant tenus de suivre une formation sur la prévention du harcèlement et de la violence.

Protocole lié à la COVID-19

Cette année, le protocole du CST lié à la COVID-19 a fluctué au gré des vagues de cas. Le principe général était d'assurer la sécurité du personnel sur place tout en poursuivant les opérations. Par exemple, le CST a maintenu l'obligation de porter le masque et de respecter la distanciation physique même après la levée de ces restrictions par les autorités locales de santé publique.

L'objectif de cette approche prudente était de protéger la santé physique des membres du personnel, mais aussi de minimiser l'anxiété chez ceux et celles qui devaient travailler sur place en raison de la nature classifiée de leur travail.

En janvier 2022, le CST a pris part à un programme de tests de dépistage rapide de la COVID-19 en partenariat avec Santé Canada. Les employés qui travaillaient sur place pouvaient choisir de subir chaque semaine trois tests rapides de détection d'antigène. La participation a été forte même si l'adhésion au programme était facultative. Le CST anonymisait les données recueillies avant de les faire parvenir à Santé Canada.

Lorsqu'il apportait des changements au protocole lié à la COVID-19, le CST communiquait clairement les changements à l'avance dans des courriels envoyés à tous les employés et dans un guide numérique tenu à jour.

Se préparer à l'avenir du travail

La pandémie a transformé notre perception du lieu de travail. Le CST s'adapte à la situation pour profiter des nouvelles technologies et des nouvelles façons de travailler.

Ententes sur le télétravail

Au cours des deux dernières années, l'effectif du CST s'est scindé en deux catégories : les employés dont le travail est classifié (comme ceux du SIGINT) ont continué de travailler dans les installations sécurisées et visées par des mesures adéquates de santé publique alors que les employés qui pouvaient travailler à domicile l'ont fait.

Les deux modes de travail comportent des avantages et des inconvénients. À l'avenir, l'objectif est de tirer le maximum des deux modes tout en évitant les inconvénients.

À l'automne 2021, les employés qui travaillaient à domicile ont amorcé un retour graduel dans les installations. Aux employés qui peuvent accomplir leurs tâches à distance, le CST a offert des ententes de télétravail à temps partiel. La période d'essai d'un an de cette approche hybride devait commencer en janvier 2022. Toutefois, l'arrivée du variant Omicron l'a repoussée à avril 2022.

Soutien aux équipes dispersées

Le CST consacre une partie de son site Web interne au soutien des équipes dispersées. Parmi les ressources qui y sont offertes :

- conseils à l'intention des gestionnaires d'équipes dispersées;
- guide de télétravail à l'intention des employés du CST;
- conseils de sécurité pour les organisations dont les employés travaillent à distance;
- liens vers des séances de formation;
- articles;
- outils de travail du gouvernement du Canada.

Environnement à niveaux de classification multiples

Par le passé, les systèmes de technologie de l'information (TI) du CST étaient branchés à un réseau classifié (c'est-à-dire un environnement protégé pour l'information classifiée Secret et Très secret).

Tout cela a changé en 2018 avec la création du Centre pour la cybersécurité qui devait travailler sur un réseau non classifié pour faciliter la collaboration avec des partenaires externes.

Puis, avec la pandémie en 2020, la situation s'est complexifiée étant donné qu'il fallait trouver une façon de soutenir le travail à distance en toute sécurité. Comme l'indiquait le rapport de l'an dernier, cette prouesse a été rendue possible grâce aux efforts extraordinaires déployés par l'équipe des services technologiques qui a rapidement fourni des dispositifs et mis au point de nouvelles capacités.

C'est en partie par choix et en partie par nécessité que le CST a pleinement adopté le travail dans un environnement à niveaux de classification multiples. Cette année, l'organisme a continué de bâtir et de maintenir sa nouvelle infrastructure de TI. Il a mis au point de nouvelles méthodes afin de sécuriser et de protéger adéquatement les dispositifs et a fait part des leçons apprises à d'autres ministères du gouvernement du Canada. Le CST a transformé sa façon de classifier et de gérer l'information. Il a conçu de nouveaux outils de collaboration entre les différents niveaux de classification. Pour y arriver, il a fallu assurer une planification minutieuse ainsi que former et sensibiliser le personnel.

Migration vers le nuage

Au sein du gouvernement du Canada, le CST fait toujours figure de précurseur de la migration vers le nuage. Il a été le premier organisme gouvernemental à déployer, en toute sécurité, plusieurs applications nuagiques commerciales qu'il a protégées avec ses capteurs au niveau du nuage et il a transmis ses leçons apprises à d'autres ministères. Cette dernière année, le CST a continué de migrer vers le nuage des charges de travail, des services, des outils et des applications du réseau non classifié. Cette migration accélère le déploiement de nouveaux outils et facilite le travail et la collaboration du personnel.

Employeur de choix

En janvier 2022, le CST a été reconnu comme un des meilleurs employeurs pour les jeunes canadiens[108] pour une sixième année d'affilée. Il a aussi été nommé parmi les meilleurs employeurs de la région de la capitale nationale[109] sept fois au cours des dix dernières années (2013, 2014, 2015, 2018, 2020, 2021 et 2022).

Le processus de sélection est supervisé par les éditeurs de la publication *Canada's Top 100 Employers*. Au nombre des critères évalués, citons :

- le lieu de travail;
- l'atmosphère au travail;
- les avantages liés à la santé, aux finances et à la famille;
- la formation et le perfectionnement;
- l'engagement communautaire.

Le CST embauche. Visitez la page des carrières[110].

Le CST a **75 ans**

Le 1er septembre 2021, le CST célébrait son 75e anniversaire. L'événement a permis à l'organisme de donner, à la population canadienne, un aperçu du travail accompli au quotidien au fil des ans.

Transmettre notre histoire

Le CST a ajouté une section spéciale sur le 75e anniversaire[111] aux pages Web externes consacrées à son histoire[112]. Le nouveau contenu comprend une série de récits[113] sur des dossiers, des personnes, des endroits, des objets et des événements qui ont joué un rôle important dans l'histoire de l'organisme. Il y a aussi des anecdotes sur les organisations qui ont précédé le CST en temps de guerre, soit la Sous-section de l'examen (civile) et la Joint Discrimination Unit (militaire).

Le CST a aussi eu le privilège d'inclure de nombreux anciens chefs dans les célébrations du 75e anniversaire. Les six derniers chefs se sont joints à la chef actuelle, Shelly Bruce, pour souligner cet anniversaire important du CST et ont fait part des hauts et des bas de leur mandat respectif à la tête de l'organisme. Ces mandats couvrent la période entre la fin de la Guerre froide et aujourd'hui :

- Stewart Woolner (de 1989 à 1999);
- Ian Glen (de 1999 à 2001);
- Keith Coulter (de 2001 à 2005);
- John Adams (de 2005 à 2012);
- John Forster (de 2012 à 2015);
- Greta Bossenmaier (de 2015 à 2018);
- Shelly Bruce (de 2018 à aujourd'hui).

Le CST a partagé dans les médias sociaux une bonne partie du contenu lié à son anniversaire et a notamment publié chaque jour un nouveau billet sur l'histoire du CST au cours des 75 jours qui ont précédé le 1er septembre 2021.

Logo et médaillon

Le CST a conçu un logo spécial CST 75 à utiliser dans ses projets liés à l'anniversaire. Le logo figurait d'ailleurs sur un côté du médaillon spécial du 75e anniversaire conçu à l'interne et distribué aux invités de marque.

Le logo représente un petit casse-tête composé de pièces rouge, or et bleu (les couleurs de l'insigne du CST) sous lesquels le nombre « 75 » est visible dans un espace blanc.

75e anniversaire du CST – Station d'événement spécial

Le code morse et la radio ont joué des rôles vitaux dans le développement des capacités liées au renseignement électromagnétique et étaient parmi les premières technologies utilisées par l'organisme à ses débuts.

Des employés du CST détenteurs de certificats d'opérateur radioamateur ont collaboré avec le programme d'histoire pour établir une station radio sur la pelouse de l'édifice Edward-Drake sous les indicatifs d'appel d'événement spécial VE3CSE75 et VE3CST75.

Le CST a annoncé[114], sur ses plateformes de médias sociaux, la création de la station qui a été en service sur les voies à onde continue (code morse) et à fréquences vocales (alphabet phonétique) pendant deux jours en octobre 2021.

La chef du CST, Shelly Bruce, a lancé officiellement l'événement en matinée le 27 octobre et a communiqué directement avec nos homologues britanniques du GCHQ. Dans le cadre de l'événement spécial, la station a établi plus de 450 contacts dans 34 pays.

Le CST **en bref**

- La chef actuelle du CST est Shelly Bruce.
- La chef relève de la ministre de la Défense nationale, l'honorable Anita Anand.
- Le budget annuel du CST pour l'année 2021-2022 s'élève à 859 millions de dollars (total des autorisations).
- L'effectif du CST est composé de 3199 employés à temps plein.

Dates importantes

1939–1945
Des unités militaires et civiles du Canada fournissent du renseignement électromagnétique pendant la Deuxième Guerre mondiale.

1946
Le Canada met sur pied la Direction des télécommunications du Conseil national de recherches.

1975
L'organisme est renommé Centre de la sécurité des télécommunications et fait désormais partie du programme de la Défense nationale.

2011
Le CST devient un organisme autonome sous la responsabilité du ministre de la Défense nationale.

2018
Le Canada établit le Centre canadien pour la cybersécurité au sein du CST.

2019
La *Loi sur le CST* entre en vigueur.

2021
Le CST protège le Canada et la population canadienne depuis 75 ans.

Notes de **fin de texte**

1 https://cyber.gc.ca/fr/

2 https://www.parl.ca/DocumentViewer/fr/42-1/projet-loi/C-59/sanction-royal#ID0EGTCK

3 https://pm.gc.ca/fr/lettres-de-mandat/2021/12/16/lettre-de-mandat-de-la-ministre-de-la-defense-nationale

4 https://www.cse-cst.gc.ca/fr/mission

5 https://cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/un-cst-integre-un-cadre-pour-lequite-la-diversite-et-linclusion

6 https://www.cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-le-ccc-rappelle-aux-exploitants-des-infrastructures

7 https://www.canada.ca/fr/affaires-mondiales/nouvelles/2021/04/declaration-sur-la-cybercompromission-de-solarwinds.html

8 https://www.cse-cst.gc.ca/fr/ressources-et-information/nouvelles/declaration-du-cst-sur-les-menaces-visant-le-developpement-dun

9 https://www.cse-cst.gc.ca/fr/ressources-et-information/annonces/declaration-du-cst-sur-les-cyberactivites-malveillantes-menees

10 https://www.cse-cst.gc.ca/fr/ressources-et-information/nouvelles/declaration-du-cst-concernant-laffaire-du-maliciel-notpetya

11 https://www.canada.ca/fr/affaires-mondiales/nouvelles/2021/04/declaration-sur-la-cybercompromission-de-solarwinds.html

12 https://www.canada.ca/fr/affaires-mondiales/nouvelles/2021/07/declaration-sur-les-campagnes-cybernetiques-de-la-chine.html

13 https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-le-ccc-exhorte-les-exploitants-des-infrastructures

14 https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-le-ccc-rappelle-aux-exploitants-des-infrastructures

15 https://cyber.gc.ca/fr/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

16 Le tableau porte sur l'année civile, car il est conforme au calendrier des organismes de surveillance du CST. Toute autre mention de « cette année » fait référence à l'année financière.

17 https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-la-menace-des-rancongiciels-en-2021

18 https://cyber.gc.ca/fr/outils-services/programme-validation-modules-cryptographiques-pvmc

19 https://cyber.gc.ca/fr/outils-services/criteres-communs

20 https://cyber.gc.ca/fr/orientation/utiliser-le-chiffrement-pour-assurer-la-securite-des-donnees-sensibles-itsap40016

21 https://cyber.gc.ca/fr/nouvelles-evenements/capteurs-au-niveau-de-lhote

22 Comité des parlementaires sur la sécurité nationale et le renseignement, *Rapport spécial portant sur le cadre de travail et les activités du gouvernement du Canada visant à défendre ses systèmes et ses réseaux contre les cyberattaques*, février 2022

23 https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-fr.pdf

24 https://cyber.gc.ca/fr/glossaire

25 https://cyber.gc.ca/fr/rapports-et-evaluations

26 https://www.gov.nl.ca/hcs/information-and-updates-on-cyber-incident/

27 https://cyber.gc.ca/fr/outils-services/chaine-montage-assemblyline

28 https://cybercentrecanada.github.io/assemblyline4_docs/fr/

29 https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html

30 https://pm.gc.ca/fr/nouvelles/declarations/2021/02/23/feuille-de-route-partenariat-renouvele-etats-unis-canada

31 https://www.cga.ca/fr/cybersecurite/

32 https://www.ieso.ca/en/Sector-Participants/Cybersecurity/Sector-Services---Lighthouse (en anglais seulement)

33 https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-les-cyberattaques-visant-le-secteur-canadien-de

34 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports/rapport-annuel-du-centre-de-la-securite-des#support

35 https://lih-cai.cse-cst.gc.ca/login/index.php?lang=fr_ca

36 Chambre de commerce de la Colombie-Britannique, *Cyber Security and Business Survey*, https://bcchamber.org/wp-content/uploads/2021/10/Cyber-Security-and-Business-Survey-Summary-Report.pdf (en anglais seulement)

37 https://cyber.gc.ca/fr/orientation/ressources-de-cybersecurite-pour-les-petites-et-moyennes-organisations-itsap00137

38 https://cyber.gc.ca/fr/cyberincidents

39 https://www.cira.ca/fr/services-de-cybersecurite/bouclier-canadien

40 https://cyber.gc.ca/fr/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

41 https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-les-cybermenaces-visant-les-technologies-operationnelles

42 https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-la-menace-des-rancongiciels-en-2021

43 https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-le-ccc-rappelle-aux-exploitants-des-infrastructures

44 https://cyber.gc.ca/fr/publications

45 https://www.cyber.gc.ca/fr/rancongiciels

46 https://cyber.gc.ca/fr/orientation/guide-sur-les-rancongiciels-itsm00099

47 https://www.cyber.gc.ca/fr/orientation/empreinte-numerique-itsap00133

48 https://www.cyber.gc.ca/fr/orientation/facteurs-considerer-en-matiere-de-cybersecurite-pour-votre-site-web-itsm60005

49 https://cyber.gc.ca/fr/orientation/reconnaitre-les-courriels-malveillants-itsap00100

50 https://cyber.gc.ca/fr/orientation/strategies-pour-proteger-les-systemes-dapplication-web-contre-les-attaques-par-bourrage

51 https://cyber.gc.ca/fr/orientation/facteurs-relatifs-la-securite-considerer-pour-les-systemes-de-controle-industriels

52 https://cyber.gc.ca/fr/orientation/proteger-le-materiel-de-recherche-medicale-contre-les-cybermenaces-itsap00134

53 https://cyber.gc.ca/fr/orientation/la-cybersecurite-et-les-dispositifs-medicaux-connectes-itsap00132

54 https://cyber.gc.ca/fr/orientation/reperer-les-cas-de-mesinformation-desinformation-et-malinformation-itsap00300

55 https://cyber.gc.ca/fr/orientation/lorganisation-benevole-et-lacces-securise-itsm30010

56 https://www.cyber.gc.ca/fr/orientation/facteurs-considerer-en-matiere-de-securite-pour-les-systemes-de-registre-electronique

57 https://cyber.gc.ca/fr/orientation/facteurs-considerer-lors-de-lutilisation-des-medias-sociaux-dans-votre-organisation

58 https://cyber.gc.ca/fr/nouvelles/bulletin-de-cybersecurite-conjoint-sur-lattenuation-des-vulnerabilites-liees-log4shell

59 https://www.cyber.gc.ca/fr/avis/exploitation-active-de-la-vulnerabilite-apache-log4j

60 https://www.pensezcybersecurite.gc.ca/fr/ressources/pensez-cybersecurite-fete-ses-10-ans

61 https://www.pensezcybersecurite.gc.ca/fr/blogues/soyez-prepare-comment-votre-entreprise-peut-se-proteger-contre-les-attaques-par

62 https://www.pensezcybersecurite.gc.ca/fr/blogues/rancongiciel-101-comment-assurer-votre-cybersecurite

63 https://www.pensezcybersecurite.gc.ca/fr/ressources/video-maliciels-et-rancongiciels

64 https://www.pensezcybersecurite.gc.ca/fr/ressources/rancongiciels-sauvegardez-vos-donnees-sinon

65 https://www.pensezcybersecurite.gc.ca/fr/ressources/liste-de-verification-de-cybersecurite

66 https://www.pensezcybersecurite.gc.ca/fr/blogues/comment-les-adultes-ages-peuvent-se-proteger-contre-les-principales-cybermenaces

67 https://www.pensezcybersecurite.gc.ca/fr/ressources/de-vrais-exemples-de-faux-courriels

68 https://www.pensezcybersecurite.gc.ca/fr/ressources/pensez-cybersecurite-pour-vous-proteger-en-ligne

69 https://www.pensezcybersecurite.gc.ca/fr/blogue/surveiller-cybermenaces-famille

70 https://www.pensezcybersecurite.gc.ca/fr/ressources/qua-t-il-dans-ton-sac-dos-cybersecuritaire

71 https://www.pensezcybersecurite.gc.ca/fr/blogues/comment-eviter-de-partager-trop-de-renseignements-en-ligne

72 https://www.pensezcybersecurite.gc.ca/fr/ressources/agence-pensez-cybersecurite

73 https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-cadeau-pensez-cybersecurite

74 https://www.pensezcybersecurite.gc.ca/fr/ressources/video-coupe-feu-de-foyer-festif-2021

75 https://pensezcybersecurite.gc.ca/fr/ressources/reseau-domestique-en-pain-depices

76 https://www.pensezcybersecurite.gc.ca/fr/mois-de-la-sensibilisation-la-cybersecurite

77 https://www.pensezcybersecurite.gc.ca/fr/ressources/ressources-msc

78 https://learning-apprentissage.ised-isde.canada.ca/course/index.php?categoryid=52&lang=fr_ca

79 https://cyber.gc.ca/fr/certifications-dans-le-domaine-de-la-cybersecurite-2020

80 https://cyber.gc.ca/fr/orientation/annexe-b-programmes-postsecondaires-lies-la-cybersecurite

81 https://cse-cst.gc.ca/fr/culture-et-communaute/engagement-communautaire#community

82 https://cse-cst.gc.ca/fr/culture-et-communaute/recherche/publications-et-evenements-de-linstitut-tutte#Activités

83 https://cyber.gc.ca/fr/orientation/faire-face-la-menace-que-linformatique-quantique-fait-peser-sur-la-cryptographie

84 https://https-partout.canada.ca/fr/index/

85 https://www.canada.ca/fr/services/defense/securitenationale/engagement-transparence-securite-nationale.html

86 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports/rapport-annuel-du-centre-de-la-securite-des%23workforce

87 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/divulgation-proactive

88 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/acces-linformation-et-protection-des-renseignements-personnels

89 https://ouvert.canada.ca/fr/search/ati?f%5B0%5D=ss_ati_organization_en%3ACommunications%20Security%20Establishment&ati%5B0%5D=ati_organization_en%3ACommunications%20Security%20Establishment%20Canada

90 Le tableau porte sur l'année civile, car il est conforme au calendrier des organismes de surveillance du CST.

91 https://nsira-ossnr.gc.ca/fr/review-of-the-communications-security-establishments-disclosures-of-canadian-identifying-information

92 https://www.canada.ca/content/dam/oic-bcr/documents/BCR-Rapport annuel-2021.pdf

93 https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-fr.html

94 https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-fr.html

95 https://nsira-ossnr.gc.ca/fr/nsiras-review-of-cses-disclosures-of-canadian-identifying-information-cii

96 https://nsira-ossnr.gc.ca/fr/review-of-departmental-implementation-of-the-avoiding-complicity-in-mistreatment-by-foreign-entities-act-for-2019

97 https://www.nsira-ossnr.gc.ca/wp-content/uploads/Annual-Report-2020-October-18-2021-FINAL-for-the-Prime-Minister-French-for-printing.pdf

98 https://www.tbs-sct.canada.ca/pses-saff/2020/results-resultats/fr/bt-pt/org/89

99 https://cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/un-cst-integre-un-cadre-pour-lequite-la-diversite-et-linclusion

100 https://www.cse-cst.gc.ca/fr/etre-noire-au-canada-une-entrevue-avec-jonathan-et-marie-collegues-du-cst

101 https://blogue-sct.canada.ca/fr/marie-calixte-mckenzie-et-jonathan-gohide-etre-noire-au-canada

102 https://alfdc.on.ca/wp-content/uploads/2021/10/GCITApprenticeship-Poster-E.pdf

103 https://www.cse-cst.gc.ca/fr/soutenir-les-personnes-transgenres-et-de-diverses-identites-de-genre-au-cst

104 https://www.cse-cst.gc.ca/fr/changer-les-choses-en-appuyant-les-personnes-transgenres-et-de-diverses-identites-de-genre-au-cst

105 Le CST reconnait que ce terme est considéré comme vieilli. Il est utilisé dans le contexte de la *Loi sur l'équité en matière d'emploi* qui fait actuellement l'objet d'une révision. https://www.canada.ca/fr/emploi-developpement-social/ministere/portefeuille/travail/programmes/equite-emploi/groupe-travail.html

106 Remarque : Les données du CST reposent sur l'information divulguée volontairement par ses employés dans le cadre du programme d'auto-identification du gouvernement conformément aux dispositions de la *Loi sur l'équité en matière d'emploi*. Les niveaux de référence relatifs à la disponibilité au sein de la population active sont basés sur les données relatives à la disponibilité sur le marché du travail tirées du recensement de 2016 et tiennent compte d'autres critères tels que la citoyenneté, l'emplacement et des comparaisons fondées sur les codes de la Classification nationale des professions.

107 https://gazette.gc.ca/rp-pr/p2/2020/2020-06-24/html/sor-dors130-fra.html

108 https://reviews.canadastop100.com/top-employer-communications-security-establishment?lang=fr#Jeunes

109 https://reviews.canadastop100.com/top-employer-communications-security-establishment?lang=fr

110 https://cse-cst.gc.ca/fr/carrieres

111 https://www.cse-cst.gc.ca/fr/culture-et-communaute/histoire/75e-anniversaire

112 https://www.cse-cst.gc.ca/fr/culture-et-communaute/histoire

113 https://www.cse-cst.gc.ca/fr/culture-et-communaute/histoire/75e-anniversaire/75e-du-cst-recits

114 https://twitter.com/cst_cse/status/1453417849209360389?cxt=HHwWisCwxar1yasoAAAA