Centre de la sécurité des télécommunications
Communications Security Establishment

ISSN 2564-0488
CAT D95-11F-PDF

Centre de la sécurité
des télécommunications

RAPPORT ANNUEL

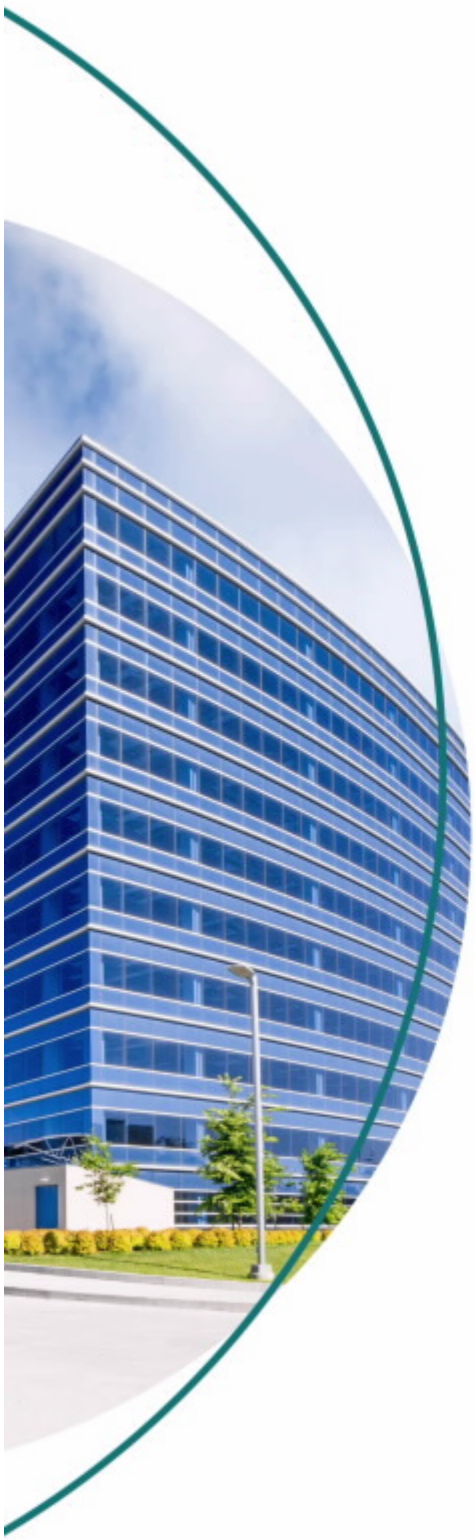
2022–2023

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



Le CST **en bref**

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

Il est un organisme autonome qui relève du ministère de la Défense nationale.

Le CST chapeaute le Centre canadien pour la cybersécurité[1] (Centre pour la cybersécurité), qui est chargé des opérations de cybersécurité pour le gouvernement fédéral.

Le mandat du CST est détaillé dans la *Loi sur le CST*[2] et comporte les 5 volets suivants :

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

La chef du CST, Caroline Xavier, est en poste depuis le 30 août 2022.

La chef relève de la ministre de la Défense nationale, l'honorable Anita Anand.

Les autorités totales du CST pour 2022 à 2023 étaient de 948 millions de dollars.

L'effectif du CST est composé de 3 232 employées et employés permanents à temps plein.

Le présent rapport est un sommaire non classifié des activités qu'a menées le CST du 1er avril 2022 au 31 mars 2023.

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

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

En novembre 2022, j'ai prononcé un discours à l'occasion de la Grande exploration, l'atelier classifié sur la cybersécurité organisé chaque année par le CST. Ce que j'ai vu à cet événement m'a donné de l'espoir : des spécialistes de diverses organisations du gouvernement du Canada, d'alliés étrangers et de partenaires de l'industrie de la technologie qui s'unissent pour surmonter certains des plus grands défis qui guettent le Canada en matière de cybersécurité.

Et ces défis peuvent être très lourds de conséquences. Compte tenu de l'intensification des activités des auteures et auteurs de menace, le CST a émis de nombreux avertissements aux fournisseurs d'infrastructures essentielles du Canada. Ces avertissements devraient servir de signaux l'alarme.

Comme le démontre le présent rapport, le CST et son Centre canadien pour la cybersécurité font des pieds et des mains pour défendre le Canada contre diverses menaces qui pèsent sur sa sécurité nationale, sa sécurité économique et même sa démocratie. Nous devons être lucides face aux menaces et travailler de concert avec tous les intervenants, y compris des partenaires de partout dans le monde, pour défendre nos intérêts communs.

Pour ce qui est du dossier de la défense, le CST a continué de jouer un rôle de premier plan en soutenant les mesures prises par le Canada en réaction à l'invasion de l'Ukraine par la Russie. Il a entre autres mis au jour les efforts continus de désinformation de la Russie et offert du soutien en matière de cybersécurité à l'Ukraine et à la Lettonie.

Le CST sera aussi appelé à jouer un rôle important dans la Stratégie du Canada pour l'Indo-Pacifique. Lancée en novembre 2022, la stratégie comprend un projet multiministériel qui vise à aider les partenaires du Canada dans la région indo-pacifique à perfectionner leur capacité de cybersécurité.

Comme je l'ai constaté en novembre lors de la Grande exploration, le CST est rempli de fonctionnaires qui font preuve d'un grand dévouement et qui ont le cœur à l'ouvrage. En tant que ministre de la Défense nationale, je sais très bien que cet événement ne représente qu'une infime partie du travail déployé chaque jour par le CST pour assurer la protection du Canada et de sa population. Pour toutes les réalisations présentées dans le rapport et celles qui doivent rester secrètes, je voue un grand respect au CST et je lui transmets mes plus sincères remerciements.

- L'honorable Anita Anand
  Ministre de la Défense nationale

Message de la **chef**

Quel honneur de pouvoir transmettre le présent rapport à la population canadienne en tant que nouvelle chef du CST! Même si j'occupe mes fonctions depuis peu, je suis très fière de tout ce que le CST a accompli cette dernière année.

Le CST a entre autres le mandat de contrer certaines des menaces les plus coriaces qui pèsent sur la sécurité nationale, que ce soit les activités étatiques hostiles, comme l'ingérence étrangère, ou la cybercriminalité. J'espère que ce rapport saura laisser transparaître la diligence, la compétence et l'innovation constante nécessaires pour contrer ces menaces.

À ce sujet, je recommande chaudement la lecture de l'Évaluation des cybermenaces nationales 2023-2024[3] qui a été publiée par le Centre pour la cybersécurité en octobre dernier et qui dresse un portrait plus détaillé des menaces. Il s'agit d'une lecture peu réjouissante, mais néanmoins importante.

Compte tenu des menaces grandissantes, le budget de 2022[4] a accordé du financement au CST pour qu'il puisse accroître ses capacités. L'organisme est donc en période de croissance. Cela signifie qu'il essaie de nouvelles choses, comme recruter du personnel à différents niveaux d'habilitation de sécurité et offrir des possibilités de télétravail à l'extérieur de la région de la capitale nationale.

D'ailleurs, si vous connaissez une Canadienne ou un Canadien qui est à la recherche d'une carrière dans laquelle il peut faire une réelle différence, montrez-lui la nouvelle vidéo de recrutement[5]. Le CST cherche à embaucher de nouvelles recrues dans différentes fonctions.

Par ailleurs, cette croissance donne au CST l'occasion rêvée de diversifier son effectif. Depuis que j'ai accédé à mes nouvelles fonctions en août, je suis émerveillée par tous les éléments qui m'entourent et qui témoignent de l'engagement du CST envers l'équité, la diversité et l'inclusion (EDI). La section Personnes du présent rapport fait d'ailleurs état de jalons importants, entre autres :

- le lancement officiel du cadre pour l'EDI;
- la publication du premier Plan d'accessibilité du CST;
- l'instauration du premier programme pilote de parrainage destiné au personnel noir, autochtone et racisé.

Comme toujours, il est impossible de rendre publics certains aspects du travail du CST. Les cibles de ses activités de collecte de renseignement électromagnétique ou de ses cyberopérations étrangères doivent rester secrètes. Elles sont classifiées. Toutefois, le CST donne des exemples de certaines des priorités en matière de renseignement qu'il soutient.

Par exemple, un chapitre du présent rapport porte sur l'ingérence étrangère et la démocratie. Au lieu de séparer les efforts de l'organisme par volet de mandat, le rapport les rassemble dans un seul document. En plus d'être plus conviviale pour le lectorat, cette approche est plus représentative du fonctionnement général du CST. Ses activités de cybersécurité reposent sur du renseignement électromagnétique étranger et vice versa. Ses cyberopérations étrangères lui permettent de contrer des menaces cernées lors de l'exécution d'autres volets de son mandat.

Comme le CST est plutôt limité dans ce qu'il peut dévoiler publiquement, il apprécie grandement les organismes de surveillance et d'examen externes qui scrutent à la loupe son travail pour le compte des Canadiennes et Canadiens. Par exemple, la section sur le partage des métadonnées décrit la collaboration étroite du CST avec le Commissariat à la protection de la vie privée du Canada qui a précédé la mise en œuvre du nouveau processus de partage de certains types de métadonnées avec les plus proches alliés du CST. Celui-ci a aussi collaboré avec l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et lui a accordé un accès indépendant à ses dossiers liés aux examens.

Dans le même ordre d'idée, le CST accueille favorablement les examens indépendants lancés en mars 2023 sur l'ingérence étrangère dans les élections au Canada. Il fera tout en son pouvoir pour faciliter le déroulement de ces examens.

Les menaces qui nous guettent sont bien réelles. Les Canadiennes et Canadiens doivent savoir qu'ils peuvent faire confiance à la collectivité de la sécurité et du renseignement du Canada pour contrer ces menaces de façon efficace, dans le respect de la loi **et** selon les règles d'éthique.

Je suis reconnaissante envers mes prédécesseurs, surtout la 10e chef Shelly Bruce, qui ont su bâtir un organisme digne de cette confiance.

C'est donc avec honneur et plaisir que je prends les commandes du CST pour la prochaine étape de son existence.

- Caroline Xavier
  elle
  11e chef du CST

Renseignement **électromagnétique étranger**

Le CST est l'organisme responsable du renseignement électromagnétique (SIGINT) étranger au Canada. À ce titre, il intercepte et analyse des communications électroniques étrangères pour fournir au gouvernement du Canada de l'information unique sur les menaces étrangères qui pèsent sur la sécurité et la prospérité du Canada et lui faire part d'observations importantes pour soutenir la politique étrangère et la prise de décisions. La loi interdit au CST de cibler les communications des Canadiennes et Canadiens ainsi que des personnes se trouvant au Canada.

Les priorités du gouvernement du Canada en matière de renseignement, qui sont fixées par le Cabinet, orientent la collecte de renseignement électromagnétique étranger du CST. Les rapports de renseignement étranger sont diffusés à une clientèle pangouvernementale et communiqués à des partenaires étrangers de premier plan.

Au cours de la dernière année financière, le CST a produit et diffusé des rapports classifiés sur diverses priorités du gouvernement du Canada, notamment :

- l'invasion de l'Ukraine par la Russie;
- l'ingérence étrangère, l'influence néfaste et la désinformation;
- d'autres activités menées par des États hostiles, entre autres :
  - → l'espionnage,
  - → le sabotage,
  - → le vol de propriété intellectuelle;
- la souveraineté dans l'Arctique;
- l'instabilité en Haïti;
- la cybercriminalité;
- le renseignement sur les cybermenaces;
- le terrorisme et l'extrémisme;
- le soutien aux Forces armées canadiennes dans ses opérations aériennes, maritimes, terrestres et spéciales partout dans le monde;
- les menaces pour les Canadiennes et Canadiens partout dans le monde.

Le renseignement étranger du CST appuie directement d'autres volets du mandat du CST :

- la cybersécurité d'autres institutions fédérales, dont les sociétés d'État et les infrastructures essentielles;
- les cyberopérations étrangères.

Rapports de renseignement étranger du CST pour l'année 2022 à 2023

3 007
rapports

1 774
clients

27
ministères et organismes

Collaboration avec les Forces armées canadiennes

Le CST travaille en étroite collaboration avec les Forces armées canadiennes (FAC) pour intégrer, prioriser et coordonner les opérations de renseignement électromagnétique militaire et répondre aux besoins en matière de renseignement de défense.

Grâce à ce partenariat, les FAC ont une meilleure connaissance du domaine et peuvent renforcer la sécurité des troupes qui mènent des opérations à l'étranger.

Ensemble, le CST et les FAC poursuivent leur partenariat opérationnel et stratégique à tous les niveaux de sorte à coordonner leurs résultats stratégiques et à maximiser les avantages stratégiques pour le Canada sur le plan des affaires internationales, de la défense, de la sécurité et de la cybersécurité.

Cette année, le CST a travaillé en étroite collaboration avec les partenaires des FAC pour fournir du renseignement :

- en soutien au Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD);
- sur l'invasion de l'Ukraine par la Russie;
- sur la souveraineté dans l'Arctique;
- en soutien aux opérations militaires IMPACT, REASSURANCE et UNIFIER.

Cyberopérations **étrangères**

Le CST a aussi pour mandat de mener des activités en ligne pour contrer les menaces de l'étranger et servir les intérêts du Canada en matière d'affaires internationales, de défense et de sécurité.

Les cyberopérations étrangères peuvent être :

- soit des cyberopérations défensives (COD), c'est-à-dire qui servent à protéger les systèmes du gouvernement du Canada et ceux ayant de l'importance pour lui contre des cyberactivités malveillantes;
- soit des cyberopérations actives (COA), c'est-à-dire qui servent à contrer des adversaires étrangers.

En 2022, la ministre de la Défense nationale a délivré 4 autorisations ministérielles de cyberopérations étrangères :

- 1 pour des COD;
- 3 pour des COA.

Pour obtenir de plus amples informations sur la façon dont les cyberopérations étrangères sont autorisées, veuillez consulter la section Reddition de comptes (page 43).

Les cyberopérations étrangères du CST s'appuient à la fois sur le volet du mandat de l'organisme touchant le renseignement étranger **et** ses capacités de cyberdéfense.

Depuis l'entrée en vigueur de la *Loi sur le CST* en 2019, le CST a mené des COA pour :

- contrer des activités d'États hostiles;
- contrer la cybercriminalité;
- perturber les activités d'extrémistes étrangers;
- prêter assistance aux FAC.

Le budget de 2022 prévoyait des fonds destinés au renforcement de la capacité du CST à mener des cyberopérations étrangères. Le financement représente, selon la comptabilité de caisse :

- 273,7 millions de dollars sur 5 ans à partir de l'année 2022 à 2023 et 96,5 millions de dollars par année suivante[6].

Ces fonds permettront au CST de défendre plus efficacement le systèmes du gouvernement et des infrastructures essentielles du Canada contre les cybercrimes et les cyberactivités parrainées par des États.

Comportement responsable dans le cyberespace

Le Canada est favorable à un ordre international fondé sur des règles, ce qui comprend l'adoption de comportements responsables dans le cyberespace.

Conformément à la *Loi sur le CST*, les cyberopérations étrangères ne doivent pas :

- viser des Canadiennes et Canadiens ou des personnes se trouvant au Canada;
- causer des lésions corporelles à une personne ou entraîner sa mort;
- contrecarrer le cours de la justice ou de la démocratie.

Le CST consulte abondamment ses partenaires fédéraux, dont Affaires mondiales Canada (AMC) et le ministère de la Justice, pour s'assurer que les cyberopérations étrangères proposées cadrent avec :

- les exigences juridiques du Canada;
- les obligations du Canada décrites dans le droit international applicable dans le cyberespace[7];
- les normes facultatives en matière de comportement responsable des États dans le cyberespace;
- les objectifs du Canada en matière de politique étrangère.

La ministre des Affaires étrangères doit consentir aux COA et être consultée concernant les COD.

De plus, toutes les opérations sont assujetties à un examen externe pour assurer le respect du mandat et des responsabilités juridiques.

Le CST parvient à contrer les menaces qui guettent le Canada et sa population tout en respectant les exigences susmentionnées et en adoptant un comportement étatique approprié dans le cyberespace.

Partenaires **étrangers**

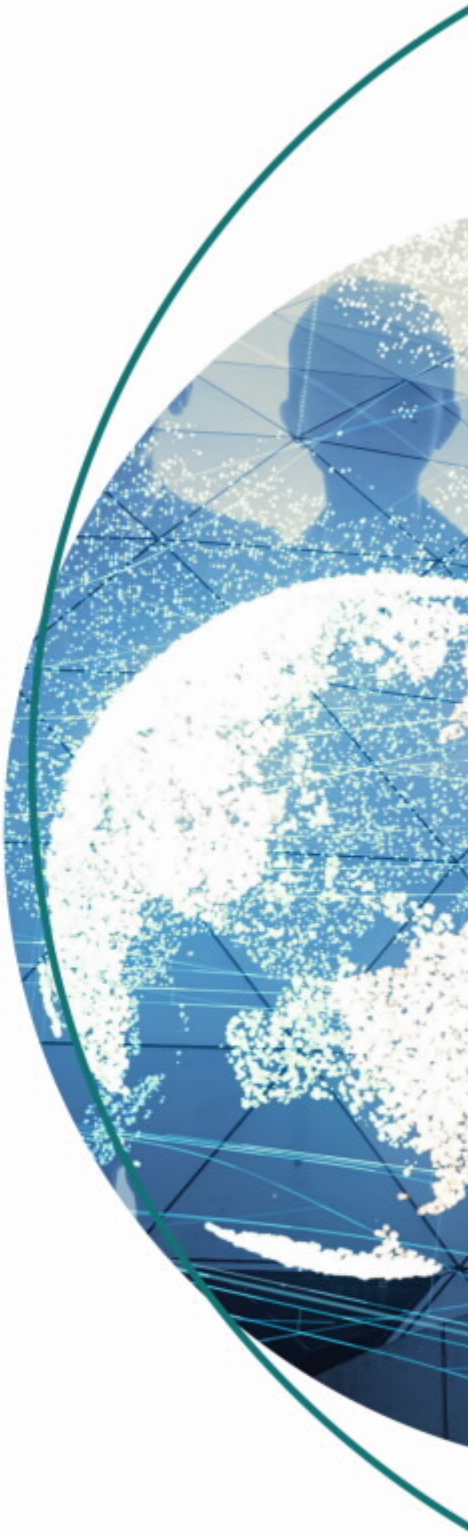
Le CST collabore avec des organismes de renseignement électromagnétique et de cyberdéfense de partout dans le monde de sorte à assurer notre sécurité commune.

Il entretient des relations d'échange de renseignement particulièrement étroites avec les pays qui, avec le Canada, forment la collectivité des cinq, c'est à dire les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle Zélande.

Cette année, le CST a continué de travailler de pair avec ses alliés de la collectivité des cinq pour protéger les intérêts nationaux communs et assurer la sécurité des Canadiennes et Canadiens. Il continue de fournir du renseignement pertinent et opportun à la collectivité et de tirer profit de l'expertise commune de celle-ci pour répondre aux besoins du Canada en matière de renseignement étranger.

En janvier 2023, le CST a recommencé à communiquer des métadonnées à ses partenaires de la collectivité des cinq. La section Reddition de comptes (page 43) décrit les mesures prises par le CST pour régler des préoccupations en matière de respect de la vie privée avant de reprendre la communication de métadonnées (voir la section Communication de métadonnées à la page 46).

Il convient de noter que le CST ne demande pas à ses partenaires de la collectivité des cinq de se livrer, pour son compte, à des activités qui lui sont illégales (par exemple, intercepter des communications de Canadiennes ou Canadiens ou de personnes se trouvant au Canada).



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

Depuis que la Russie a entrepris d'envahir l'Ukraine en février 2022, le Canada apporte un soutien indéfectible au peuple ukrainien qui se bat pour garder sa souveraineté.

Le CST a collaboré étroitement avec des partenaires nationaux et des alliés étrangers pour promouvoir une intervention mondiale unifiée. Il a entre autres :

- fourni du renseignement électromagnétique exploitable au gouvernement du Canada pour :
  - → soutenir les ripostes stratégiques du Canada et de ses alliés (comme l'imposition de sanctions),
  - → surveiller les cyberactivités malveillantes de la Russie contre le Canada, l'Ukraine et les alliés de l'Organisation du Traité de l'Atlantique Nord (OTAN),
  - → protéger les membres du personnel diplomatique, de délégations gouvernementales et de l'armée du Canada en Ukraine;
- offert du renseignement électromagnétique et du soutien en matière de cybersécurité à l'opération UNIFIER, c'est-à-dire la mission de formation des FAC en soutien à l'Ukraine;
- travaillé de près avec ses alliés pour répondre à des besoins pressants en matière de renseignement;
- renforcé les défenses du gouvernement du Canada contre les activités de cybermenace connues appuyées par la Russie;
- contré la désinformation russe;
- communiqué de l'information sur les cybermenaces aux :
  - → principaux partenaires en Ukraine,
  - → alliés de l'OTAN,
  - → infrastructures essentielles du Canada.

Ces activités se sont poursuivies au courant de l'année financière.

Mesures visant à contrer la désinformation russe

D'après du renseignement du CST, le Kremlin a dirigé et coordonné des campagnes de désinformation sur l'invasion. Moscou a notamment accusé à tort les FAC de commettre des crimes de guerre en Ukraine et les États Unis de se servir de l'Ukraine comme d'un terrain d'essai pour des armes biologiques.

En avril 2022, le CST a fait part de ces exemples, entre autres, à la population canadienne pour l'informer des efforts de désinformation appuyés par la Russie (résumé dans le rapport annuel du CST 2021-2022[8]). Il s'agissait de la toute première fois que le CST publiait du renseignement déclassifié sur les médias sociaux[9].

En juillet 2022, le CST a encore une fois eu recours aux médias sociaux pour démentir d'autres **fausses** allégations véhiculées par la Russie selon lesquelles :

- des « radicaux ukrainiens » avaient saboté des installations chimiques et nucléaires en Ukraine;
- le sabotage faisait partie d'une stratégie pour accuser la Russie d'employer des armes chimiques et nucléaires contre des civils ukrainiens;
- des « néonazis ukrainiens » possédaient des armes chimiques qu'ils pourraient utiliser contre la population.

Chaque fois, le CST a aussi dispensé des conseils aux Canadiennes et Canadiens pour les aider à repérer et à contrer la désinformation. En mars 2023, les publications en question dans les médias sociaux avaient été consultées plus de 650 000 fois.

Assistance en matière de cybersécurité à l'Ukraine et à la Lettonie

Le 17 mars 2022, la ministre de la Défense nationale a pris 2 arrêtés ministériels pour désigner l'information électronique et les réseaux de l'Ukraine et de la Lettonie comme étant des systèmes d'importance pour le gouvernement du Canada.

Il s'agissait de la première fois qu'une ou un ministre recourait aux pouvoirs prévus dans la *Loi sur le CST* pour désigner des entités de l'**extérieur du Canada** comme étant des systèmes d'importance.

Grâce à ces désignations, le CST peut apporter de l'assistance en matière de cybersécurité aux entités désignées et ainsi aider à les protéger.

Les arrêtés sont encore en vigueur et le CST continue d'apporter son assistance.

Assistance à l'Ukraine

Au cours de la dernière année, le Centre pour la cybersécurité a avisé l'Ukraine :

- de cyberactivités hostiles menées contre son infrastructure nationale;
- de vulnérabilités dans son infrastructure réseau afin de prévenir des activités hostiles.

Ces alertes ont été rendues possibles grâce aux données communiquées au CST de façon proactive par les autorités ukrainiennes.

En octobre 2022, la ministre de la Défense nationale a annoncé qu'environ 2 millions de dollars allaient servir à offrir des services de télécommunications par satellite à l'Ukraine. Le projet mené conjointement par les FAC et le ministère de la Défense nationale (FAC/MDN), le CST et l'exploitant de satellite Telesat est entré en vigueur le 1er avril 2023 et aidera l'Ukraine à assurer la continuité des services, y compris le maintien de cybersystèmes essentiels.

Le CST collabore avec son pendant ukrainien pour cerner des secteurs dans lesquels il pourrait intensifier son assistance en matière de cybersécurité.

Déploiements en Lettonie

À la demande de ses alliés lettons, le Centre pour la cybersécurité a déployé du personnel en Lettonie pour aider le pays à repousser les cybermenaces qui pèsent sur ses infrastructures essentielles et ses réseaux gouvernementaux.

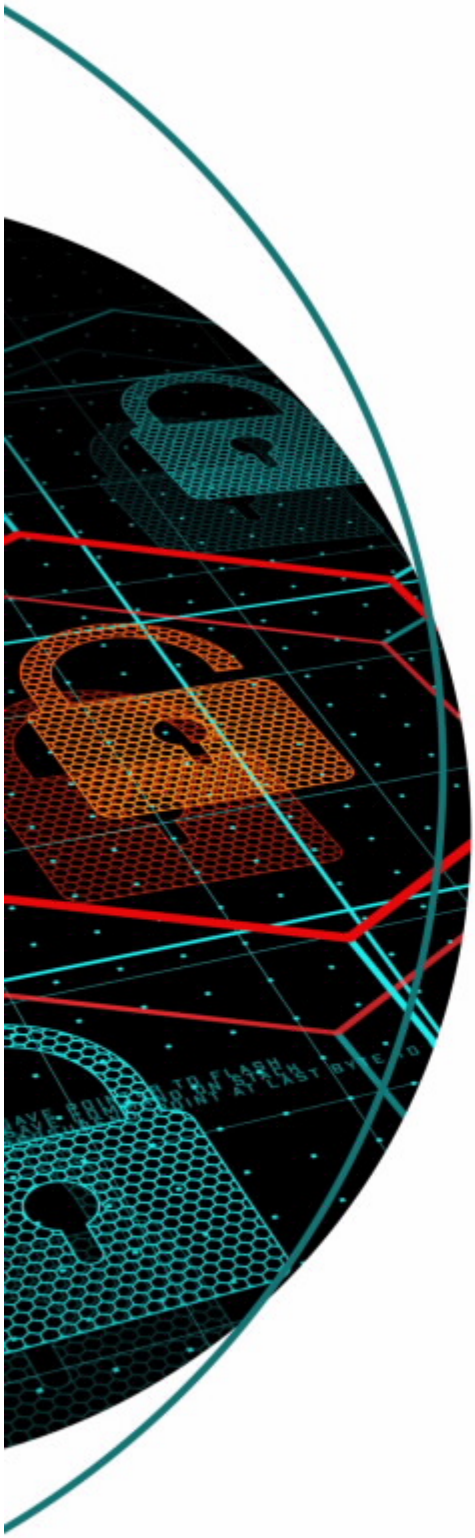
Les déploiements s'inscrivent dans une mission conjointe faisant appel à des spécialistes de la cybersécurité du MDN, des FAC, du Centre pour la cybersécurité et de son équivalent letton, CERT.LV.

Lors des 4 déploiements réalisés au cours de l'année financière visée, le personnel du Centre pour la cybersécurité a aidé à défendre le cyberespace letton en prenant les mesures suivantes :

- enquêter sur des cyberincidents;
- mener des opérations de chasse aux cybermenaces;
- repérer des activités de menace réalisées par les adversaires sur les réseaux essentiels;
- offrir des outils et de la formation sur place;
- présenter des recommandations;
- faire part de pratiques exemplaires;
- améliorer la coordination en matière de cybersécurité entre le Canada et ses alliés de l'OTAN.

Cette mission conjointe a aidé à défendre le flanc est de l'OTAN contre des cybermenaces adverses. Les déploiements du Centre pour la cybersécurité en Lettonie se poursuivent au cours de l'année 2023 à 2024.

> **« Il est intimidant d'être déployé pour une mission comme celle-là. Mais une fois arrivé sur place, on se dit : "Je suis à ma place. Je possède l'expertise qui peut faire une réelle différence." »**
>
> JD, analyste du Centre pour la cybersécurité



Communication d'information au public

Cette année, le Centre pour la cybersécurité a publié des rapports publics, des alertes et des documents d'orientation portant sur les cybermenaces soutenues par la Russie :

- Bulletin de cybersécurité conjoint sur les cybermenaces criminelles et parrainées par la Russie qui planent sur les infrastructures essentielles[10] (avril 2022)
- Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie[11] (juillet 2022)
- Conseils en matière de cybersécurité en cas de niveaux de menace élevés[12] (juillet 2022)
- Risques de cyberactivités malveillantes contre les nations alliées de l'Ukraine[13] (février 2023)

Avec des partenaires de la collectivité des cinq, le Centre pour la cybersécurité a aussi fait paraître 3 bulletins de cybersécurité conjoints pour informer le lectorat des techniques employées par les auteures et auteurs œuvrant pour le compte de la Russie.

De plus, il a tenu des séances d'information à l'intention des organisations du secteur des infrastructures essentielles canadiennes, entre autres les autorités provinciales et territoriales, portant sur le risque accru d'activités de cybermenace.

Ingérence étrangère et **menaces pour la démocratie**

Les auteures et auteurs étatiques hostiles tentent par différents moyens, dont l'espionnage, les cyberactivités malveillantes et la désinformation en ligne, d'influencer et de perturber la société et la démocratie du Canada.

Pour les contrer, il faut adopter une approche pangouvernementale à laquelle le CST participe activement en prenant les mesures suivantes :

- offrir du renseignement électromagnétique étranger aux décisionnaires du gouvernement du Canada sur les intentions, les moyens et les activités des auteures et auteurs de menace étrangers;
- défendre l'infrastructure électorale fédérale du Canada contre des cyberactivités malveillantes;
- aider, à titre préventif, les institutions démocratiques à renforcer leur cybersécurité;
- transmettre des évaluations des menaces non classifiées au public;
- communiquer de l'information aux Canadiennes et Canadiens pour les aider à :
  - → repérer la désinformation,
  - → protéger leur confidentialité et sécurité en ligne.

Groupe de travail MSRE

Depuis 2019, le CST fait partie, avec le Service canadien du renseignement de sécurité (SCRS), la Gendarmerie royale du Canada (GRC) et Affaires mondiales Canada (AMC), du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GT MSRE)[14]. Le rôle du CST consiste à éplucher le renseignement électromagnétique étranger et les cyberactivités sur les réseaux du gouvernement du Canada pour trouver des indications d'ingérence étrangère dans le processus électoral.

Tout au long de la période électorale et à la suite de la mise en œuvre du protocole public en cas d'incident électoral majeur[15] du Canada, les partenaires du GT MSRE tiennent informé un panel composé de hautes et hauts fonctionnaires. Il incombe au panel de déterminer si les activités qui lui sont signalées nuisent à la faculté du Canada de tenir des élections libres et justes. Si une activité atteint le seuil fixé, un protocole établi se met en branle pour informer le public de la situation.

Lors des élections fédérales de 2019 et de 2021, le panel a indiqué que des tentatives d'ingérence étrangère avaient bel et bien eu lieu, mais qu'elles n'avaient pas empêché la tenue d'élections libres et justes.

En mars 2023, le premier ministre a annoncé l'adoption de nouvelles mesures pour renforcer la confiance dans la démocratie canadienne[16]. Parmi ces mesures, citons la tenue d'examens externes sur les élections de 2019 et de 2021 pour évaluer l'influence étrangère exercée sur celles ci et la réaction des organismes de sécurité nationale, dont le CST, face à cette menace.

Le CST continue d'apporter son entière collaboration à ces examens dans le but de renforcer le processus électoral du Canada face à l'ingérence étrangère et de bâtir la confiance de la population à l'égard de ce processus.

Le GT MSRE a tenu des réunions tout au long de la dernière année pour :

- conserver son esprit de collectivité;
- continuer de surveiller les activités d'ingérence étrangère en cours.

Défense de l'infrastructure électorale

Un des volets du mandat du CST consiste à mener des COD pour contrer des cyberattaques contre les systèmes essentiels.

À l'aube des élections fédérales de 2019 et de 2021, le ministre de la Défense nationale de l'époque a délivré une autorisation de COD qui visait entre autres la protection de l'infrastructure électronique d'Élections Canada. Il s'agissait d'une mesure préventive pour contrer toute cyberactivité malveillante qui aurait pu survenir lors de la période électorale. Par exemple, si une auteure de menace étrangère avait compromis le site Web d'Élections Canada, le CST aurait pu lancer une cyberopération pour nuire au serveur utilisé pour l'attaque. En l'occurrence, aucune activité n'a nécessité le recours à des COD. Toutefois, les COD sont un outil important pour contrer les cybermenaces qui pèsent sur le processus démocratique du Canada.

Cybersécurité des institutions démocratiques

Les institutions démocratiques font partie intégrante des infrastructures essentielles du Canada. Le Centre pour la cybersécurité travaille de concert avec les organismes électoraux et les partis politiques fédéraux pour les aider à renforcer leur cybersécurité.

À l'approche des élections fédérales de 2019 et de 2021, le Centre pour la cybersécurité a informé les partis politiques fédéraux des cybermenaces et les a conseillés en lien avec les pratiques exemplaires en matière de cybersécurité. Lors des deux périodes électorales, le Centre pour la cybersécurité a mis à la disposition des candidates et candidats une ligne téléphonique qu'ils pouvaient appeler à toute heure du jour et de la nuit s'ils avaient des inquiétudes par rapport à la cybersécurité. En dehors de ces périodes, les partis politiques peuvent communiquer avec une personne-ressource attitrée du Centre pour la cybersécurité pour discuter de questions liées à la cybersécurité.

En mars 2022, le Centre pour la cybersécurité a informé les partis des risques accrus d'activités de cybermenace soutenues par la Russie à la suite de l'invasion de l'Ukraine. Des personnes représentant 5 partis ont assisté à la séance d'information lors de laquelle des recommandations en matière de cybersécurité ont été présentées. Le Centre pour la cybersécurité a envoyé le contenu de la séance aux 19 partis politiques fédéraux enregistrés.

Au cours de l'année financière, le Centre pour la cybersécurité :

- a offert du soutien aux organismes électoraux à l'approche des élections provinciales au Québec, en Ontario et en Alberta;
- a transmis des ressources d'orientation aux municipalités;
- a offert aux organismes électoraux :
  - → des séances d'information sur l'Évaluation des cybermenaces nationales,
  - → des conseils techniques,
  - → des ressources d'orientation,
  - → des services de cybersécurité.

Cybersécurité des technologies de vote

Depuis 2022, le Centre pour la cybersécurité contribue à l'élaboration des toutes premières normes techniques relatives aux technologies d'élection et de vote au Canada. Des spécialistes du Centre pour la cybersécurité font partie des comités techniques chargés d'élaborer des normes pour :

- le vote en ligne pour les élections municipales au Canada;
- les tabulatrices de votes;
- les registres électroniques du scrutin.

Le processus est dirigé par l'Institut des normes de gouvernance numérique, qui a publié des projets de normes[17] aux fins de consultation publique en avril 2023.

Information sur les cybermenaces pour les élections

En mai 2022, le CST a créé une page Web portant uniquement sur les cybermenaces et les élections[18]. La page fait un survol des moyens que les auteures et auteurs de menace peuvent utiliser pour perturber les processus démocratiques, entre autres :

- perturber l'infrastructure électorale en lançant des attaques par déni de service distribué (DDoS);
- imiter des justificatifs d'identité pour répandre de la fausse information dans les médias sociaux;
- compromettre les systèmes de TI des partis politiques;
- lancer des campagnes d'influence étrangère en ligne pour miner la crédibilité du processus démocratique;
- lancer des attaques au rançongiciel pour perturber l'accès aux données liées aux élections.

La page Web contient des liens vers des rapports du Centre pour la cybersécurité portant sur les cybermenaces contre le processus démocratique du Canada. Elle offre aussi des ressources fournissant des avis et des conseils à jour sur la cybersécurité à l'intention :

- des partis politiques;
- des organismes électoraux;
- de l'électorat.

Désinformation et démocratie

La désinformation est une fausse information qui vise délibérément à causer du tort. Souvent conçue pour susciter une réponse émotionnelle, elle se propage très rapidement dans les médias sociaux. Il est ainsi difficile pour les Canadiennes et Canadiens d'évaluer la véracité de ce qu'ils lisent ou la fiabilité de la source de l'information.

Des États étrangers se servent de la désinformation en ligne pour déstabiliser la démocratie du Canada en ayant recours aux moyens suivants :

- diffuser de la fausse information;
- influencer les décisions de l'électorat;
- polariser les opinions;
- discréditer les personnes et les établissements;
- miner la confiance du public dans le processus démocratique.

Cette année, le CST a contribué à une campagne de sensibilisation pangouvernementale sur la désinformation en ligne[19].
La campagne offre :

- des outils pour aider les Canadiennes et Canadiens à repérer la désinformation et à vérifier les faits présentés;
- du contenu et des vidéos de partenaires externes comme MediaSmarts et CIVIX: CTRL-F;
- de l'information tirée des rapports de menace du Centre pour la cybersécurité, entre autres :
  → de l'Évaluation des cybermenaces nationales[20],
  → des Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021[21];
- de la publication « Repérer les cas de mésinformation, désinformation et malinformation »[22].

Mesures prises contre les **activités d'États hostiles**

Le CST met à profit tous les aspects de son mandat (renseignement étranger, cybersécurité, cyberopérations étrangères et assistance technique et opérationnelle) pour contrer les activités d'États hostiles. Ces activités menaçantes comprennent l'espionnage, les cyberactivités malveillantes et l'ingérence étrangère.

Attributions publiques

Le Canada soutient et défend l'adoption d'un comportement étatique responsable dans le cyberespace.

En avril 2022, AMC a affirmé la position du Canada sur le sujet dans la déclaration Droit international applicable dans le cyberespace[23]. AMC s'unit à des alliés étrangers pour dénoncer les comportements étatiques qui vont à l'encontre des normes établies.

Au cours de l'année financière, les rapports de renseignement et les analyses de cybersécurité du CST ont contribué aux attributions publiques suivantes :

- Déclaration sur les cyberactivités malveillantes de la Russie qui touchent l'Europe et l'Ukraine[24] (mai 2022);
- Déclaration sur la cyberactivité malveillante de l'Iran portant atteinte à l'Albanie[25] (septembre 2022).

Auteures et auteurs de cybermenace parrainés par un État

Le CST tire parti des volets de son mandat touchant le renseignement étranger, les cyberopérations actives et défensives et la cyberdéfense pour contrer les auteures et auteurs de cybermenace étrangers, y compris ceux recevant l'appui d'un État.

Ces derniers représentent la plus grande menace stratégique pour le Canada et ses infrastructures essentielles. Ils recourent à des techniques secrètes et hautement sophistiquées au détriment du Canada et de pays alliés, et ont des objectifs variés allant de la collecte de renseignement jusqu'à la perpétration d'actions destructrices.

Le renseignement électromagnétique du CST continue de fournir de l'information unique et opportune sur les tactiques, techniques et procédures employées par des auteures et auteurs de cybermenace très diversifiés qui sont parrainés par un État. Cette information sert également à alimenter les avis et conseils formulés par le Centre pour la cybersécurité.

Compte tenu de l'évolution continue de ces cybermenaces, entre autres menaces, la cyberdéfense qui repose sur le renseignement offrira un avantage stratégique au Canada.

Répression transnationale

Les États autoritaires déploient différents moyens pour surveiller et intimider les membres de leur diaspora dispersés un peu partout dans le monde, dont au Canada. Par exemple, la République populaire de Chine exploite des « postes de services policiers » au Canada.

Le CST, de pair avec des partenaires étrangers et fédéraux, s'emploie à atténuer les risques que représentent ces activités de répression transnationale. Pour y arriver, il recueille du renseignement électromagnétique étranger et appuie la collectivité de la sécurité et du renseignement du Canada.

Ballon de surveillance à haute altitude

En janvier et février 2023, un ballon de surveillance à haute altitude appartenant à la République populaire de Chine volait illégalement dans l'espace aérien du Canada et des États-Unis. Les forces aériennes américaines l'ont abattu en toute sécurité.

Tout au long de l'incident, le CST était en contact étroit avec ses partenaires américains. Il a collaboré étroitement avec ses partenaires nationaux, dont les FAC, pour appuyer l'intervention du gouvernement du Canada et assurer la sécurité du Canada et de sa population.

Souveraineté dans l'Arctique

Le CST met tout en œuvre pour que le gouvernement du Canada dispose du renseignement nécessaire pour protéger la souveraineté du Canada dans l'Arctique.

En étroite collaboration avec les FAC, le CST veille à ce que le Canada puisse prévoir les tentatives des adversaires qui cherchent à exploiter l'Arctique et qui menacent les intérêts canadiens dans la région, à se défendre contre eux et à les dissuader d'agir ainsi. Pour ce faire, il surveille et analyse les intentions, les capacités et les investissements des auteures et auteurs étatiques hostiles en lien avec l'Arctique.

Le CST préside un forum multinational de renseignement électromagnétique qui s'intéresse aux régions polaires. Il collabore et assure une coordination avec ses partenaires à l'échelle du gouvernement du Canada pour faire en sorte que ses activités de collecte de renseignement répondent à leurs besoins.

> **« L'Arctique canadien suscite de plus en plus d'intérêt à l'échelle internationale et fait l'objet d'une concurrence croissante de la part d'acteurs étatiques et non étatiques qui cherchent à profiter des riches ressources naturelles et de la position stratégique de la région. […] [Cette situation] pos[e] des défis en matière de sécurité auxquels le Canada doit être prêt à répondre. »**
>
> Cadre stratégique pour l'Arctique et le Nord[26]

Mesures prises contre le terrorisme et l'extrémisme

En exécutant le volet de son mandat touchant le renseignement étranger, le CST s'emploie à repérer les menaces de terrorisme et d'extrémisme étrangers qui guettent le Canada et ses alliés. Ces menaces comprennent :

- l'extrémisme violent à caractère religieux (EVCR);
- l'extrémisme violent à caractère idéologique (EVCI).

Cette année, le CST a pu fournir à ses partenaires canadiens et alliés du renseignement unique sur les réseaux, les capacités, les motivations et les intentions liés aux activités extrémistes.

De plus, il a produit du renseignement ayant servi aux cyberopérations étrangères et à la perturbation d'activités extrémistes.

Par exemple, il a exécuté des COA pour supprimer du contenu nuisible qui faisait la promotion du terrorisme et qui était diffusé en ligne par des extrémistes de l'étranger ayant des motivations idéologiques. Cette perturbation a fragilisé la cohésion du groupe extrémiste et a réduit considérablement sa portée en ligne et sa capacité de recrutement.

En raison de la nature complexe des réseaux extrémistes et de l'étendue des sujets connexes, le CST travaille conjointement avec ses partenaires pour fournir le renseignement nécessaire à la perturbation des activités extrémistes. Dans cette optique, le CST participe toujours à un forum multinational de renseignement électromagnétique qui se penche sur le contreterrorisme et qui facilite la collaboration entre les partenaires dans le domaine du renseignement électromagnétique. En faisant partie de cette collectivité, le CST est plus à même de protéger la population et les intérêts du Canada.

Cybercriminalité

La cybercriminalité génère beaucoup d'argent pour les personnes qui s'y adonnent et a une incidence importante sur la sécurité économique du Canada. Comme l'indique l'Évaluation des cybermenaces nationales, le paiement moyen d'extorsion par rançongiciel s'élevait à plus de 250 000 dollars canadiens en 2022. Ce montant exclut d'autres coûts connexes, notamment :

- les interruptions de service;
- le vol d'identité;
- le vol de propriété intellectuelle;
- la reprise informatique;
- les atteintes à la réputation.

> **La cybercriminalité continue d'être l'activité de cybermenace la plus susceptible de toucher les Canadiens et les organisations canadiennes.**
>
> Évaluation des cybermenaces nationales 2023-2024[27]

Compréhension de la cybercriminalité

Le CST effectue de la recherche approfondie sur l'écosystème de la cybercriminalité. Son évaluation s'appuie sur les éléments suivants :

- le renseignement classifié;
- les incidents signalés au Centre pour la cybersécurité;
- les données commerciales;
- l'information accessible au public, comme les articles journalistiques.

Cette année, le Centre pour la cybersécurité a évalué les principaux groupes opérateurs de rançongiciel qui sévissent au Canada pour produire une série de rapports de classement des menaces. Les rapports contiennent de l'information exploitable sur les caractéristiques de chaque groupe afin d'aider les responsables de la cyberdéfense à prioriser leurs ressources.

Le Centre pour la cybersécurité a fait suivre son classement à ses partenaires du fédéral et de la collectivité des cinq pour faciliter la prise de mesures coordonnées contre ces menaces. Il prépare une version du document qui sera acheminé aux clients des infrastructures essentielles au cours de la prochaine année financière.

Les évaluations, telles que le rapport de classement des menaces, servent aussi au CST et au Centre pour la cybersécurité dans la planification de leurs propres activités, notamment la cybersécurité et les COA.

Mesures prises contre la cybercriminalité

Le CST met à profit l'ensemble de son mandat pour minimiser les effets de la cybercriminalité sur les entreprises, les organisations et les personnes au Canada. Parmi les efforts en cours, citons :

- la collecte de renseignement sur les groupes de la cybercriminalité;
- l'amélioration des moyens de cyberdéfense pour protéger les systèmes essentiels contre les menaces de la cybercriminalité;
- la prestation de conseils aux exploitants d'infrastructures essentielles du Canada concernant la protection contre la cybercriminalité;
- le recours aux COA pour contrecarrer les activités des groupes de la cybercriminalité.

Par exemple, le CST a profité de ses pouvoirs pour lancer une campagne de longue haleine visant à perturber les activités des cybercriminelles et cybercriminels étrangers qui menacent de lancer des attaques au rançongiciel contre des systèmes du Canada et de ses alliés. Au nombre des systèmes visés figurent ceux des fournisseurs de soins de santé et des propriétaires d'autres infrastructures essentielles.

Dans le cadre de cette campagne, le CST a exécuté des dizaines d'opérations qui ont perturbé l'infrastructure étrangère utilisée par ces groupes criminels. Grâce à ces opérations, le Centre pour la cybersécurité et d'autres organismes de cyberdéfense ont pu collaborer avec les propriétaires de systèmes visés et prendre des mesures préventives pour éviter qu'ils deviennent des victimes d'attaques au rançongiciel.

De plus, de concert avec des partenaires canadiens et étrangers, le CST a mené des COA afin de réduire la capacité des groupes criminels :

- à cibler la population, les entreprises et les institutions du Canada;
- à lancer des attaques au rançongiciel;
- à solliciter, à acheter ou à vendre des produits et services de la cybercriminalité, entre autres :
  - → des renseignements personnels de Canadiennes et Canadiens,
  - → des renseignements exclusifs du Canada,
  - → des maliciels.

Les opérations ont entraîné des coûts pour les groupes de la cybercriminalité et rendu leurs activités plus laborieuses et moins profitables. L'objectif est d'avoir un effet dissuasif sur les tentatives d'activités de cybercriminalité contre des cibles canadiennes.

Demandes d'assistance technique et opérationnelle

Selon la *Loi sur le CST*, les organismes fédéraux chargés de l'application de la loi, de la défense et de la sécurité nationale peuvent demander au CST de leur prêter une assistance technique et opérationnelle. Grâce à cette approche, le gouvernement n'a pas à instaurer les mêmes expertises et capacités coûteuses dans plusieurs organismes, notamment :

- 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).

Lorsqu'il prête assistance à ces organismes, le CST a les mêmes pouvoirs qu'aurait le partenaire demandeur.

Le CST, la GRC et le SCRS se rencontrent régulièrement pour les besoins du Comité directeur de partenariats techniques (CDPT) qui vise à approfondir la collaboration entre les organismes membres et à mettre à profit les forces et les capacités de chacun afin de satisfaire à leurs mandats indépendants tout en réduisant au minimum la duplication des efforts.

En 2022, le CST a reçu 62 demandes d'assistance technique et opérationnelle de la part des partenaires fédéraux. De ce nombre, 59 demandes ont été approuvées, 1 a été refusée et 2 ont été annulées.

Voici le nombre de demandes d'assistance technique et opérationnelle reçues et approuvées ces 3 dernières années :

- 2022 :
  → Reçues : 62
  → Approuvées : 59
- 2021 :
  → Reçues : 35
  → Approuvées : 32
- 2020 :
  → Reçues : 24
  → Approuvées : 23

Sécurité économique

Le CST fait partie des nombreux ministères et organismes fédéraux qui contribuent à protéger la sécurité économique du Canada. Pour ce faire, il recourt aux volets de son mandat touchant le renseignement étranger et la cybersécurité et met à profit son expertise technique.

Protection de la recherche

La prospérité du Canada dans l'avenir dépend de la recherche et de la propriété intellectuelle du pays. Cependant, ces deux éléments sont souvent la cible de cyberespionnage. Le CST aide à préserver la sécurité économique du Canada en conseillant les organismes canadiens de recherche sur les façons de protéger leur information précieuse.

Il arrive aussi que la protection de l'information devienne une question de sécurité nationale.

En juillet 2021, Innovation, Sciences et Développement économique Canada (ISDE) a publié les Lignes directrices sur la sécurité nationale pour les partenariats de recherche[28]. Ce document vise à éviter que la recherche scientifique du Canada tombe entre les mains d'entités qui représentent une menace pour la sécurité nationale du pays, comme des armées ou des gouvernements étrangers.

En juillet 2022, le CST et ses partenaires qui sont aussi responsables de la sécurité nationale ont amorcé le processus d'examen des risques pour la sécurité nationale prévu dans les lignes directrices.

> **Des auteurs de menace parrainés par des États se livrent à de l'espionnage commercial et ciblent la propriété intellectuelle et d'autres renseignements commerciaux importants dans le but de partager les renseignements volés avec des entreprises appartenant à des États ou avec des industries nationales de leur pays d'origine.**
>
> Évaluation des cybermenaces nationales 2023-2024[29]

Examens relatifs à la sécurité nationale

Le CST a également continué à fournir des examens relatifs à la sécurité nationale à des partenaires gouvernementaux en appui à :

- la *Loi sur Investissement Canada*;
- la *Loi sur les licences d'exportation et d'importation*.

De plus, le CST a donné un coup de main à la Banque du Canada et au ministère des Finances pour concevoir des mesures de protection de la sécurité nationale prévues dans la *Loi sur les activités associées aux paiements de détail*, qui a été sanctionnée en juin 2021.

Intégrité de la chaîne d'approvisionnement

Lorsque les ministères et organismes gouvernementaux se procurent des produits de TI, ils doivent s'assurer que ceux-ci garderont les données et les communications en sécurité. Un produit peut présenter des vulnérabilités à n'importe quelle étape de son cycle de vie, que ce soit lors de la conception, du déploiement ou de la maintenance. Ces vulnérabilités sont connues comme étant des risques liés à la chaîne d'approvisionnement.

Cette année, le Centre pour la cybersécurité a réalisé, pour le compte de clients gouvernementaux, plus de 1 300 évaluations des risques pour l'intégrité de la chaîne d'approvisionnement. Parmi les questions soulevées dans ces évaluations, citons :

- Est-ce que la technologie répond aux normes internationales?
- Qui est le fournisseur?
- Quel est son degré de maturité sur le plan de la cybersécurité?
- Appartient-il à des intérêts étrangers ou est-il assujetti à un contrôle ou à une influence de l'étranger?

Le Centre pour la cybersécurité a aussi publié 3 ressources qui portent sur les risques pour la chaîne d'approvisionnement et qui s'adressent à différents lectorats :

- La cybersécurité et la chaîne d'approvisionnement : évaluation des risques[30] (aperçu pour les Canadiennes et Canadiens)
- Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels[31] (aperçu pour les gestionnaires)
- La cybermenace provenant des chaînes d'approvisionnement[32] (bulletin sur les menaces s'adressant aux spécialistes de la cybersécurité)

Protection de l'infrastructure des télécommunications du Canada

Les réseaux mobiles constituent l'épine dorsale des infrastructures qui permettent aux Canadiennes et Canadiens de communiquer et de mener leurs activités professionnelles et personnelles en ligne. Le CST collabore étroitement avec ses partenaires fédéraux et les fournisseurs de services de télécommunications (FST) du Canada pour assurer la protection de ces réseaux.

En mai 2022, le gouvernement du Canada a annoncé son intention d'interdire l'utilisation de produits et services Huawei et ZTE sur les réseaux 5G du Canada, évoquant des préoccupations pour la sécurité.

En juin 2022, le CST a annoncé les modifications apportées à son programme d'examen de la sécurité[33] à la lumière de ce changement. Des FST canadiens prennent part à ce programme depuis 2013 afin d'atténuer les risques en matière de cybersécurité qui pèsent sur leurs réseaux. Le processus comprenait entre autres l'examen des produits et services de fournisseurs désignés, comme Huawei et ZTE. Résultat : il est interdit d'utiliser certains produits pour des fonctions sensibles dans les réseaux canadiens.

Dans le cadre du nouveau Programme de cyberrésilience des télécommunications, le CST continue d'aider les FST canadiens à atténuer les risques en matière de cybersécurité et ceux liés à la chaîne d'approvisionnement. Le programme intègre maintenant **tous** les fournisseurs clés et porte sur la résilience des réseaux.

Normes internationales

Le Centre pour la cybersécurité travaille en étroite collaboration avec des partenaires fédéraux et étrangers afin de concevoir et de maintenir des normes internationales pour les produits de TI.

Cette année, il a continué de certifier des produits commerciaux de TI selon :

- le programme des Critères communs[34] (normes de cybersécurité);
- le Programme de validation des modules cryptographiques[35] (normes de cryptographie).

Il a aussi poursuivi son travail mené conjointement avec des partenaires étrangers dans le but d'établir des normes de cryptographie post-quantique (voir la section Cryptographie à la page 22).

Sécurité des **communications**

La sécurité des communications (COMSEC pour *Communications Security*) représente une grosse partie de la mission du CST. En fait, elle fait partie du nom de l'organisme. Les efforts en ce sens sont continus et ne stagnent jamais. Le CST adapte ses méthodes et sa posture au gré de l'évolution technologique pour empêcher les adversaires de compromettre les communications sensibles du gouvernement du Canada.

COMSEC

La COMSEC désigne le matériel, les logiciels, la technologie, les algorithmes et les procédures utilisés pour protéger les communications gouvernementales sensibles. Cette année, le CST a continué de fournir au gouvernement du Canada :

- des téléphones protégés, des crypteurs de réseau et d'autres solutions de COMSEC servant aux déploiements au pays et à l'étranger;
- des clés cryptographiques pour protéger les communications et les données sensibles;
- des avis et des conseils au gouvernement et aux exploitants d'infrastructures essentielles concernant :
  - → la cryptographie,
  - → la sécurité des émissions (EMSEC pour *Emissions Security*),
  - → la sécurité opérationnelle (OPSEC pour *Operational Security*),
  - → les vulnérabilités,
  - → les communications sécurisées au moyen de produits commerciaux.

Par exemple, le CST a continué de soutenir les solutions protégées de vidéoconférence et de mobilité offertes aux membres du Cabinet et aux hautes et hauts fonctionnaires.

Cette année, le Centre pour la cybersécurité a constaté une hausse dans les besoins en matière de communications protégées et de soutien dans le domaine des infrastructures essentielles.

Formation COMSEC

Le Carrefour de l'apprentissage du Centre pour la cybersécurité donne des formations obligatoires aux fonctionnaires du gouvernement du Canada qui utilisent de l'équipement COMSEC. Cette année, il a offert un nouveau cours de mise à niveau basé sur les incidents COMSEC les plus signalés.

Il continue de collaborer avec les FAC et le MDN pour normaliser la formation COMSEC à l'échelle du gouvernement du Canada.

Cryptographie

La cryptographie est un élément essentiel à la COMSEC et à la cybersécurité. Elle empêche les adversaires d'accéder sans autorisation aux données et aux communications et de les modifier.

Par contre, les menaces qui guettent la cryptographie évoluent sans cesse. En effet, selon les spécialistes du domaine, des superordinateurs recourant à la physique quantique pourraient, dès les années 2030, percer la cryptographie utilisée de nos jours. Si de nouvelles solutions de cryptographie résistantes aux ordinateurs quantiques ne sont pas développées et déployées partout dans le monde, toute l'information numérique au repos ou en transit pourrait être à risque de compromission.

Nouvelles normes de cryptographie post-quantique

En collaboration avec des partenaires du gouvernement fédéral, du secteur commercial, du milieu universitaire et d'autres pays, le Centre pour la cybersécurité développe la cryptographie post-quantique (CPQ) fiable. La CPQ repose sur des techniques cryptographiques résistantes aux attaques connues lancées par des ordinateurs quantiques.

Les efforts internationaux de recherche sur la CPQ ont fait un bond de géant en juillet 2022 lorsque le National Institute of Standards and Technology (NIST) des États-Unis a annoncé les sélections initiales dans le cadre de la normalisation de la CPQ[36]. Le Centre pour la cybersécurité a évalué les candidats pour veiller à ce qu'ils offrent des moyens de sécurité suffisants pour protéger l'information et les systèmes d'importance du Canada et de sa population.

Le NIST devrait finaliser la première norme de CPQ en 2024, après quoi le Centre pour la cybersécurité mettra à jour sa liste d'algorithmes cryptographiques approuvés[37]. D'ici là, le Centre pour la cybersécurité a publié de nouveaux documents d'orientation mis à jour pour aider les organisations canadiennes à se préparer à la transition vers la CPQ :

- Conseils sur la mise en œuvre de l'agilité cryptographique[38]
- Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B[39] (document mis à jour avec des conseils concernant la mise hors service de certains algorithmes d'ici 2023)

Stratégie quantique nationale du Canada

En janvier 2023, ISDE a publié la Stratégie quantique nationale du Canada[40]. La Stratégie s'articule autour de 3 missions :

- Faire du Canada un chef de file mondial dans le domaine de l'innovation quantique;
- Assurer la protection de la vie privée et la cybersécurité des Canadiennes et Canadiens dans un monde axé sur l'informatique quantique;
- Permettre au gouvernement du Canada et aux industries clés de développer et d'adopter rapidement les technologies quantiques.

Le CST a mis son savoir-faire technique au profit de l'élaboration de la stratégie. Ses spécialistes participeront à l'évaluation des propositions déposées dans le cadre de la stratégie et donneront leurs avis sur les répercussions que ces propositions pourraient avoir sur la cybersécurité du gouvernement du Canada.

Cybersécurité

Le CST a le mandat d'aider à protéger les institutions fédérales et les infrastructures essentielles du Canada contre les cybermenaces. Le Centre pour la cybersécurité est chargé des opérations de cybersécurité pour le gouvernement et à cette fin, il collabore étroitement avec Services partagés Canada et d'autres partenaires fédéraux. Le Centre pour la cybersécurité profite aussi de l'expertise du CST dans d'autres domaines, entre autres dans le renseignement électromagnétique étranger.

Investissements du budget de 2022

Le contexte de la cybermenace évolue rapidement. Pour cette raison, le budget de 2022[41] alloue des fonds au CST pour l'aider à :

- rendre les systèmes gouvernementaux essentiels plus résilients aux cyberincidents;
- prévenir les cyberattaques contre les infrastructures essentielles et à y réagir;
- élargir la protection de la cybersécurité pour les petits ministères, les organismes et les sociétés d'État;
- prévenir et à contrer les cyberattaques (voir la section Cyberopérations étrangères à la page 8);
- poursuivre la recherche sur les technologies émergentes (voir la section Recherche à la page 38).

Ces investissements jettent des bases solides sur lesquelles le CST peut s'appuyer pour prendre de l'expansion. Le CST tente aussi d'étoffer son effectif pour suffire à la demande croissante (voir la section Recrutement à la page 53).

Protection des institutions fédérales

Le Centre pour la cybersécurité recourt à des capteurs, c'est à dire des outils logiciels installés sur les systèmes de TI de partenaires, pour détecter des cyberactivités malveillantes sur les réseaux, les systèmes et les infrastructures infonuagiques du gouvernement.

Ses outils automatisés et ses analystes spécialistes scrutent les données des capteurs à la recherche de flux inhabituels (similitudes dans le trafic réseau), entre autres :

- des tentatives de déploiement de maliciels;
- des tentatives de mappage des systèmes et des réseaux;
- des tentatives d'extraction d'information.

Si le Centre pour la cybersécurité détecte des activités malveillantes, il prend des mesures pour les contrecarrer. Il peut par exemple diriger les capteurs de sorte qu'ils bloquent les activités automatiquement.

Cette année, les moyens de défense automatisés ont protégé les systèmes et réseaux du gouvernement du Canada contre 2,3 billions d'activités malveillantes, ce qui représente une moyenne de 6,3 milliards d'activités par jour.

Le budget de 2022 annonçait du nouveau financement accordé au CST pour qu'il puisse rendre les systèmes essentiels du gouvernement plus résilients aux cyberincidents. Le financement représente, selon la comptabilité de caisse :

- 312,9 millions de dollars sur 5 ans à partir de l'année 2022 à 2023 et 61,7 millions de dollars par année suivante[42].

Déploiements des capteurs en date de mars 2023 :

- Capteurs au niveau de l'hôte (HBS)
  → 85 institutions fédérales (comparativement à 79 en 2022)
  → 860 000 dispositifs (comparativement à 730 000)
- Capteurs au niveau du nuage (CBS)
  → 72 institutions fédérales (comparativement à 70)
- Capteurs au niveau du réseau (NBS)
  → 84 institutions fédérales profitent de capteurs au périmètre de réseau.
- Capteurs virtuels au niveau du réseau (voir la section Protection du nuage à la page 24)
  → 5 institutions fédérales

Protection du nuage

MapleTap est un capteur infonuagique au niveau du réseau qui peut être déployé directement dans l'infrastructure d'un partenaire. À l'instar des autres capteurs, cette technologie a été mise au point par le Centre pour la cybersécurité pour détecter et contrer les cyberactivités suspectes. L'outil MapleTap a été lancé en janvier 2022, et en date de mars 2023, il comptait 10 déploiements uniques dans 5 institutions fédérales.

MapleTap est offert dans la place de marché infonuagique publique. Les responsables de la cyberdéfense peuvent se servir de l'outil et l'agrémenter pour renforcer leurs capacités de cyberdéfense. Le Centre pour la cybersécurité travaille aussi en étroite collaboration avec les fournisseurs infonuagiques. Par exemple, en octobre 2022, un grand fournisseur infonuagique a remercié l'équipe de MapleTap de lui avoir fait part d'une vulnérabilité réseau. Il s'agit d'un exemple parmi tant d'autres qui démontre que le Centre pour la cybersécurité contribue à renforcer les services infonuagiques pour des millions d'utilisatrices et utilisateurs dans le monde.

Sociétés d'État et petits ministères et organismes

Dans un rapport de 2022, le Comité des parlementaires sur la sécurité nationale et le renseignement[43] a attiré l'attention sur la vulnérabilité des sociétés d'État et petits ministères et organismes dont les infrastructures de TI ne sont pas protégées par les défenses de réseau du gouvernement. Le Comité a recommandé de maximiser le nombre d'institutions fédérales qui bénéficient des capteurs du CST pour détecter les cybermenaces sur leurs réseaux.

Le Centre pour la cybersécurité a intensifié ses communications auprès du secteur en question ces 3 dernières années. Depuis mars 2020, le nombre de sociétés d'État et de petits ministères et organismes qui ont adopté les capteurs est passé de 12 à 37 (sur 86).

Le Centre pour la cybersécurité considère toujours ce secteur comme une grande priorité et tente de mobiliser davantage d'institutions fédérales pour qu'elles adhèrent à ses services.

Voici le cumul total des sociétés d'État et des petits ministères et organismes qui participaient au programme de capteurs du CST en date du 31 mars de chaque année :

- Mars 2023 :
  → Sociétés d'État : 11
  → Petits ministères et organismes : 26
- Mars 2022 :
  → Sociétés d'État : 10
  → Petits ministères et organismes : 22
- Mars 2021 :
  → Sociétés d'État : 5
  → Petits ministères et organismes : 19
- Mars 2020 :
  → Sociétés d'État : 1
  → Petits ministères et organismes : 11

Le budget de 2022 propose du nouveau financement pour élargir la protection de la cybersécurité pour les petits ministères, les organismes et les sociétés d'État. Le financement représente, selon la comptabilité de caisse :

- 57,5 millions de dollars sur 5 ans à partir de l'année 2022 à 2023 et 12,8 millions de dollars par année suivante[44].

Déploiement de capteurs au niveau de l'hôte dans des institutions non fédérales

Cette année, le Centre pour la cybersécurité a aussi déployé plus de 5 100 capteurs au niveau de l'hôte pour protéger une institution non fédérale aux prises avec un grave cyberincident. Le déploiement d'urgence a été autorisé par la ministre de la Défense nationale. En effet, selon la *Loi sur le CST*, la ou le ministre peut désigner des systèmes non fédéraux comme étant d'importance pour le gouvernement du Canada. Grâce à cette désignation, le CST peut prendre des mesures pour protéger les systèmes au titre du volet de son mandat touchant la cybersécurité.

Tableau de bord de la posture de sécurité

ObservationDeck est une application Web interactive qui aide les ministères du gouvernement du Canada à se faire une meilleure idée de leur posture de cybersécurité.

Chaque partenaire peut consulter des données sur mesure sur des cybermenaces quotidiennes qui touchent les biens de son réseau. En cas de cyberincident, ObservationDeck permet aussi aux analystes du Centre pour la cybersécurité de jeter un coup d'œil rapide aux biens qui pourraient avoir été compromis.

Par le passé, ObservationDeck comprenait des données :

- de capteurs au niveau de l'hôte;
- de capteurs au niveau du réseau;
- de certains flux de données sur les menaces.

Depuis cette année, ObservationDeck comprend des données tirées de capteurs au niveau du nuage.

Voici le cumul total des ministères du gouvernement du Canada qui prenaient part à ObservationDeck en date du 31 mars de chaque année :

- Mars 2023 :
  → Ministères : 57
    - Avec CBS : 53
- Mars 2022 :
  → Ministères : 50
    - Avec CBS : 0

Collaboration avec les infrastructures essentielles

Il s'agit d'un fait connu : les infrastructures essentielles du Canada sont la cible d'activités de cybermenace.

Les cyberincidents qui surviennent dans ces secteurs clés peuvent causer des perturbations majeures et mettre en péril la santé et la sécurité de la population.

Au printemps de 2023, le Centre pour la cybersécurité a publié un cyberflash à l'intention de ses partenaires. Il portait sur un rapport confirmé qui indiquait qu'une ou un auteur de cybermenace avait la possibilité de causer des dommages physiques aux infrastructures essentielles du Canada. Il n'y a eu aucun dommage, mais la menace est bien réelle et présente.

Le budget de 2022 accordait du nouveau financement au CST pour améliorer sa capacité à prévenir les cyberattaques contre les infrastructures essentielles et à y réagir. Le financement représente, selon la comptabilité de caisse :

- 185,5 millions de dollars sur 5 ans à partir de l'année 2022 à 2023 et 40,6 millions de dollars par année suivante[45].

> **Les infrastructures essentielles demeurent des cibles de choix pour les cybercriminels et les auteurs parrainés par des États.**
>
> Évaluation des cybermenaces nationales 2023-2024[46]

Secteurs

Cette année, l'équipe des partenariats du Centre pour la cybersécurité a collaboré avec près de 1 400 organisations du secteur des infrastructures essentielles (une augmentation comparativement aux quelques 1 000 organisations de l'année précédente). Ces partenaires sont issus des secteurs suivants :

- Milieu universitaire
- Sociétés d'État
- Institutions démocratiques
- Énergie
- Finances
- Alimentation/Gestion de l'eau/Manufacture
- Santé
- Technologies de l'information et communications
- Provinces, territoires et municipalités
- Petites et moyennes organisations
- Transports

L'équipe qui se consacre au secteur de l'alimentation, de la gestion de l'eau et de la manufacture a été mise sur pied cette année.

Infrastructure énergétique

Le Centre pour la cybersécurité poursuit sa coopération avec ses partenaires du secteur de l'énergie dans le but de les informer sur les cybermenaces et de renforcer leur cybersécurité.

Les projets de coopération en cours comprennent :

- le Programme de la flamme bleue[47] (avec l'Association canadienne du gaz);
- l'initiative Lighthouse[48] (en anglais seulement) (avec la Société indépendante d'exploitation du réseau d'électricité de l'Ontario).

Les organisations participantes transmettent au Centre pour la cybersécurité des données sur leur réseau et reçoivent en échange des rapports de menace personnalisés.

Un nombre accru de partenaires du secteur de l'énergie se sont joints à ces initiatives cette année. Au cours de la prochaine année financière, le Centre pour la cybersécurité modifiera et actualisera ces programmes.

Évaluation des besoins

En octobre 2022, Sécurité publique Canada a lancé une nouvelle version de l'Outil canadien de cybersécurité[49] (OCC 2.0). L'OCC 2.0 a été conçu en collaboration avec le Centre pour la cybersécurité et est destiné aux fournisseurs d'infrastructures essentielles. Les organisations utilisent l'outil virtuel pour évaluer leur résilience technique comparativement aux pratiques exemplaires actuelles. Les données, recueillies par Sécurité publique Canada, servent aussi à cerner les lacunes les plus courantes en matière de résilience. Elles aident également le Centre pour la cybersécurité à planifier ses ressources afin de combler ces lacunes.

Projet pilote pour les municipalités

Les municipalités sont souvent ciblées par des attaques au rançongiciel. En effet, elles ont une grande exposition aux menaces (grand nombre de dispositifs, d'utilisatrices et utilisateurs et de données), mais disposent de budgets de cybersécurité plutôt limités.

Cette année financière, Sécurité publique Canada et le Centre pour la cybersécurité ont lancé un projet pilote qui vise à aider les municipalités canadiennes à cerner les lacunes dans leur cybersécurité.

En tout, 18 municipalités ont procédé à une autoévaluation virtuelle de leur cybersécurité au moyen de l'OCC 2.0. L'équipe-conseil du Centre pour la cybersécurité leur a ensuite expliqué les résultats de l'évaluation et les a aidées à cerner les priorités et à échafauder un plan d'action. Une des municipalités participantes a dressé un plan d'action approfondi et a offert de le transmettre à d'autres municipalités canadiennes.

Gestion d'incidents

> **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[50]

Lorsque des cyberincidents se produisent sur les réseaux du gouvernement fédéral ou des infrastructures essentielles du Canada, le Centre pour la cybersécurité est là pour aider.

Les cyberincidents sont variés, allant de tentatives d'hameçonnage de base aux activités sophistiquées perpétrées par des auteures et auteurs de menaces persistantes avancées. Ils peuvent mener à des compromissions, mais ce n'est pas nécessairement le cas.

L'équipe de gestion des incidents du Centre pour la cybersécurité offre des avis et des conseils spécialisés pour aider l'équipe de TI de l'organisation visée à atténuer les dommages et à remettre les systèmes en ligne. Une fois l'incident résolu, le Centre pour la cybersécurité assure un suivi auprès de la victime pour l'aider à repérer et à corriger les vulnérabilités dans son infrastructure de TI.

Cette année, le Centre pour la cybersécurité a ouvert 2 089 dossiers d'incident de cybersécurité. De ce nombre, 957 incidents visaient des institutions fédérales et 1 132 ciblaient des infrastructures essentielles.

Dans certains cas, l'équipe d'intervention en cas de cyberincident a prêté assistance à d'autres organisations gouvernementales au Canada ainsi qu'aux responsables de systèmes désignés comme étant d'importance pour le gouvernement fédéral.

Voici le nombre de dossiers de cyberincident ouverts par le Centre pour la cybersécurité au cours des 3 dernières années financières :

- 2022 à 2023 :
  → Total de dossiers : 2 089
  - Institutions fédérales : 957
  - Infrastructures essentielles : 1 132
- 2021 à 2022 :
  → Total de dossiers : 2 195
  - Institutions fédérales : 1 152
  - Infrastructures essentielles : 1 043
- 2020 à 2021 :
  → Total de dossiers : 2 047
  - Institutions fédérales : 881
  - Infrastructures essentielles : 1 166

(Les statistiques des années précédentes ont été mises à jour pour présenter des chiffres calculés selon la même méthodologie que cette année.)

Ces statistiques ne représentent qu'une fraction des incidents, car la grande majorité de ceux-ci ne sont pas signalés. Pourtant, les auteures et auteurs de cybermenace ne se contentent jamais de faire qu'une seule victime. Le CST presse donc les organisations canadiennes de signaler les cyberincidents[51] aux organismes d'application de la loi et au Centre pour la cybersécurité pour qu'ils puissent :

- offrir des avis et des conseils;
- avertir d'autres organisations.

Réseaux internationaux

Le Centre pour la cybersécurité est l'équipe nationale d'intervention en cas d'incident lié à la sécurité informatique (CSIRT pour *Computer Security Incident Response Team*) du Canada. Il travaille avec d'autres équipes nationales de partout dans le monde pour échanger de l'information et pour aider chaque pays à se préparer à faire face aux cybermenaces et à y réagir plus efficacement.

Cette année, le Centre pour la cybersécurité a adhéré au CSIRTAmericas Network, une collectivité composée de 36 CSIRT représentant 21 pays d'Amérique.

De tels réseaux constituent d'importantes plateformes d'échange qui permettent d'améliorer la cybersécurité collective.

Renseignement sur les cybermenaces

Le programme de renseignement sur les cybermenaces du CST est axé sur la communication de renseignement étranger sur les cybermenaces contre le Canada et ses intérêts.

Cette année, le programme a continué de permettre de détecter et de surveiller les tactiques, les techniques et les procédures dont se sont servis les auteures et auteurs de menace dotés de moyens sophistiqués, parrainés par des États ou non, ainsi que les cybercriminelles et cybercriminels, et d'enquêter sur ces tactiques, techniques et procédures.

Le programme aide à contrer ces activités en fournissant du renseignement opportun et exploitable sur la manière dont ces auteures et auteurs malveillants mènent leurs activités.

Il fait en sorte de protéger les systèmes fédéraux, les infrastructures essentielles du Canada, nos alliés et d'autres systèmes d'importance pour le gouvernement du Canada.

Communication d'information sur les cybermenaces à nos partenaires

Le Centre pour la cybersécurité transmet de l'information sur les cybermenaces de plusieurs façons à ses partenaires du gouvernement et des infrastructures essentielles.

Flux automatisé de renseignements sur les menaces

Aventail est le service de diffusion automatisé de renseignements sur les menaces du Centre pour la cybersécurité. Il transmet des détails techniques sur les activités de cybermenace, appelés des indicateurs de compromission. Entre autres, on compte parmi ces indicateurs, les suivants :

- domaines Web malveillants;
- adresses URL malveillantes;
- adresses IP malveillantes;
- codes de hachage malveillants.

Le Centre pour la cybersécurité examine ces indicateurs de compromission et les communique à ses partenaires du gouvernement et des infrastructures essentielles pour qu'ils puissent protéger leurs réseaux contre ces menaces connues. (Le CST s'assure que ses partenaires respectent ses exigences juridiques et politiques avant de leur donner accès à Aventail.)

De plus, le Centre pour la cybersécurité met également Aventail à la disposition de plusieurs organisations partenaires dans le cadre d'accords de redistribution. Ce faisant, ces organisations peuvent faire usage d'Aventail pour aider à protéger les Canadiennes et les Canadiens (voir la section Soutien pour protéger les appareils des Canadiennes et Canadiens à la page 36).

Jusqu'à cette année, seuls les partenaires ayant un serveur dédié pouvaient ingérer Aventail. En décembre 2022, le Centre pour la cybersécurité a lancé une application Web permettant aux plus petites organisations du secteur des infrastructures essentielles d'accéder au flux de menaces. Les nouveaux partenaires peuvent dorénavant se prévaloir du flux de communication entre machines, de l'application Web ou des deux.

Au cours de l'année, Aventail a transmis 37 000 indicateurs de compromission uniques. Il s'agit d'une moyenne quotidienne d'un peu plus de 100 indicateurs de compromission.

Voici le nombre total d'organisations inscrites à Aventail en date du 31 mars de chaque année :

- Mars 2023 :
  → Nombre total de partenaires : 152
  - Institutions fédérales : 20
  - Infrastructures essentielles : 132
- Mars 2022 :
  → Nombre total de partenaires : 120
  - Institutions fédérales : 13
  - Infrastructures essentielles : 107

Notifications

Le Centre pour la cybersécurité envoie différents types de notifications à la collectivité de la cybersécurité.

Sur son site Web et ses médias sociaux, il publie :

- des avis sur les problèmes courants de cybersécurité;
- des alertes sur les vulnérabilités critiques.

Les partenaires du Centre pour la cybersécurité peuvent également s'inscrire pour recevoir :

- des cyberflashs : notifications urgentes envoyées par courriel qui contiennent de l'information sensible ne pouvant pas être rendue publique;
- des avis du Système national de notification de cybermenace (SNNC) : mises à jour quotidiennes sur les maliciels et les vulnérabilités dans l'espace d'adressage IP des partenaires;
- des tableaux de bord : résumé mensuel des données du SNNC qui compare les pratiques exemplaires en cybersécurité d'un abonné avec celles de ses pairs anonymisés dans son secteur.

Au cours de l'année, le Centre pour la cybersécurité a transmis :

- 737 avis;
- 21 alertes;
- 14 cyberflashs.

Voici le nombre d'organisations inscrites à ses services de notification en date du 31 mars 2023 :

- Cyberflashs : 960 organisations (comparativement à 790 lors de l'année précédente)
- SNNC : plus de 1 000 organisations (comparativement à 750)
- Tableaux de bord : 214 organisations (comparativement à 179)

Mobilisation de la collectivité

Le Centre pour la cybersécurité a continué cette année de mobiliser ses partenaires des infrastructures essentielles en tenant :

- des séances d'information sur les cybermenaces :
  - → appels vidéo chaque 2 semaines organisés par le Centre pour la cybersécurité et auxquels assistaient régulièrement plus de 600 partenaires,
  - → appels de la collectivité visant des secteurs particuliers organisés par des partenaires de l'industrie et auxquels assistaient des spécialistes du Centre pour la cybersécurité;
- 10 séances d'information « Passons à l'action » : séances techniques approfondies de 30 minutes abordant un sujet précis;
- 161 conférences publiques.

Analyse de maliciels

Assemblyline[52] est la plateforme de détection et d'analyse des maliciels du Centre pour la cybersécurité.

Les partenaires et les capteurs de défense soumettent des fichiers suspects aux fins d'analyse. Assemblyline en fait l'analyse au moyen de technologies avancées de détection des maliciels et fournit les résultats en quelques minutes, ainsi que des détails permettant d'éclairer les mesures à prendre.

Au cours de l'année, Assemblyline a analysé plus d'un milliard de fichiers suspects.

Voici le nombre d'organisations inscrites à Assemblyline en date du 31 mars :

- Mars 2023 :
  - → Nombre total de partenaires : 228
    - Gouvernement du Canada : 45
    - Infrastructures essentielles : 183
- Mars 2022 :
  - → Nombre total de partenaires : 165
    - Gouvernement du Canada : 32
    - Infrastructures essentielles : 133

Les maliciels évoluent constamment, et les auteures et auteurs de menace conçoivent sans arrêt de nouvelles manières de les installer. C'est pourquoi les analystes du Centre pour la cybersécurité s'efforcent tout au long de l'année d'ajouter de nouvelles capacités de détection dans Assemblyline, en fonction des méthodes et des types de maliciels les plus récents.

Conseils au gouvernement et aux infrastructures essentielles

Le Centre pour la cybersécurité est l'autorité technique du Canada en matière de cybersécurité.

Il donne des conseils aux ministères fédéraux sur la façon de protéger leurs biens de TI, l'information qu'ils détiennent et leurs services à la population.

Par exemple, il conseille Emploi et Développement social Canada (EDSC) sur un projet pluriannuel visant à transformer la manière de verser les prestations. L'objectif est de concevoir une plateforme numérique conviviale qui simplifiera et accélérera le processus pour demander et recevoir des prestations, comme l'assurance-emploi et la pension de la Sécurité de vieillesse. L'établissement de normes strictes de cybersécurité dès le départ garantira que la nouvelle plateforme :

- soit résiliente contre les rançongiciels et d'autres cyberattaques;
- protège les renseignements personnels des Canadiennes et des Canadiens.

Le Centre pour la cybersécurité conseille également les fournisseurs d'infrastructures essentielles du Canada à propos des problèmes de cybersécurité qui peuvent les affecter.

Par exemple, il a créé cette année une communauté d'intérêts axée sur la cybersécurité des systèmes de contrôle industriels (SCI). Ce sont des systèmes électroniques qui contrôlent la machinerie ou les processus industriels. S'ils sont connectés à l'Internet, ils deviennent une cible de grande valeur pour les auteures et auteurs de cybermenace. En date de mars 2023, environ 40 partenaires du gouvernement et de l'industrie ont intégré la communauté d'intérêts. Cette communauté permet au Centre pour la cybersécurité de mieux comprendre les besoins et d'offrir des conseils approfondis en matière de cybersécurité.

> **[Les SCI sont] une cible de choix pour les auteurs de menace, puisque ces derniers peuvent en tirer avantage pour avoir de réelles répercussions sur la population, que ce soit en causant de petits désagréments (p. ex. allumer et éteindre les lumières) ou en provoquant des incidents ou [sic] susceptibles d'entraîner des coûts importants ou de poser un danger à la vie humaine (p. ex. entraîner la défaillance de l'équipement ou des dommages permanents).**
>
> Centre pour la cybersécurité, Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels[53]

Formation en matière de cybersécurité

Le Carrefour de l'apprentissage offre de la formation en cybersécurité et en sécurité des communications (COMSEC pour *Communications Security*) aux fonctionnaires et aux membres du personnel des infrastructures essentielles.

Avant la pandémie, le Carrefour de l'apprentissage n'offrait de la formation qu'en personne. Toutefois, depuis les 3 dernières années, il a monté un catalogue de cours en ligne à rythme libre et de cours virtuels donnés par une instructrice ou un instructeur. Ce faisant, le Carrefour de l'apprentissage a pu joindre plus d'apprenantes et apprenants au Canada.

La participation à des cours en ligne au cours de l'année financière était 4 fois plus forte que l'année précédente. Dans l'ensemble, la participation à des cours du Carrefour de l'apprentissage a plus que doublé. Le Carrefour de l'apprentissage a créé une nouvelle équipe dont l'objectif est d'améliorer l'expérience d'apprentissage en ligne.

Le Carrefour de l'apprentissage de 2022 à 2023 :

- 8 422 participantes et participants (une augmentation de 123 %)
- Format :
  - → 70 % de cours en ligne
  - → 30 % de cours dirigés par une instructrice ou un instructeur (en virtuel ou en personne)
- Public :
  - → 98 % du gouvernement du Canada
  - → 2 % des infrastructures essentielles

Formation à l'intention des fonctionnaires

Afin de garantir la sécurité des systèmes du gouvernement, il est important que toutes et tous les fonctionnaires appliquent les pratiques exemplaires en cybersécurité. Au cours de l'année, le Centre pour la cybersécurité a collaboré avec l'École de la fonction publique du Canada pour développer le Parcours d'apprentissage : Découvrez la cybersécurité[54]. Le parcours comprend :

- 1 nouveau cours en ligne : À la découverte de la cybersécurité;
- 3 cours existants donnés par des instructrices ou instructeurs;
- des vidéos et des ressources de Pensez cybersécurité;
- des documents d'orientation du Centre pour la cybersécurité.

Le Carrefour de l'apprentissage a également lancé un cours d'une journée donné par une instructrice ou un instructeur portant sur les pratiques exemplaires en cybersécurité à l'intention des fonctionnaires et des membres du personnel des infrastructures essentielles.

Résilience numérique des **Canadiennes et Canadiens**

Le Centre pour la cybersécurité aide à protéger les Canadiennes et les Canadiens contre les cybermenaces en effectuant des activités de sensibilisation, en collaborant avec des partenaires afin de détecter et d'éliminer les menaces, ainsi qu'en faisant la promotion des compétences en cybersécurité.

Pensez cybersécurité

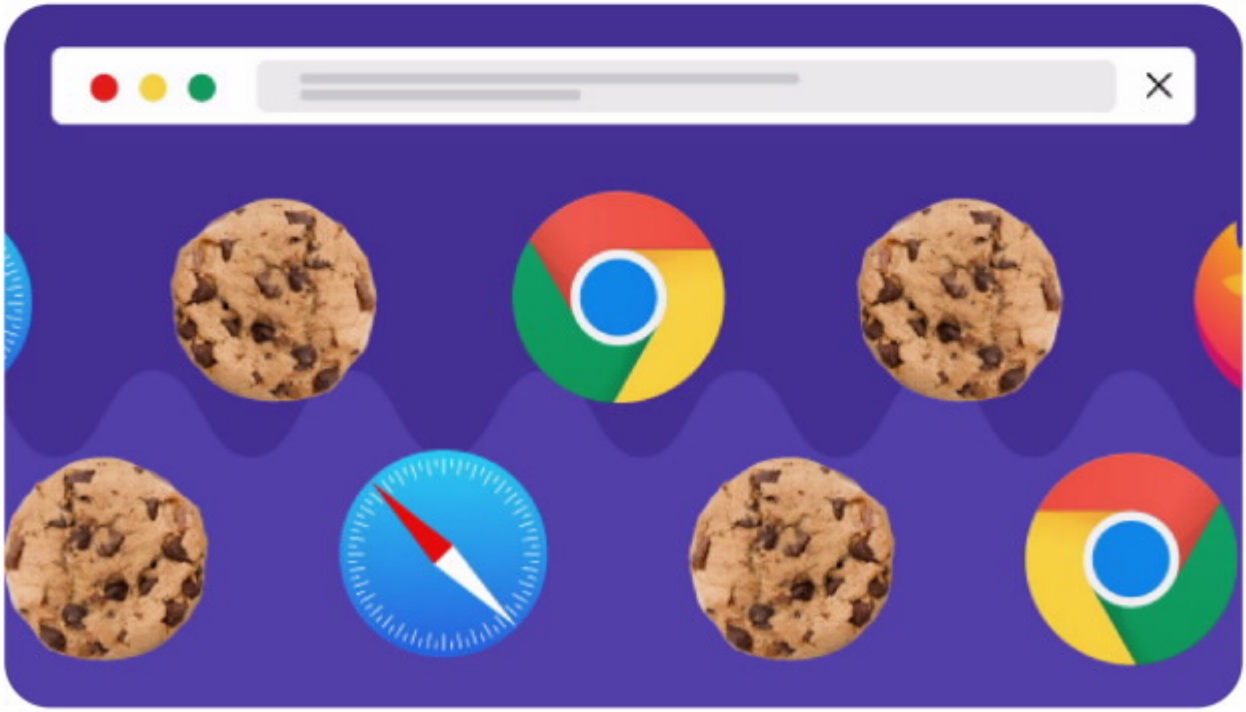
Pensez cybersécurité[55] est une campagne de sensibilisation publique nationale visant à informer la population canadienne sur les mesures simples à prendre pour se protéger en ligne.

Durant l'année, Pensez cybersécurité a continué de faire la promotion de ses ressources les plus populaires, qui informent les Canadiennes et les Canadiens sur la cybersécurité au quotidien. Elle a également produit une cinquantaine de nouveaux produits, comme :

- Comment sécuriser vos opérations financières en ligne[56];
- Ce qu'il faut savoir sur les cookies Internet[57];
- Identifier les signes d'un arnacœur sur les plateformes de rencontre[58];
- Que faire si vous êtes victime d'une tentative d'hameçonnage[59].

Pensez cybersécurité travaille sur les 6 grosses campagnes suivantes pendant l'année :

- la sensibilisation à la cybersécurité pour les personnes âgées (juin);
- la campagne de retour à l'école pour les étudiantes et étudiants du postsecondaire (septembre);
- le Mois de la sensibilisation à la cybersécurité (octobre);
- la campagne publicitaire « Ne vous laissez pas prendre » (octobre);
- la campagne des Fêtes de Pensez cybersécurité (novembre à janvier);
- le Mois de la prévention de la fraude (mars).



Mois de la sensibilisation à la cybersécurité

Le Mois de la sensibilisation à la cybersécurité a lieu chaque année au mois d'octobre. Le thème de la campagne en 2022 était « Combattez l'hameçonnage : Gâchez la journée d'un cybercriminel ».

Pensez cybersécurité a produit plusieurs ressources dans le cadre du Mois de la sensibilisation à la cybersécurité[60], notamment une trousse à outils pour les champions, des billets de blogue, des infographies, des vidéos, un jeu-questionnaire interactif sur l'hameçonnage et un chant de l'hameçonnage[61].

En tout, 7 partenaires ont aidé Pensez cybersécurité à créer du contenu, soit :

- l'Agence du revenu du Canada;
- Innovation, Sciences et Développement économique Canada;
- les Cadets du Canada;
- l'Association des banquiers canadiens;
- le Bureau d'assurance du Canada;
- Microsoft Canada;
- National Cybersecurity Alliance et CybSafe.

Ce sont 350 champions qui ont transmis du contenu du Mois de la sensibilisation à la cybersécurité à leur public (comparativement à 247 en 2021).

Au total, le contenu de la campagne a été vu 350 000 fois, un chiffre légèrement inférieur comparativement à 390 000 expositions en 2021.

Campagne publicitaire « Ne vous laissez pas prendre »

Pensez cybersécurité a également tenu une campagne publicitaire sur l'hameçonnage ayant pour nom « Ne vous laissez pas prendre »[62] pendant le Mois de la sensibilisation à la cybersécurité. Les publicités ont été vues 47 millions de fois, dont 6,1 millions de vues sur les vidéos. En octobre 2022, les visites sur le site Web de Pensez cybersécurité ont également triplé en raison de la campagne (124 000 visites au total, comparativement à 39 000 visites en octobre 2021).

Campagne des Fêtes de Pensez cybersécurité

Pendant la période des Fêtes, Pensez cybersécurité a travaillé avec des partenaires stratégiques, dont le Centre antifraude du Canada (CAFC) et la Gendarmerie royale du Canada (GRC), afin de créer du contenu, par exemple :

- Partenaires fédéraux rappellent aux consommateurs canadiens d'être vigilants envers les cybermenaces au cours des soldes du Vendredi fou et du Cyberlundi[63] (en partenariat avec le CAFC et la GRC)
- Les 12 escroqueries du temps des Fêtes[64] (en partenariat avec le CAFC)
- Adoptez des habitudes de jeu sensées pendant le temps des Fêtes[65] (en partenariat avec la plateforme de jeu Roblox)

Pensez cybersécurité a également créé la toute première fête du Cyberdéballage[66] ayant pour seul objectif de configurer les nouveaux appareils afin qu'ils soient cybersécurisés.

Mois de la prévention de la fraude

Pendant le Mois de la prévention de la fraude 2023, Pensez cybersécurité a collaboré avec la GRC et le CAFC afin de produire des ressources portant sur les techniques frauduleuses les plus courantes en ligne, y compris :

- les stratagèmes d'investissement[67];
- le harponnage[68];
- les escroqueries de services[69];
- l'hameçonnage[70];
- la boîte à outils du fraudeur[71].

L'établissement de relations solides demeure une priorité pour Pensez cybersécurité en vue d'accroître la portée de ses campagnes au pays.

Rapports et conseils

Le Centre pour la cybersécurité publie des rapports sur les menaces et des conseils en ligne afin que toute la population puisse accéder à de l'information de qualité sur la cybersécurité.

En octobre 2022, le Centre pour la cybersécurité a publié l'Évaluation des cybermenaces nationales (ECMN) 2023-2024[72].

Ce rapport emblématique est publié tous les 2 ans. Il s'appuie sur des sources classifiées et non classifiées pour cerner des tendances clés dans l'environnement de cybermenaces. Cette édition du rapport se concentre sur 5 tendances :

- les rançongiciels;
- les menaces contre les infrastructures essentielles;
- les cyberactivités parrainées par des États;
- la désinformation en ligne;
- les technologies perturbatrices.

Pour accompagner l'ECMN, le Centre pour la cybersécurité a publié des conseils abordant ces 5 tendances[73] et une mise à jour de son document « Introduction à l'environnement de cybermenaces[74] ».

Au cours de l'année, le Centre pour la cybersécurité a publié :

- 4 rapports et évaluations;
- 51 publications contenant des avis et de l'orientation :
  → 40 nouvelles publications,
  → 11 mises à jour.

Refonte du site Web

En mai 2022, le Centre pour la cybersécurité a revu son site Web[75] afin d'améliorer l'accessibilité pour les personnes handicapées et de faciliter la recherche de contenu pertinent. La page d'accueil permet maintenant aux utilisatrices et aux utilisateurs de sélectionner de l'information pour :

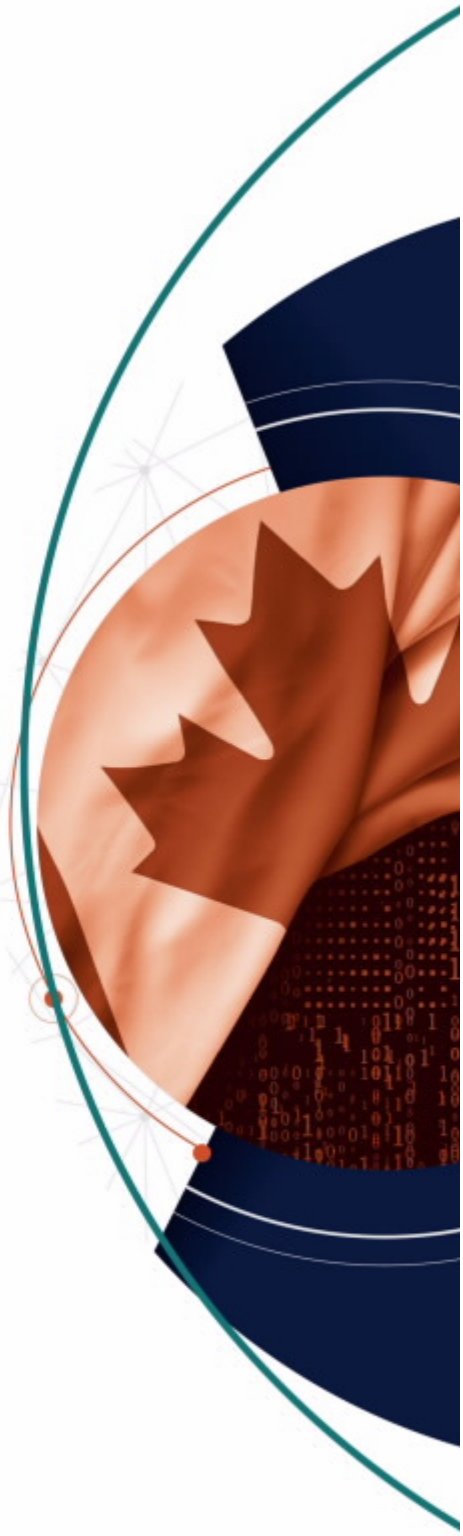
- le grand public;
- les petites et moyennes entreprises;
- les grandes organisations et infrastructures;
- les institutions gouvernementales;
- le milieu universitaire.

Le bouton « Signaler un cyberincident » est plus facile à trouver au haut de la page d'accueil. Il oriente plus clairement les Canadiennes et les Canadiens vers l'organisme qui peut le mieux répondre à leur situation.

Médias sociaux

Les médias sociaux sont l'un des moyens les plus importants pour le CST de transmettre de l'information à la population canadienne, y compris un grand nombre des points saillants mentionnés dans le présent rapport, comme :

- la mise au jours des campagnes de désinformation de la Russie;
- le Mois de la sensibilisation à la cybersécurité;
- l'Évaluation des cybermenaces nationales.



Les médias sociaux en chiffres

Le CST, le Centre pour la cybersécurité et Pensez cybersécurité ont chacun une présence distincte sur les médias sociaux. Au total, ils détiennent ensemble 17 comptes sur 5 plateformes de médias sociaux.

Au cours de l'année financière, le contenu de ces comptes a été vu plus de 5,2 millions de fois (un chiffre inférieur aux 6,6 millions de l'année précédente).

Le nombre total d'abonnements est passé de 172 500 à 184 000.

En date du 31 mars 2023, le nombre d'abonnements combinés en anglais et en français pour chaque compte (arrondi au millier le plus près) s'élevait à :

Plateforme	Compte	Abonnés	Changement
Twitter	CST	22 000	Augmentation de 5 %
	Centre pour la cybersécurité	32 000	Augmentation de 18 %
	Pensez cybersécurité	54 000	Diminution 1,8 %
Facebook	Pensez cybersécurité	52 000	Aucun changement
LinkedIn	CST	15 000	Augmentation de 50 %
	Pensez cybersécurité	2 000	Aucun changement
Instagram	CST	3 000	Augmentation de 50 %
	Pensez cybersécurité	3 000	Aucun changement
YouTube	CST	1 000	Augmentation de 100 %

Recherche de domaines malveillants

Les domaines, comme Canada.ca, sont comme les voisinages de l'Internet. Les auteures et auteurs de menace se servent de domaines malveillants pour mener des activités comme :

- héberger des sites Web frauduleux;
- envoyer des courriels d'hameçonnage;
- diffuser des maliciels.

Le Centre pour la cybersécurité cherche ces domaines malveillants de plusieurs façons, notamment :

- les flux de source ouverte et de menaces commerciaux;
- les capteurs de données sur les réseaux du gouvernement;
- les cyberincidents signalés au Centre pour la cybersécurité;
- la recherche proactive de cybermenaces;
- les soumissions de partenaires de l'industrie (voir la section Protection des Canadiennes et Canadiens contre l'hameçonnage et l'hameçonnage par message texte à la page 35).

Une fois qu'il a examiné l'information et a éliminé les doublons, le Centre pour la cybersécurité prend des mesures pour atténuer la menace des domaines malveillants, comme :

- les bloquer sur les réseaux du gouvernement du Canada;
- en transmettre les détails par les flux de menaces;
- charger les partenaires de confiance de les bloquer ou de les éliminer de l'Internet (voir la section Mesures d'atténuation à la page 36).

Protection des Canadiennes et Canadiens contre l'hameçonnage et l'hameçonnage par message texte

Une des façons les plus courantes qu'utilisent les auteures et auteurs de menace pour inciter les Canadiennes et Canadiens à visiter des domaines malveillants est l'hameçonnage (par courriel) ou l'hameçonnage par message texte. Ces messages contiennent souvent des liens qui dirigent vers des domaines malveillants qui vous incitent à inscrire vos mots de passe ou vos renseignements de carte de crédit. Ils peuvent également installer des maliciels sur votre appareil.

Les fournisseurs d'infrastructures essentielles, en particulier les secteurs des finances, des TI et des télécommunications, jouent un rôle crucial afin de protéger la population canadienne contre les tentatives d'hameçonnage et d'hameçonnage par message texte.

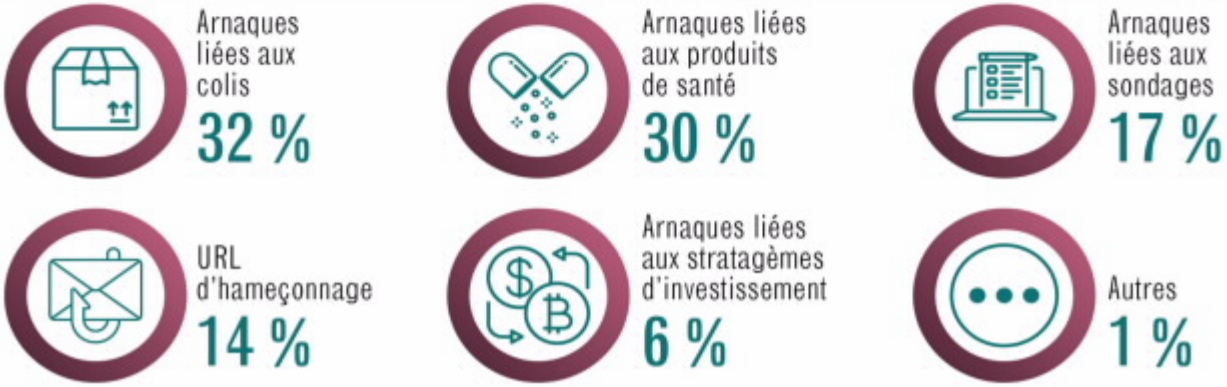
Le Centre pour la cybersécurité travaille avec d'importants partenaires dans ce secteur depuis 2019 afin de recueillir le contenu malveillant aux fins d'analyse. Aucune information des utilisatrices ou des utilisateurs n'est transmise au Centre pour la cybersécurité dans le cadre de cette initiative, seulement le contenu des messages.

En 2021, le Centre pour la cybersécurité a lancé Fox, une plateforme qui ingère les données de partenaires plus facilement. Au cours de l'année, les partenaires ont utilisé Fox pour soumettre environ :

- 850 000 adresses URL (liens Web) dont :
  → 274 000 adresses malveillantes,
  → 12 700 nouvelles découvertes.

Le Centre pour la cybersécurité transmet ces adresses URL aux partenaires participants afin qu'ils puissent les utiliser pour protéger leur clientèle.

Types d'arnaques les plus courants soumis par les partenaires au cours de l'année



Mesures d'atténuation

Durant la pandémie, le Centre pour la cybersécurité a commencé à travailler avec des partenaires commerciaux de confiance afin de retirer les sites Web et les domaines de courriel imitant ceux d'institutions fédérales.

En juillet 2021, il a élargi ses demandes de mesure d'atténuation pour inclure d'autres sources de contenu malveillant. Elles comptent celles que lui transmettent les partenaires des infrastructures essentielles (voir la section Protection des Canadiennes et Canadiens contre l'hameçonnage et l'hameçonnage par message texte à la page 35).

Voici le nombre de domaines malveillants bloqués ou retirés par les partenaires au cours des 3 dernières années :

- 2022 à 2023 :
  → Usurpation de domaines du gouvernement du Canada : 3 167
  → Autres domaines malveillants : 306 000
- 2021 à 2022 :
  → Usurpation de domaines du gouvernement du Canada : 2 943
  → Autres domaines malveillants : 312 000
- 2020 à 2021 :
  → Usurpation de domaines du gouvernement du Canada : 7 348
  → Autres domaines malveillants : 0

Soutien pour protéger les appareils des Canadiennes et Canadiens

Le Centre pour la cybersécurité maintient un partenariat avec l'organisme sans but lucratif ACEI afin d'aider les Canadiennes et les Canadiens à protéger leurs appareils personnels contre les maliciels et les tentatives d'hameçonnage.

Le Bouclier canadien de l'ACEI est un service gratuit qui sert à protéger la vie privée des Canadiennes et des Canadiens lorsqu'ils naviguent le Web. Il s'agit d'une option qui permet de bloquer les menaces en empêchant les utilisatrices et les utilisateurs de se connecter à des sites Web malveillants connus. Il peut être téléchargé comme application mobile ou utilisé pour configurer des appareils personnels, y compris des routeurs domestiques. La liste de sites bloqués du Bouclier canadien est montée à partir du renseignement sur les menaces du Centre pour la cybersécurité ainsi que des données d'autres partenaires de l'ACEI.

Au cours de l'année financière, le nombre d'utilisatrices et d'utilisateurs inscrits aux services de blocage de sites Web du Bouclier canadien est passé de 177 000 à 279 000. Le service a enregistré plus de 215 millions blocages entre mars 2022 et mars 2023.

Sensibilisation communautaire

Le programme d'approche communautaire du CST vise à inspirer les jeunes Canadiennes et Canadiens et à les rendre passionnés par la technologie et le codage. L'objectif est d'appuyer la création d'un effectif robuste en cybersécurité au Canada.

Le CST souhaite tout particulièrement atteindre les jeunes faisant partie de groupes sous-représentés dans les domaines techniques, dont les filles, les élèves non binaires et les jeunes des communautés noires et autochtones.

Au cours de l'année, les bénévoles du CST ont pu recommencer à participer à des événements de sensibilisation en personne, notamment les suivants :

- 7 ateliers Raspberry Pi dans 3 écoles d'Ottawa;
- des cyberjournées dans 2 classes d'élèves surdouées et surdoués d'Ottawa (en collaboration avec le Conseil des technologies de l'information et des communications).

> **Un grand merci pour votre dévouement à faire découvrir la cybersécurité à nos élèves! Chaque élève a pu apprendre quelque chose de nouveau, beaucoup de choses même. Nombre d'élèves envisagent désormais une carrière en TI à la suite des activités stimulantes auxquelles elles et ils ont participé. Quel succès!**
>
> Enseignante du programme d'apprenantes et d'apprenants surdoués, Commission scolaire catholique d'Ottawa

Le CST a participé à des marathons de programmation et à d'autres événements virtuels avec ses partenaires, dont les suivants :

- Hackergal;
- CyberTitan.

Il a également mis sur pied 3 nouveaux partenariats avec les groupes suivants :

- Actua;
- Black Boys Code;
- Département de mathématiques et de statistique de l'Université d'Ottawa.

Collaboration avec des partenaires autochtones

Le Centre pour la cybersécurité collabore avec des partenaires autochtones afin de renforcer la cybersécurité dans leurs communautés.

Au cours de l'année, le Centre pour la cybersécurité a organisé des séances d'information en cybersécurité avec de nombreuses organisations partout au Canada, y compris des organisations des gouvernements territoriaux et des organismes autochtones.

Le CST a créé des liens avec des organismes autochtones et a mis à leur disposition des ressources en cybersécurité, notamment lors des événements suivants :

- Indigenous Technology Summit (Halifax, septembre 2022);
- Assemblée spéciale des chefs de l'Assemblée des Premières Nations (Ottawa, décembre 2022);
- Inuit Technology Forum (Iqaluit, mars 2023).

En juin 2022, le Centre pour la cybersécurité a organisé la finale canadienne de la compétition Cyber*Sci[76]. Cyber*Sci est un organisme sans but lucratif qui travaille avec les jeunes talents en cybersécurité aux quatre coins du Canada. À la demande du CST, une première équipe composée de jeunes Autochtones seulement a participé à la compétition. L'événement a mis de l'avant les compétences des participantes et des participants, leur permettant également de se créer un réseau professionnel.

Promotion du talent en cybersécurité

Le Canada manque de personnes qualifiées dans le domaine de la cybersécurité.

Le Centre pour la cybersécurité a soutenu le développement des compétences en cybersécurité au Canada au cours de l'année en :

- conseillant des établissements d'enseignement sur le contenu de leur programme d'enseignement;
- produisant des ressources sur la cybersécurité à l'intention des élèves et des enseignantes et enseignants;
- identifiant les déficits dans les compétences avec l'aide de partenaires de l'industrie et du milieu universitaire;
- actualisant ses ressources, dont :
  → le Guide sur les carrières en cybersécurité[77],
  → la publication « Certifications dans le domaine de la cybersécurité[78] ».

> **Le nombre d'emplois en cybersécurité au Canada ne cesse de croître chaque année. Cette tendance ne se remarque pas uniquement au Canada. Il y a des millions de postes vacants dans le domaine de la cybersécurité aux quatre coins du monde.**
>
> Guide sur les carrières en cybersécurité[79]

Innovation

La technologie évolue rapidement. Afin de suivre ce rythme, le CST encourage une culture d'innovation constante, notamment par la recherche et des événements de collaboration.

Recherche

Le CST mène des recherches dans le cadre de sa mission afin de protéger le Canada et de contribuer plus généralement à la collectivité de la cybersécurité.

Le budget de 2022 proposait du financement supplémentaire en vue d'améliorer les capacités en cybersécurité du Canada en investissant dans la recherche. Le CST a depuis obtenu 44,5 millions de dollars sur 9 ans pour financer la recherche universitaire sur les technologies de pointe qui sont pertinentes dans le cadre des activités du CST.

Cet important investissement lui permettra d'élargir ses activités de recherche et de renforcer ses capacités.

Institut Tutte pour les mathématiques et le calcul

Les chercheuses et chercheurs de l'Institut Tutte pour les mathématiques et le calcul (ITMC)[80] du CST travaillent avec leurs collègues du CST ainsi que les partenaires de la collectivité des cinq, de l'industrie et du milieu universitaire afin de relever les plus gros défis liés à la mission du CST.

Un des principaux sujets à l'étude cette année était celui des campagnes d'ingérence étrangère sur les médias sociaux. Les chercheuses et chercheurs du CST ont produit un « carnet de problèmes » détaillé qui relève les difficultés à détecter les campagnes malveillantes d'ingérence étrangère. Ils ont également fourni des outils visant à détecter les activités coordonnées.

Les autres activités de recherche comprenaient :

- le développement de cartes de données et l'analyse de données exploratoires;
- la mobilisation des partenaires de l'industrie afin de développer et de mettre à l'essai des méthodes de calcul sécurisé dans des environnements non sécurisés;
- l'amélioration des outils et des flux de travaux pour rendre possible une science des données éthique et robuste, qui peut facilement être reproduite et interprétée;
- la recherche à l'appui des processus de normalisation de la cryptographie post-quantique.

L'ITMC a redonné au milieu universitaire en :

- organisant 2 conférences;
- donnant 6 présentations de recherche;
- participant à 7 ateliers spéciaux et conférences;
- publiant du contenu dans plus de 10 revues, comptes rendus de conférence et manuels;
- dirigeant des panels sur l'équité, la diversité et l'inclusion dans les STIM;
- donnant des conférences dans des universités locales;
- siégeant au comité de la Société mathématique du Canada.

La bibliothèque de logiciels de l'ITMC a vu une moyenne de 2,5 millions de téléchargements par mois au cours de l'année.

En novembre 2022, le Museum of Modern Art (MoMA) a exposé de l'art généré au moyen de l'algorithme UMAP[81], une technique développée par un chercheur du CST.

> **C'est stupéfiant de voir que mon travail se rend jusqu'au MoMA. Il existe des liens étroits entre les mathématiques abstraites et l'art. Refik Anadol les transpose concrètement dans ses œuvres.**
>
> Leland McInnes, chercheur au CST, sur Artnet News[82] (en anglais seulement)

Recherche appliquée

Le personnel du CST travaillant en recherche appliquée[83] explore les défis actuels et éventuels auxquels est confronté le CST dans le cadre de sa mission. Le CST crée des solutions qui lui permettent d'accroître ses capacités.

Au cours de l'année, le CST a eu recours à la science des données pour mettre au point les produits suivants visant à appuyer le travail des analystes :

- un **logiciel de traduction automatique pour les langues essentielles à la mission** qui est plus rapide et exact que les méthodes disponibles auparavant. Créé en collaboration avec des partenaires du SIGINT, le logiciel se sert de l'apprentissage machine;
- un **ensemble de services d'analyse d'images** pour traiter et enrichir la collection de données et mener des recherches dans la collection;
- des **outils de triage des données relatives à la mission** au moyen d'outils de la science des données pour analyser les textes et déterminer les sujets;
- des **outils permettant aux analystes du renseignement étranger et du renseignement électromagnétique** de mieux comprendre et détecter les influences et les effets.

Le CST a également créé un nouveau module de détection des maliciels dans les fichiers qui exécutent diverses fonctions ou actions dans un ordinateur. Le module a été intégré à l'outil public du CST Assemblyline[84] afin de trier et d'analyser les maliciels.

Recherche sur les vulnérabilités

Dans le cadre de son mandat, le CST effectue des recherches sur les vulnérabilités[85] afin de découvrir des faiblesses liées à la cybersécurité dont pourraient profiter les auteures et auteurs de menace. Il se fie à son Cadre de gestion du partage des nouvelles capacités[86] pour déterminer s'il est dans l'intérêt primordial en matière de sécurité du Canada et de la population canadienne de révéler une vulnérabilité.

Au cours de l'année, nos chercheuses et chercheurs ont :

- découvert plusieurs vulnérabilités à fort impact et les a divulguées aux fournisseurs concernés;
- lancé une nouvelle initiative d'exploration des préoccupations en matière de cybersécurité liées à une vaste gamme de logiciels et de matériels de l'Internet des objets.

Le CST a accru ses activités de collaboration avec le milieu universitaire dans le domaine de la recherche sur les vulnérabilités afin de joindre les jeunes talents techniques au Canada.

Comme par les années passées, nombre de chercheuses et chercheurs du CST ont contribué à des événements de collaboration, comme la Grande exploration et la GeekWeek.

Événements de collaboration

Le CST encourage l'innovation en tenant des ateliers de cybersécurité et d'autres événements de collaboration. Les partenaires du gouvernement, de l'industrie, du milieu universitaire et des alliés internationaux examinent ensemble des problèmes actuels et futurs en lien avec la mission du CST.

GeekWeek

La GeekWeek est l'atelier de cybersécurité non classifié du Centre pour la cybersécurité.

D'avril à mai 2022, la GeekWeek 7.5 s'est tenue en mode virtuel en raison des restrictions imposées par la pandémie.

Les équipes ont exploré de nombreux sujets, dont :

- l'amélioration des capacités d'analyse de maliciels;
- la réduction du nombre de faux positifs dans la détection de cybermenaces;
- l'amélioration de la cybersécurité :
  - → de l'infrastructure infonuagique,
  - → des appareils de l'Internet des objets (IdO);
- l'exploration des façons dont les auteures et auteurs malveillants peuvent exploiter :
  - → l'infrastructure de télécommunications 5G,
  - → les véhicules connectés;
- la recherche de cryptomonnaies liées à une activité malveillante et au blanchiment d'argent;
- l'utilisation de l'apprentissage machine pour détecter des courriels d'hameçonnage.

Toute l'année, le Centre pour la cybersécurité cherche à innover et à développer de nouveaux systèmes et de nouvelles techniques afin d'améliorer la résilience du Canada en matière de cybersécurité.

GeekWeek 7.5 en chiffres

282 participantes et participants

105 organisations

30 projets

10 fuseaux horaires

9 jours

GeekWeek 7.5 par secteur

Industrie
31 %

CST et Centre pour la cybersécurité
29 %

Provinces et municipalités
13 %

Gouvernement du Canada
10 %

International
10 %

Étudiantes et étudiants
7 %

La Grande exploration

La Grande exploration est l'atelier de cybersécurité annuel classifié du CST.

Pendant 2 semaines, les équipes participantes collaborent afin de trouver des solutions novatrices à des problèmes réels.

Les participantes et participants proviennent du CST, du secteur privé, d'autres ministères du gouvernement du Canada et d'organismes partenaires de la collectivité des cinq.

Cette année, la participation des partenaires de l'industrie et de la collectivité des cinq a battu un record.

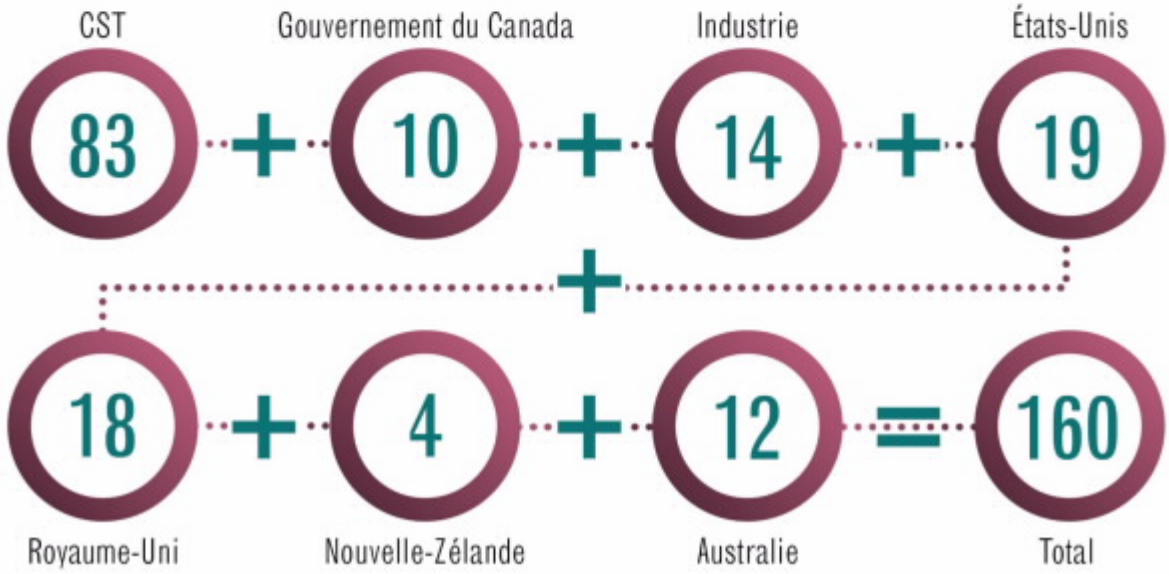
Étant donné que les équipes utilisent les systèmes et les outils classifiés du CST, toute personne qui participe doit détenir une habilitation de sécurité valide.

Les équipes ont travaillé sur des preuves de concept visant à résoudre divers problèmes, notamment :

- comment accélérer la détection et l'atténuation des maliciels sur les réseaux du gouvernement du Canada;
- comment veiller à ce que les réseaux demeurent protégés dans :
  - → le nuage,
  - → un environnement de travail hybride;
- comment créer une plateforme d'analyse prête à utiliser à déployer chez les victimes non gouvernementales de cyberattaques;
- comment mieux protéger les appareils connectés à l'Internet, comme :
  - → les systèmes de contrôle industriels,
  - → les appareils intelligents.

> **Je suis si heureuse de voir autant de grands esprits dans ce secteur se réunir en un lieu. Vous collaborerez pour relever des défis afin de résoudre des problèmes complexes et d'améliorer notre résilience collective en cybersécurité.**
>
> Anita Anand, ministre de la Défense nationale, Discours à l'occasion de la Grande exploration, novembre 2022

Participantes et participants de la Grande exploration 2022



Reddition de **comptes**

De stricts mécanismes internes et externes sont en place afin de veiller à ce que les activités du CST soient conformes à la loi et respectent la vie privée des Canadiennes et Canadiens.

Il faut noter que certaines statistiques dans la section suivante sont représentées selon l'année civile afin de correspondre au calendrier des organes d'examen et de surveillance.

Autorisations ministérielles

Les autorisations ministérielles sont des instruments législatifs qui permettent au CST de mener certaines activités en vertu de son mandat. Il y a 4 types d'autorisations, soit :

- renseignement étranger;
- cybersécurité;
- cyberopérations actives;
- cyberopérations défensives.

Autorisations de renseignement étranger et de cybersécurité

La ou le ministre de la Défense nationale doit autoriser toute activité de renseignement étranger ou de cybersécurité qui :

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

Par exemple, toute activité qui risque d'intercepter accidentellement les communications privées d'une Canadienne ou un Canadien ou d'une personne se trouvant au Canada doit d'abord être autorisée par la ou le ministre.

La ou le commissaire au renseignement doit également approuver les autorisations de renseignement étranger et de cybersécurité avant que l'activité ne soit menée. Chaque autorisation est valide pour une durée maximale d'un an.

En 2022, le CST a soumis au total 6 autorisations ministérielles au commissaire au renseignement :

- 3 autorisations de renseignement étranger;
- 1 autorisation de cybersécurité (visant à protéger les institutions fédérales);
- 2 autorisations de cybersécurité (visant à protéger des institutions non fédérales).

Le commissaire au renseignement a approuvé 5 autorisations dans leur entièreté et a approuvé en partie 1 autorisation de cybersécurité concernant une infrastructure fédérale. Dans ce cas, le commissaire au renseignement a approuvé l'autorisation à l'exception d'une activité, selon le raisonnement qu'il n'y avait pas suffisamment d'information pour déterminer si l'activité était visée par la *Loi sur le CST*.

Un résumé de ces conclusions se trouve dans le Rapport annuel 2022[87] du commissaire au renseignement.

Si une autorisation n'est qu'en partie approuvée, le CST ne mène que les activités approuvées.

Le CST accueille favorablement la perspective du commissaire sur la façon d'améliorer le processus associé aux autorisations ministérielles. Il continue de tenir compte des commentaires dans ses lettres de décision visant à éclairer le prochain cycle annuel d'autorisations ministérielles.

Autorisations de cyberopérations étrangères

Les cyberopérations étrangères désignent les activités menées en vertu des volets touchant les cyberopérations actives (COA) et les cyberopérations défensives (COD) du mandat du CST[38]. Les autorisations de cyberopérations étrangères permettent au CST de mener une variété d'activités en ligne, y compris nuire aux menaces étrangères visant le Canada.

La ou le ministre des Affaires étrangères joue un rôle important afin de veiller à ce que les activités de cyberopérations étrangères soient alignées avec la politique étrangère du Canada. Il doit demander ou consentir à ce que toute autorisation de COA soit délivrée, ainsi qu'être consulté avant que ne soit délivrée toute autorisation de COD.

Voici le nombre d'autorisations ministérielles de COA et de COD pour chaque année civile depuis l'entrée en vigueur de la *Loi sur le CST* :

- 2022 :
  → COA : 3
  → COD : 1
- 2021 :
  → COA : 2
  → COD : 1
- 2020 :
  → COA : 1
  → COD : 1
- 2019 :
  → COA : 1
  → COD : 1

Chaque autorisation est valide pour une durée maximale d'un an. Le CST peut mener plusieurs opérations en vertu d'une même autorisation. Dans certains cas, l'autorisation peut constituer une mesure préventive, sans qu'une opération ait lieu.

Arrêtés ministériels

En vertu de la *Loi sur le CST*, la ou le ministre de la Défense nationale peut utiliser un arrêté ministériel pour désigner des personnes ou des organisations avec lesquelles le CST peut collaborer ou auxquelles il peut transmettre de l'information. Par exemple, si le CST offre son aide en matière de cybersécurité à une institution non fédérale, la ou le Ministre devrait désigner les cybersystèmes de cette organisation comme étant d'importance pour le gouvernement fédéral.

En date du 31 mars 2023, 5 arrêtés ministériels étaient en vigueur, soit :

- 3 arrêtés désignant des cybersystèmes non fédéraux comme étant d'importance pour le gouvernement fédéral;
- 1 arrêté désignant des entités auxquelles le CST peut transmettre de l'information liée à une Canadienne ou un Canadien ou à une personne se trouvant au Canada si elle est nécessaire pour protéger l'information ou les systèmes d'institutions fédérales ou des infrastructures essentielles;
- 1 arrêté désignant des entités auxquelles le CST peut transmettre des informations nominatives sur des Canadiennes et Canadiens, s'il est essentiel de le faire pour des raisons d'affaires internationales, de défense ou de sécurité.

Organes d'examen de la sécurité nationale

Toutes les activités du CST sont assujetties à des examens externes par :

- 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).

Ces organes d'examen jouent un rôle essentiel au nom de la population canadienne pour ce qui est de confirmer la légalité des activités du CST. Le CST accueille favorablement leur point de vue pour améliorer ses processus.

Au cours de l'année, le CST a restructuré la coordination des examens pour mieux soutenir l'OSSNR.

Il continue de travailler avec l'OSSNR dans le but de résoudre les préoccupations concernant l'accès à l'information du CST. Les deux parties ont convenu de mettre en place une solution pilote qui permettra à l'OSSNR d'accéder de façon indépendante aux fichiers du CST touchés par les examens de l'OSSNR. Cette solution pilote a débuté en mars 2023, et le CST continue de surveiller les progrès et de tenir compte des avis de l'OSSNR.

Examens sur l'ingérence étrangère

En mars 2023, le premier ministre a annoncé des mesures visant à accroître la confiance dans la démocratie canadienne[89]. Parmi ces mesures, il a demandé au CPSNR et à l'OSSNR d'examiner les répercussions de l'ingérence étrangère lors des élections fédérales de 2019 et de 2021, ainsi que la façon dont les organismes de sécurité nationale canadiens ont géré la menace.

Le premier ministre a également nommé un rapporteur spécial indépendant sur l'ingérence étrangère[90] ayant pour mandat de donner des recommandations provisoires d'ici le 23 mai 2023.

En mars, le CST a commencé à appuyer le travail du rapporteur spécial indépendant en :

- offrant des séances d'information;
- répondant aux questions;
- fournissant des documents classifiés et non classifiés.

L'OSSNR et le CPSNR ont entamé leurs examens en mars, et les premières demandes au CST ont été faites en avril.

Le CST est en faveur de ces examens. Comme il l'a souligné dans des rapports, comme les Cybermenaces contre le processus démocratique du Canada[91], il existe une réelle menace d'ingérence étrangère. Il faut que la population canadienne puisse avoir confiance dans les résultats des élections.

Statistiques liées aux examens

Au cours de l'année, le CST :

- a contribué à 22 examens externes :
  → 17 de l'OSSNR,
  → 4 du CPSNR,
  → 1 du rapporteur spécial indépendant;
- a participé à plus de 52 séances d'information, réunions ou entrevues avec le personnel des organes d'examen;
- a répondu à 502 questions des organes d'examen.

Le CST a répondu à 89 % des questions que lui ont posé le CPSNR et l'OSSNR dans les délais prévus.

Rapports des organes d'examen et de surveillance

Les rapports non classifiés des organes d'examen et de surveillance externes sont accessibles sur leur site Web respectif :

- Commissaire au renseignement[92]
- CPSNR[93]
- OSSNR[94]

Protection de la vie privée des Canadiennes et Canadiens

Le CST suit des protocoles stricts afin de garantir que ses activités sont conformes à la loi et qu'elles respectent la vie privée de la population canadienne et des personnes au Canada. Ses activités sont assujetties à des examens par les organes d'examen externes, y compris le Commissariat à la protection de la vie privée.

Plus d'information sur la façon dont le CST protège la vie privée[95] est disponible sur son site Web.

Communication de métadonnées

En janvier 2023, le CST a recommencé à communiquer des métadonnées à ses partenaires de la collectivité des cinq, à la suite d'un long processus approfondi visant à résoudre des préoccupations en matière de protection de la vie privée.

Les métadonnées désignent l'information **concernant** une communication, mais pas le contenu de celle-ci.

En voici quelques exemples :

- date et heure d'une communication;
- adresses courriel;
- adresses IP;
- numéros de téléphone.

Les métadonnées sont essentielles dans le renseignement étranger, car elles aident les analystes à identifier la ou le destinataire et le moment d'une communication, ainsi que les méthodes de communication. Ce contexte est précieux afin de permettre au gouvernement du Canada et à ses alliés de la collectivité des cinq de contrer les menaces étrangères de manière appropriée.

Métadonnées et informations nominatives sur des Canadiennes et Canadiens

Le CST recueille des métadonnées en vertu du volet touchant le renseignement étranger de son mandat, lequel lui interdit de cibler les communications des Canadiennes ou Canadiens ou des personnes se trouvant au Canada. Toutefois, l'infrastructure mondiale de l'information (IMI) est, comme son nom l'indique, mondiale. C'est pourquoi, lorsqu'il obtient de l'information dans l'IMI, le CST peut acquérir accidentellement de l'information qui peut identifier une Canadienne ou Canadien ou une personne au Canada.

Apprenez-en plus sur la façon dont le CST protège l'information nominative sur des Canadiennes et Canadiens[96] sur son site Web.

Avant 2014, le CST utilisait un processus automatisé pour « réduire » l'information nominative sur des Canadiennes et Canadiens (en la dépersonnalisant) avant de communiquer les métadonnées à ses partenaires de la collectivité des cinq.

En 2014, il a toutefois découvert que le processus automatisé ne dépersonnalisait pas cette information correctement. Il a immédiatement cessé la communication de métadonnées et a informé le Commissariat à la protection de la vie privée et le Commissaire du CST, l'organe d'examen externe à l'époque.

Le chef du CST et le ministre de la Défense nationale s'étaient engagés à ce que le CST ne recommence à communiquer des métadonnées que lorsque des mesures efficaces afin de protéger la vie privée des Canadiennes et Canadiens seraient prises.

Requêtes en place

Afin de résoudre ce problème, le CST a adopté un nouveau processus pour permettre aux partenaires de la collectivité des cinq d'utiliser les métadonnées obtenues par le CST. Ce processus se nomme « requêtes en place » (QIP pour *query-in-place*), car le CST maintient le contrôle de l'ensemble de la base de données en tout temps. Maintenant, les analystes d'organismes partenaires doivent faire une requête au CST pour obtenir des données précises. Ces requêtes doivent respecter les critères suivants :

- **ne pas** porter sur des Canadiennes ou Canadiens ou des personnes se trouvant au Canada;
- énoncer clairement la cible de la requête;
- énoncer clairement les résultats anticipés de la requête, ainsi que la valeur de l'information sur le plan du renseignement étranger.

Le CST s'assurera que ces critères sont respectés. Toute et tout analyste de la collectivité des cinq qui souhaite soumettre une requête au moyen du QIP doit d'abord suivre la formation obligatoire et passer un test de connaissances sur les exigences juridiques et politiques du CST.

Consultation

Avant le lancement de QIP, le CST a tenu un processus de consultation approfondi. Il a informé l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). Il a collaboré étroitement avec le Commissariat à la protection de la vie privée (CPVP) afin de cerner et de gérer les risques d'atteinte à la vie privée, de même que mettre en place des mesures techniques pour les atténuer.

Conformément à la recommandation du CPVP, le CST a effectué une évaluation des facteurs relatifs à la vie privée (EFVP) sur son processus de transmission de métadonnées. Étant donné que l'EFVP touchait de l'information TRÈS SECRET, les discussions approfondies sur l'information classifiée ont eu lieu lors de plusieurs séances d'information en personne avec le CPVP.

Le CST a accepté chacune des 6 recommandations du CPVP visant à clarifier certains concepts de l'EFVP.

Transmission

Le CST a mis à l'essai le processus de requêtes en place de novembre 2021 à décembre 2022 et n'a signalé aucun incident relatif à la vie privée.

Ayant confirmé que le processus fonctionnait comme prévu, le CST a avisé ses partenaires de la collectivité des cinq en janvier 2023 que le QIP deviendrait la nouvelle norme de transmission de métadonnées du CST.

Le CST continue de mener des examens de la conformité afin de garantir que le CST respecte les exigences juridiques et politiques qui lui incombent.

Depuis l'adoption du processus QIP, le CST a pu recommencer à offrir une précieuse contribution à la collectivité des cinq, une alliance qui partage les valeurs démocratiques du Canada et qui l'aide à protéger ses intérêts dans le monde.

Divulgation d'information nominative sur des Canadiennes et Canadiens

Comme susmentionné, les activités de renseignement étranger du CST ne doivent pas cibler les communications de Canadiennes ou Canadiens ou de personnes se trouvant au Canada. Si de l'information nominative sur une Canadienne ou un Canadien (INC) est obtenue accidentellement, le CST la dépersonnalise dans ses rapports de renseignement.

Toutefois, en vertu de la *Loi sur la protection des renseignements personnels*, un nombre limité de personnes qui reçoivent les rapports de renseignement classifiés du CST peuvent demander les détails de l'INC, tant qu'elles ont l'autorisation légale et un besoin opérationnel de la connaître. Par exemple, il pourrait s'agir d'information sur le rôle d'une Canadienne ou d'un Canadien nommé dans le cadre d'activités qui soulèvent des préoccupations sur le plan de la sécurité nationale. La divulgation d'INC peut faire l'objet d'un examen de l'OSSNR.

En 2022, le CST a reçu :

- 719 demandes de divulgation d'INC, dont :
  - → 657 provenaient de partenaires du gouvernement du Canada,
  - → 62 provenaient de partenaires de la collectivité des cinq.

De ces demandes, le CST :

- en a approuvé : 530
- en a refusé : 65

La différence correspond aux demandes annulées ou à celles qui sont en cours en date du 31 décembre 2022.

Incidents de nature opérationnelle liés à la vie privée

Le CST est doté de politiques internes détaillées sur la manière de gérer l'information qui se rapporte à une Canadienne ou à un Canadien. La moindre contravention à ces politiques est considérée comme un incident de nature opérationnelle lié à la vie privée. Il s'agit d'un mécanisme de suivi interne, qui comprend les erreurs procédurales mineures (comme des données mal étiquetées) qui n'atteignent pas le seuil de signalement au Commissariat à la protection de la vie privée[97]. Les incidents liés à la vie privée par un organisme de seconde part sont comptés séparément. Ce sont des incidents qui concernent un organisme de la collectivité des cinq.

En 2022, le CST a fait le suivi interne de :

- 114 incidents de nature opérationnelle liés à la vie privée;
- 23 incidents d'organismes de seconde part.

Lorsqu'un incident de nature opérationnelle lié à la vie privée est détecté, le CST prend des mesures pour corriger l'erreur, par exemple, en supprimant les données. Le CST consigne et suit les incidents liés à la vie privée afin de prendre des mesures préventives à l'avenir, notamment mettre à jour les politiques et redonner de la formation au personnel.

Conformité interne

En plus de la surveillance et des examens externes, le CST a également un programme de conformité interne rigoureux afin de veiller à ce que ses activités soient conformes avec la loi et qu'elles protègent la vie privée des Canadiennes et Canadiens. L'équipe responsable de la conformité surveille les activités opérationnelles du CST et offre de la formation sur la conformité au personnel du CST.

Au cours de l'année financière, l'équipe de la conformité du CST s'est livrée aux activités suivantes :

- 17 examens;
- 8 études;
- 2 vérifications ponctuelles.

Toute ou tout employé du CST qui doit avoir accès à des données brutes dans le cadre de son travail doit suivre une formation annuelle sur la conformité et passer un test de connaissances. En cas d'échec, les accès de cette personne aux systèmes sont retirés et elle doit suivre la formation à nouveau.

De plus, on encourage les analystes à signaler tout incident possible lié à la vie privée. La grande majorité des incidents de conformité interne du CST sont autodéclarés.

En novembre 2022, le CST a tenu sa première Semaine de la conformité opérationnelle. Durant cette semaine ont eu lieu des activités officielles et informelles afin d'accroître la sensibilisation et faire connaître les pratiques exemplaires.

Plaintes

Le public peut déposer une plainte[98] concernant les activités du CST en écrivant à la ou au chef du CST. Si la personne ayant déposé plainte n'est pas satisfaite de la réponse du CST, elle peut envoyer sa plainte à l'OSSNR. L'OSSNR enquêtera pour déterminer si la plainte relève de sa compétence.

Au cours de l'année, le CST a reçu :

- 8 plaintes externes, dont :
  - → 4 plaintes qui ont fait l'objet d'une enquête et ont été réglées,
  - → 4 plaintes qui en sont à différentes étapes d'avancement (en date du 31 mars 2023).

Cette année, le CST et l'OSSNR ont travaillé ensemble à établir un processus permettant à l'OSSN d'examiner les conclusions du CST en lien avec les plaintes. Ce nouveau processus vise à accroître la transparence, de sorte à faciliter la détermination de l'OSSNR à savoir si une plainte relève de sa compétence. C'est en janvier 2023 que le processus a été utilisé pour la première fois.

Transparence

Il est essentiel dans notre démocratie que la population canadienne comprenne ce que fait le CST pour protéger la sécurité nationale. Toutefois, certaines informations trop sensibles ne peuvent être divulguées, car les adversaires pourraient s'en servir pour nuire au Canada.

Le CST est déterminé à collaborer avec les organes d'examen, ses partenaires externes, les médias et la population afin de favoriser la transparence quant à ses activités dans le cadre de son engagement de transparence en matière de sécurité nationale[99].

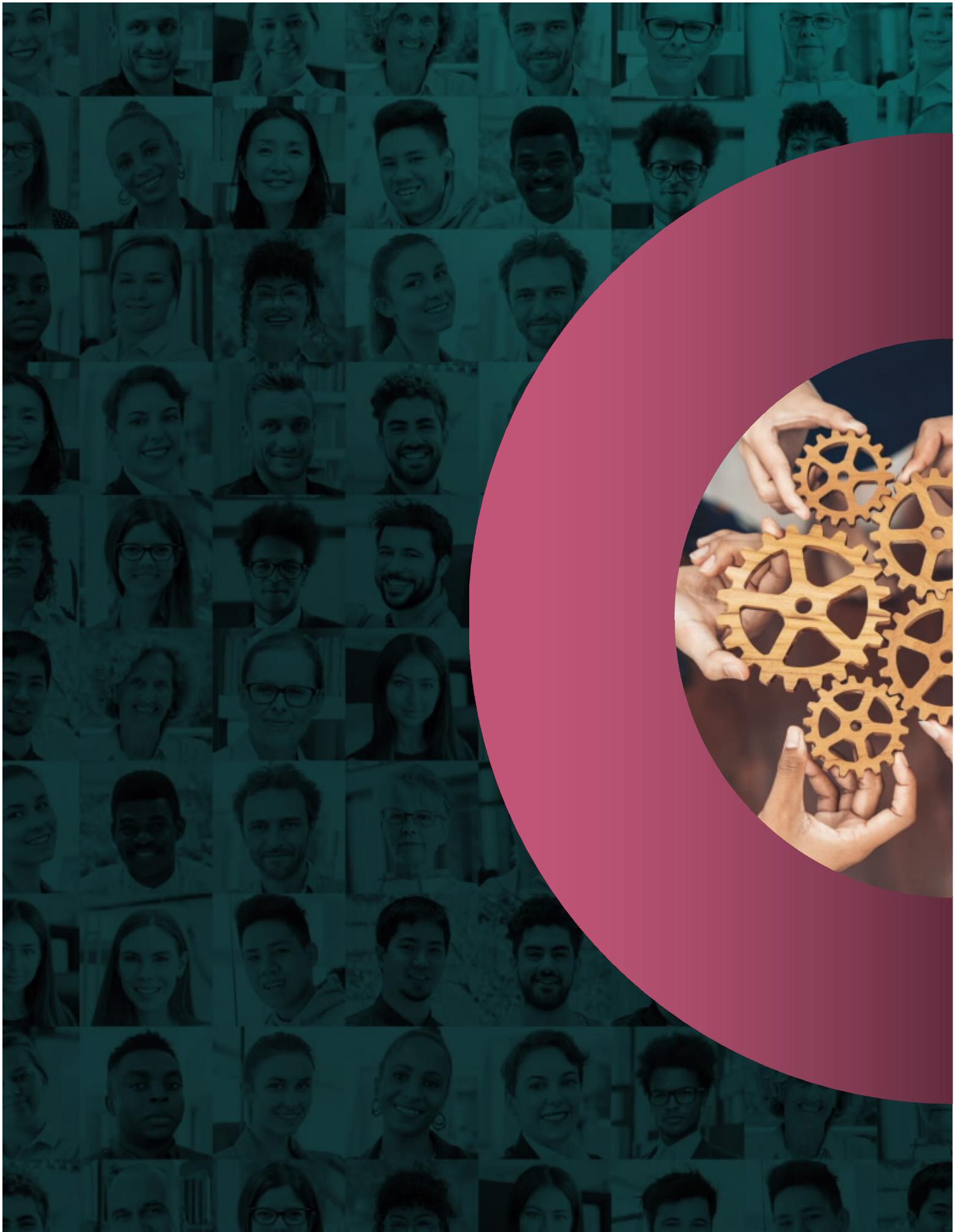
Le Groupe consultatif sur la transparence de la sécurité nationale (GCT-SN) conseille les représentantes et représentants du gouvernement sur l'équilibre entre la transparence et les préoccupations de sécurité. En octobre 2022, la chef Caroline Xavier a informé le GCT-SN des activités du CST et a répondu à des questions portant sur :

- les politiques de conservation de données;
- l'assistance offerte aux infrastructures essentielles;
- l'assistance technique et opérationnelle offerte à des partenaires fédéraux.

Cette année, les activités liées à la transparence du CST consistaient en :

- 4 rapports publics[100];
- 4 divulgations proactives[101];
- 11 témoignages parlementaires;
- 14 entrevues avec les médias;
- 34 publications sur le portail du gouvernement ouvert[102];
- 53 réponses à des demandes d'accès à l'information[103];
- de nombreux discours, conférences et événements publics.

Le CST a également mis à profit des outils numériques, comme son site Web et ses comptes de médias sociaux, pour sensibiliser la population à son travail et communiquer de l'information sur ses activités à un plus grand nombre de Canadiennes et Canadiens.



Personnes

Le personnel du CST regroupe des personnes ayant des expériences et des connaissances différentes qui aident à faire avancer l'objectif commun de protéger le Canada et la population canadienne.

Si les membres du personnel sentent que leur travail et leur identité sont valorisés, le CST est mieux placé pour mener à bien sa mission. Au cours de la dernière année, le CST a accru ses efforts en vue de favoriser un environnement sain et inclusif qui soutient l'effectif et attire de nouveaux talents.

Résultats du Sondage auprès des fonctionnaires fédéraux

Le Sondage auprès des fonctionnaires fédéraux (SAFF) recueille des données auprès des fonctionnaires au sujet de leurs expériences au travail. Le CST a obtenu de meilleurs résultats lors du sondage de 2022[104] que la moyenne de la fonction publique. Par exemple :

	CST	Fonction publique
Je suis fièr(e) du travail que je fais.	90 %	85 %
Les personnes avec lesquelles je travaille valorisent mes idées et mes opinions.	92 %	83 %
Dans l'ensemble, mon ministère ou organisme me traite avec respect.	91 %	84 %
Mon (ma) superviseur(e) immédiat(e) soutient ma santé mentale et mon bien-être.	91 %	83 %

Toutefois, on peut faire mieux dans certains domaines. Par exemple, le pourcentage d'employées et employés du CST qui ont vécu du harcèlement ou de la discrimination, même s'il est faible, n'est pas nul, comme il se devrait. Il a même légèrement augmenté depuis 2020.

- Harcèlement :
  → 2022 : 8 %
  → 2020 : 6 %
- Discrimination :
  → 2022 : 6 %
  → 2020 : 5 %

Le pourcentage d'employées et employés signalant vivre du stress au travail a diminué depuis 2020, mais demeure plus élevé qu'avant la pandémie :

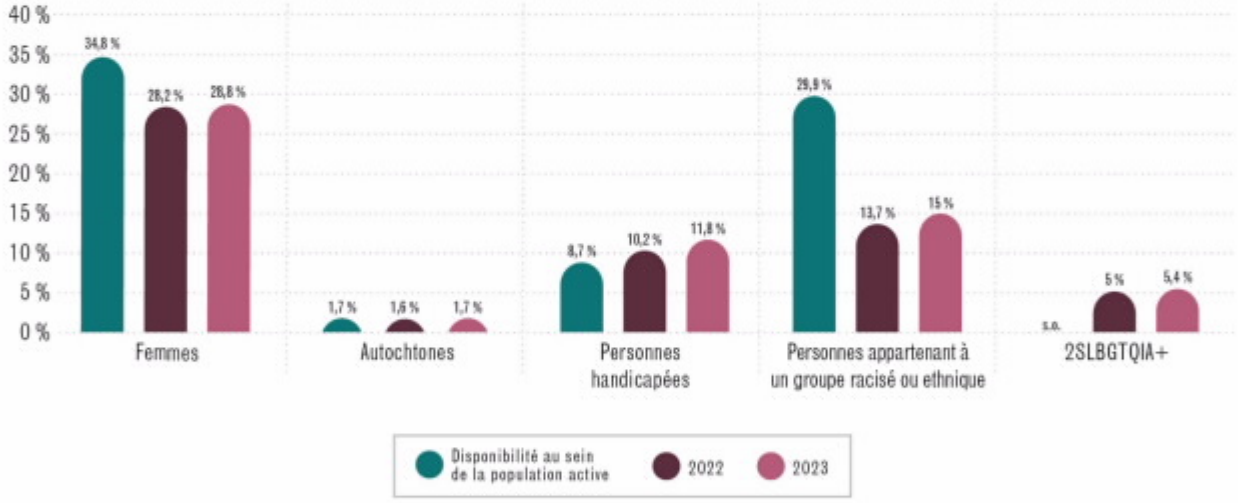
- Niveau de stress au travail élevé ou très élevé :
  → 2022 : 13 %
  → 2020 : 15 %
  → 2019 : 9 %

Le premier principe du cadre pour l'équité, la diversité et l'inclusion[105] (EDI) est « le CST vise l'amélioration ». Le CST cherche constamment à s'améliorer. Le SAFF de 2022 présente des données précieuses pour l'aider à déterminer dans quels domaines des changements sont nécessaires

Données démographiques

En 2022, le CST a adopté un nouveau processus de collecte de données démographiques et de données sur la représentation de l'équité en matière d'emploi au sein de son effectif. Ce processus comprend des définitions à jour et une nouvelle option d'auto-identification comme membre de la communauté 2SLGBTQIA+. Jusqu'à maintenant, 75 % du personnel a choisi volontairement de soumettre ses données d'auto-identification.

Données démographiques de l'effectif du CST pour 2022 à 2023



Les derniers chiffres montrent que la diversité augmente petit à petit au CST. La représentation des Autochtones et des personnes handicapées au sein de l'effectif du CST est maintenant égale ou supérieure à la disponibilité au sein de la population active. Toutefois, les femmes ainsi que les personnes appartenant à un groupe racisé ou ethnique demeurent sous-représentées. Le CST est déterminé à changer la situation, conformément à son cadre pour l'équité, la diversité et l'inclusion ainsi qu'à l'appel à l'action en faveur de la lutte contre le racisme dans la fonction publique[106]. Le CST continue de collaborer avec ses partenaires internes et externes pour améliorer ces chiffres, notamment par des activités de recrutement adaptées, des initiatives sur l'avenir du travail et des efforts de promotion de l'EDI.

Recrutement

Comme mentionné, le budget de 2022 alloue des fonds au CST pour qu'il puisse améliorer ses capacités. C'est pourquoi la croissance est en tête des priorités cette année. Le CST a entrepris plusieurs initiatives visant à améliorer sa capacité à attirer et à embaucher les personnes dont il a besoin pour mener à bien efficacement sa mission et répondre à la demande croissante.

Événements de recrutement

L'équipe chargée du recrutement a adopté une approche hybride en participant à des événements en personne et en ligne. Elle a participé à 90 événements, comme des salons de carrière dans les collèges et les universités, des marathons de programmation, des séances d'information et des ateliers techniques. Afin d'encourager nos efforts de recrutement envers un effectif diversifié, près d'un quart de ces événements visaient particulièrement les personnes de communautés sous-représentées à la recherche d'un emploi.

Recrutement de personnes autochtones

Alors qu'il travaille à avancer la réconciliation, le CST s'engage à combler les lacunes à l'emploi auxquels sont confrontées les personnes autochtones et à leur offrir un accès équitable aux occasions d'emploi. Cette année, le CST a participé à des événements de recrutement dans des villes ayant de fortes populations autochtones et a collaboré étroitement avec une spécialiste autochtone interne afin de mieux joindre ces communautés.

Le CST continue de participer au Programme d'apprentissage en TI pour les personnes autochtones[107] du gouvernement du Canada. Ce programme permet de jumeler des personnes inuites, métisses et des Premières Nations avec des organisations participantes pour les aider à développer les compétences nécessaires à un emploi en TI dans la fonction publique.

Le CST a consulté ses groupes d'affinité[108] afin de cerner les iniquités systémiques dans ses pratiques d'embauche. Il en est notamment ressorti que le besoin de déménager représentait un obstacle pour les Autochtones dont l'identité est profondément ancrée à leur communauté. Le nouveau modèle de travail hybride permet aux candidates et candidats autochtones qui le souhaitent de demander à travailler à distance, si la nature du poste le permet (voir la section Avenir du travail à la page 54).

Marketing lié au recrutement

Au printemps 2022, le CST a mené à bien une campagne publicitaire visant à recruter des analystes du renseignement en langues étrangères spécialisées et spécialisés dans les langues chinoises. La campagne est apparue dans des médias de langue chinoise afin de joindre des Canadiennes et des Canadiens possédant des compétences linguistiques en chinois. La campagne a engendré plus de 2 500 visites sur la page Web des carrières.

En décembre 2022, le CST a publié une nouvelle vidéo de recrutement[109] qui met l'accent sur les différents types d'emploi disponibles au CST et les éléments de la culture au travail qui le distinguent. La vidéo a été entièrement créée à l'interne et s'accompagnait d'une nouvelle image de marque et d'un nouveau slogan : « Le CST, l'organisme le plus important dont vous n'avez jamais entendu parler ».

Autres efforts de recrutement

Pour la première fois depuis 3 ans, le CST a publié une affiche de poste précisément pour des analystes du renseignement sur sa page des carrières. Il y a eu plus de 1 900 candidatures admissibles.

Le CST continue de joindre les talents techniques actuels et futurs par l'entremise d'événements de collaboration, tels que la GeekWeek, et de son programme d'approche communautaire.[110]

Sécurité

Une grande partie du processus d'embauche comprend une évaluation de sécurité. Cette évaluation est nécessaire, car le travail du CST consiste à protéger la sécurité nationale du Canada. Toutefois, il sait que ce processus est intimidant, surtout pour des candidates et candidats provenant de groupes qui souffrent souvent de discrimination.

Cette année, l'équipe responsable de la sécurité du CST a consulté les groupes d'affinité afin de cerner les obstacles qui décourageraient les membres de groupes sous-représentés de poser leur candidature. Ils ont ensemble envisagé des manières de rendre le processus de filtrage de sécurité plus inclusif, par exemple :

- accroître la sensibilisation culturelle et la connaissance des préjugés inconscients auprès du personnel de sécurité;
- accroître la diversité au sein du personnel de sécurité en recrutant à l'externe et à l'interne.

Avenir du travail

Comme le mentionnait le rapport de l'année dernière, le CST tire parti de l'environnement hybride à niveaux de classification multiples que la pandémie a engendré. Il permet d'offrir une meilleure flexibilité au personnel et d'embaucher des gens à divers niveaux d'habilitation de sécurité.

Milieu de travail hybride

Le projet pilote de télétravail que le CST a lancé l'année dernière a été un véritable succès. Le CST s'est maintenant doté officiellement un modèle de travail hybride. La stratégie est adaptée du modèle de travail hybride de la fonction publique fédérale[111] et la plupart des membres du personnel se présentent au bureau en personne au moins 3 jours par semaine.

Afin de favoriser une approche juste, équitable et durable, il est possible de demander des journées de télétravail supplémentaires. Une fois les approbations nécessaires obtenues, des exceptions peuvent être faites dans des situations comme :

- des personnes qui travaillent ailleurs au Canada;
- des personnes autochtones qui souhaitent demeurer dans leur communauté;
- des personnes travaillant dans les secteurs de TI prioritaires.

Cependant, les personnes dont le travail est classifié continuent, comme ce fut le cas durant la pandémie, de travailler en personne à temps plein.

La priorité est de mener à bien la mission efficacement, tout en soutenant l'effectif au moyen d'arrangements de travail flexible.

Cote de fiabilité approfondie

Le modèle de travail hybride a prouvé qu'il permettait de maintenir le même niveau d'efficacité et d'excellence dans un environnement à niveaux de classification multiples. Le CST en a profité pour embaucher plus de personnes à divers niveaux d'habilitation de sécurité et plus rapidement.

Cette année, le CST a mis en place un programme d'embauche avec la **cote de fiabilité approfondie** pour les rôles qui ne nécessitent pas d'accès aux systèmes et à l'information classifiés. Le programme permet :

- d'accélérer le processus de filtrage de sécurité, car les entrevues peuvent se tenir à distance et l'examen polygraphique n'est pas requis;
- d'obtenir un plus grand bassin de candidates et candidats, car les personnes qui habitent ailleurs que dans la région de la capitale nationale peuvent travailler à distance;
- de progresser dans son cheminement de carrière sans nécessiter d'habilitation de sécurité TRÈS SECRET.

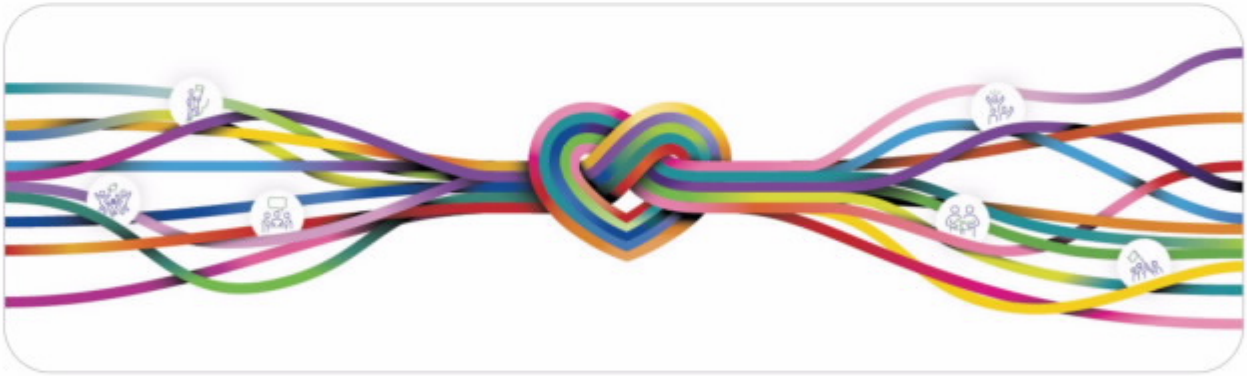
Depuis que le processus avec cote de fiabilité approfondie a été lancé en juillet 2022, le CST a embauché 17 employées et employés à temps plein et 10 étudiantes et étudiants. Le CST continuera de mettre à profit le programme d'embauche avec la cote de fiabilité approfondie dans les prochaines années afin d'atteindre ses objectifs de croissance.

Équité, diversité et inclusion (EDI)

Le CST s'engage à établir un effectif aussi diversifié que possible. Il s'efforce de favoriser un environnement inclusif et équitable, où chaque membre de son personnel peut s'épanouir. C'est un aspect essentiel non seulement pour la culture de travail, mais aussi pour la mission.

La collaboration interne et externe permet au CST de prendre des mesures pour accroître la sensibilisation, cerner les iniquités systémiques et trouver des solutions pour améliorer l'expérience de tout le monde au CST.

Pour en apprendre plus sur les autres initiatives liées à l'EDI, consultez la section sur la diversité et l'inclusion[112] du site Web.



Cadre pour l'EDI

En juin 2022, le CST a lancé son cadre pour l'EDI[113]. Au cours de la dernière année, le cadre a servi plusieurs fonctions, comme :

- orienter les efforts en vue de créer un organisme inclusif;
- promouvoir l'EDI à tous les échelons et dans tous les secteurs d'activités;
- faire en sorte que la voix des bonnes personnes se fasse entendre;
- accroître l'efficacité de la mission.

Cette année, chaque secteur d'activités a élaboré un plan d'action annuel en matière d'EDI, qui concrétise les aspects énoncés dans le cadre par des actions adaptées. Les responsables de chaque secteur collaboreront pour assurer la reddition des comptes et faire rapport des progrès.

Programme pilote de parrainage

En décembre 2022, le CST a lancé un programme pilote de parrainage. Ce programme a été créé afin d'atteindre les objectifs suivants :

- éliminer les obstacles à l'avancement professionnel auxquels sont confrontées les personnes noires, autochtones et autres personnes racisées;
- offrir à ces personnes des occasions de les aider à faire avancer leur carrière;
- créer des processus de développement de carrière équitables au CST.

Pour y parvenir, le programme jumelle les personnes participantes avec des marraines ou parrains au sein de la direction (cadres du CST) qui :

- les encadreront et les soutiendront;
- veilleront à ce qu'elles soient prises en compte pour les occasions;
- les aideront à obtenir une nomination intérimaire appropriée.

Le programme pilote a reçu 56 candidatures, dont 14 ont été retenues pour participer au programme pendant 12 mois à partir d'avril 2023. Les candidates et candidats non retenus dans cette première ronde se sont vu offrir du soutien de carrière et des occasions de mentorat informelles.

> **Le programme de parrainage est la preuve que le CST s'efforce d'éliminer certains des obstacles systémiques auxquels les employées et employés racisés ou autochtones sont confrontés. Il montre que le CST ne craint pas d'être un leader en matière de changement. En tant que femme racisée, je suis au courant des iniquités auxquels peuvent faire face de nombreuses personnes au travail. Je suis reconnaissante que le CST prenne les mesures nécessaires pour lutter contre ces obstacles.**
>
> Sabeena S. (elle), employée du CST et participante du programme de parrainage

Plan d'accessibilité du CST 2022-2025

Le CST a publié son tout premier plan d'accessibilité[114] en décembre 2022. Le plan présente un aperçu des mesures prises par le CST en vue d'éliminer les obstacles à l'accessibilité des membres du personnel et des personnes qui visitent les édifices. Plusieurs groupes internes ont contribué à sa création, notamment :

- les groupes d'affinité (y compris les groupes des personnes handicapées et de la neurodiversité);
- les représentantes et représentants du syndicat;
- le Comité des personnes[115].

Au cours des 3 prochaines années, le CST continuera de travailler avec les divers groupes afin de peaufiner le plan et de veiller à ce que personne ne soit exclu. Il a également mis en place un processus de rétroaction sur l'accessibilité au CST[116].

Groupes d'affinité

Les groupes d'affinité[117] du CST sont des réseaux dirigés par des employées et employés, qui jouent un rôle important dans la mise en œuvre du cadre pour l'EDI du CST. Depuis 2023, ils sont également représentés au Comité des personnes, où les responsables occupent un siège à tour de rôle afin de présenter une diversité de points de vue.

Cette année, 2 nouveaux groupes d'affinité ont vu le jour, soit :

- le groupe d'affinité juif;
- le Réseau franco.

Pendant l'année, les groupes d'affinité ont aidé à élaborer des politiques et ont mené des initiatives qui profitent à tout le monde au CST, y compris :

- le Cadre pour l'EDI du CST;
- le Plan d'accessibilité 2022-2025 du CST;
- le guide interne sur le soutien de la neurodiversité au CST;
- un programme de mentorat structuré auquel participent plus de 100 personnes.

Ils ont également organisé de nombreux événements et commémorations (page 58), ont défendu les besoins de leurs communautés et ont communiqué des expériences vécues.

En janvier 2023, EmbRACE, le réseau des personnes racisées et autochtones, a organisé la visite d'une délégation de son homologue au Government Communications Headquarters (GCHQ) afin de renforcer le partenariat en matière d'EDI. Apprenez-en plus sur cette visite historique visant à promouvoir la lutte contre le racisme au CST et au GCHQ[118] sur le site Web.

Formation sur l'EDI

Un des principaux principes du cadre pour l'EDI du CST est que le CST est un apprenant. Afin d'appuyer ce principe, le cadre souligne le besoin de mettre en place des formations obligatoires sur l'analyse comparative entre les sexes plus et d'autres sujets liés à l'EDI.

Cette année, le CST a rendu obligatoires les formations suivantes :

- Pour tout le personnel :
  - → Introduction à l'analyse comparative entre les sexes plus (ACS+)
  - → Passer des biais à l'inclusion
- Pour les superviseures et superviseurs et les gestionnaires :
  - → Diriger la diversité
  - → Adopter un état d'esprit d'inclusion sur le lieu de travail

Le CST a également offert d'autres formations informelles qui abordent la question des microagressions ainsi que de l'identité et l'expression de genre.

Conseillère supérieure, Personnes, équité, diversité et inclusion

Cette année, le CST a accueilli une nouvelle conseillère supérieure, Personnes, équité, diversité et inclusion. Elle a aidé à intégrer durablement l'EDI au sein de l'organisme en soutenant le changement des façons suivantes :

- lancement du programme pilote de parrainage;
- restructuration du Comité des personnes afin d'inclure les responsables des groupes d'affinité;
- soutien organisationnel aux groupes d'affinité;
- amélioration de la collecte et de l'utilisation des données afin d'appuyer l'EDI au CST.

Une lutte contre le racisme primée

Depuis un an, Marie Calixte-McKenzie et Jonathan Gohidé continuent de parler franchement de leur expérience en tant que personnes noires au Canada dans l'ensemble de la fonction publique et ailleurs. Ces deux collègues du CST ont donné 11 présentations dans les deux langues officielles, joignant plus de 1 000 personnes. Leur présentation « Être Noir(e) au Canada »[119] fait également partie du programme d'intégration des nouvelles et nouveaux employés.

En octobre 2022, Marie et Jonathan ont reçu le Prix Joan Atkinson pour les valeurs du secteur public en milieu de travail[120] lors des Prix d'excellence de la fonction publique de 2021. Il s'agit des plus hautes distinctions qui reconnaissent les contributions exceptionnelles de fonctionnaires.

Événements et commémorations liés à l'EDI

Pendant l'année, le CST a organisé plus de 25 événements visant à accroître la sensibilisation à divers enjeux liés à l'EDI. Un grand nombre de ces événements ont été organisés par les groupes d'affinité dans le but de sensibiliser les collègues et de commémorer les dates importantes. Certains événements conjoints ont donné l'occasion de collaborer avec les partenaires d'EDI de la collectivité des cinq.

13
événements spéciaux en personne

Performance du duo de chant de gorge, Tarniriik, au CST afin de souligner la Journée nationale des peuples autochtones

10
panels de membres du personnel

Matériel d'information dans le cadre de la Journée internationale des femmes au CST

5
conférences de personnes invitées

Eva Kuper, survivante de l'Holocauste, au CST dans le cadre de la Journée internationale dédiée à la mémoire des victimes de l'Holocauste

Langues officielles

Le CST a continué, cette année, de faire la promotion de la dualité linguistique à tous les échelons et dans tous les secteurs de l'organisme. En novembre 2022, le CST a lancé un plan d'action pour les langues officielles ayant 2 objectifs principaux :

- Créer un milieu de travail inclusif bilingue en augmentant l'usage du français;
- Veiller à ce qu'il y ait suffisamment de membres du personnel bilingues pour mettre efficacement en œuvre les programmes et les services publics destinés à la population canadienne dans les deux langues officielles.

Le CST a appuyé son effectif en offrant de la formation officielle à temps partiel et à temps plein en langues officielles, en plus de faire la promotion des occasions d'apprentissage informelles. Comme nouveauté cette année, des volontaires ont organisé des groupes de conversation hebdomadaires à l'intention des personnes qui souhaitent améliorer leur français ou maintenir leurs acquis dans cette langue.

En mars 2023, le CST a lancé le Réseau franco, un nouveau groupe d'affinité qui représente les besoins et les intérêts de la communauté francophone au CST. Le Réseau franco a organisé des événements durant la Semaine de la francophonie afin de célébrer et de faire la promotion de la langue française et de la culture francophone.

Bien-être du personnel

Le travail du CST peut être exigeant. L'accent que met le CST sur la santé mentale et le bien-être du personnel garantit que son effectif est résilient sur le plan émotionnel et qu'il a accès aux ressources dont il a besoin au moment opportun.

Le Programme de mieux-être des employées et employés et de l'organisme (MEEO) est composé des services suivants :

- Programme de consultation et d'orientation (PCO);
- Services d'orientation professionnelle;
- Programme de gestion de l'incapacité.

Pendant l'année 2022 à 2023, le PCO interne du CST a orienté ses efforts sur les activités suivantes :

- prendre part à une consultation à l'échelle de l'organisme concernant la santé mentale afin d'appuyer l'élaboration d'une stratégie pluriannuelle sur la santé mentale;
- créer des formations obligatoires sur la santé mentale, la gestion des conflits et l'acte de donner et de recevoir de la rétroaction à l'intention des membres de la direction;
- offrir du soutien de réintégration dans l'environnement de travail hybride;
- offrir du soutien opportun en matière de gestion des conflits et de santé mentale.

La page « Accent mis sur les employés[121] » présente plus d'information sur le Programme de MEEO et les services connexes.

Le virage vert du CST

Le programme Virage vert du CST a travaillé fort cette année à offrir des conseils dans le cadre de projets organisationnels et à éduquer le personnel sur divers enjeux environnementaux.

Par exemple, en juin 2022, il a dirigé l'installation d'une ruche sur le terrain extérieur de l'édifice Edward-Drake du CST.

À l'automne, la petite mais puissante ruche hébergeait environ 40 000 abeilles qui ont produit 125 pots de miel de fleurs sauvages non pasteurisé tout en contribuant à la prospérité de la flore locale.

Prix

Le CST était fier d'être à nouveau reconnu comme un des meilleurs employeurs pour les jeunes canadiens[122] (2023) et d'être nommé comme l'un des meilleurs employeurs de la région de la capitale nationale[123] (2023).

Cette année, le CST a également reçu le Prix de la Coupe du président de la Campagne de charité en milieu de travail du gouvernement du Canada - grands organismes pour 2022[124]. La Coupe du président reconnaît le succès de la campagne de charité du CST qui vise à soutenir les communautés locales.

Le CST fait des efforts remarquables afin d'être un employeur de choix, car attirer et retenir les meilleurs talents est essentiel à l'atteinte de sa mission envers la population canadienne.

Notes en **fin de texte**

1 cyber.gc.ca/fr/

2 laws-lois.justice.gc.ca/fra/lois/c-35.3/page-1.html

3 www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

4 www.budget.canada.ca/2022/report-rapport/chap5-fr.html#2022-1

5 www.youtube.com/watch?v=wCZ9o4y2sZg

6 Le budget de 2022 affiche 263,9 millions de dollars sur 5 ans et 96,5 millions de dollars par année suivante, ce qui est représentatif d'une méthode de comptabilité d'exercice. Le CST fait état du financement selon une comptabilité de caisse ou, autrement dit, selon le montant reçu.

7 www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=fra

8 www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports/rapport-annuel-du-cst-2021-2022

9 twitter.com/cst_cse/status/1509873583388086312

10 www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-de-cybersecurite-conjoint-sur-les-cybermenaces-criminelles-et-parrainees-par-la

11 www.cyber.gc.ca/fr/orientation/bulletin-cybermenaces-activites-cybermenace-liees-invasion-Ukraine-Russie

12 www.cyber.gc.ca/fr/orientation/conseils-matiere-cybersecurite-cas-niveaux-menace-eleves-itsap10101

13 www.cyber.gc.ca/fr/alertes-avis/risques-cyberactivites-malveillantes-contre-nations-alliees-ukraine

14 www.canada.ca/fr/institutions-democratiques/services/protection-democratie/groupe-travail-securite.html

15 www.canada.ca/fr/institutions-democratiques/services/protection-democratie/protocole-public--incident-critique-elections.html

16 pm.gc.ca/fr/nouvelles/communiques/2023/03/06/prendre-de-nouvelles-mesures-contre-lingerence-etrangere-et

17 dgc-cgn.org/fr/linstitut-des-normes-de-gouvernance-numerique-publie-des-projets-de-normes-pour-les-tabulateurs-de-vote-et-les-cahiers-electroniques-de-scrutin-dans-le-cadre-dune-periode-de-consulta/

18 www.cyber.gc.ca/fr/orientation/cybermenaces-elections

19 www.canada.ca/fr/campagne/desinformation-enligne.html#q

20 www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

21 www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

22 www.cyber.gc.ca/fr/orientation/reperer-les-cas-de-mesinformation-desinformation-et-malinformation-itsap00300

23 www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=fra

24 www.canada.ca/fr/affaires-mondiales/nouvelles/2022/05/declaration-sur-les-cyberactivites-malveillantes-de-la-russie-qui-touchent-leurope-et-lukraine.html

25 www.canada.ca/fr/affaires-mondiales/nouvelles/2022/09/declaration-sur-la-cyberactivite-malveillante-de-liran-portant-atteinte-a-lalbanie.html

26 www.rcaanc-cirnac.gc.ca/fra/1562939617400/1562939658000

27 www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

28 science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/lignes-directrices-securite-nationale-pour-partenariats-recherche

29 www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

30 www.cyber.gc.ca/fr/orientation/la-cybersecurite-et-la-chaine-dapprovisionnement-evaluation-des-risques-itsap10070

Notes en fin de texte

31 www.cyber.gc.ca/fr/orientation/proteger-votre-organisation-contre-les-menaces-de-la-chaine-dapprovisionnement-des-logiciels-itsm10071

32 www.cyber.gc.ca/fr/orientation/cybermenace-provenant-chaines-approvisionnement

33 www.cyber.gc.ca/fr/nouvelles-evenements/programme-evolue-dexamen-de-la-securite-du-cst

34 cyber.gc.ca/fr/outils-services/criteres-communs

35 cyber.gc.ca/fr/outils-services/programme-validation-modules-cryptographiques-pvmc

36 www.cyber.gc.ca/fr/nouvelles-evenements/nist-selectionne-mecanismes-cryptographiques-post-quantiques

37 www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b

38 www.cyber.gc.ca/fr/orientation/conseils-sur-la-mise-en-oeuvre-de-lagilite-cryptographique-itsap40018

39 www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111

40 ised-isde.canada.ca/site/strategie-quantique-nationale/fr/strategie-quantique-nationale-canada

41 www.budget.canada.ca/2022/home-accueil-fr.html

42 Le budget de 2022 affiche 252,3 millions de dollars sur 5 ans et 61,7 millions de dollars par année suivante, ce qui est représentatif d'une méthode de comptabilité d'exercice. Le CST fait état du financement selon une comptabilité de caisse ou, autrement dit, selon le montant reçu.

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

44 Le budget de 2022 fait état de 178,7 millions de dollars sur 5 ans à partir de 2022-2023 et de 39,5 millions de dollars par année suivante. Les montants comprennent la part de financement accordée à Services partagés Canada.

45 Le budget de 2022 affiche 180,3 millions de dollars sur 5 ans et 40,6 millions de dollars par année suivante, ce qui est représentatif d'une méthode de comptabilité d'exercice. Le CST fait état du financement selon une comptabilité de caisse ou, autrement dit, selon le montant reçu.

46 www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

47 www.cga.ca/fr/cybersecurite/

48 www.ieso.ca/en/Sector-Participants/Cybersecurity/Sector-Services---Lighthouse

49 www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-scrt-tl/index-fr.aspx

50 cyber.gc.ca/en/glossary

51 www.cyber.gc.ca/fr/cyberincidents

52 www.cyber.gc.ca/fr/outils-services/chaine-montage-assemblyline

53 www.cyber.gc.ca/fr/orientation/facteurs-relatifs-la-securite-considerer-pour-les-systemes-de-controle-industriels

54 busrides-trajetsenbus.csps-efpc.gc.ca/fr/ep-85-fr

55 www.pensezcybersecurite.gc.ca/fr

56 www.pensezcybersecurite.gc.ca/fr/blogues/comment-securiser-vos-operations-financieres-en-ligne

57 www.pensezcybersecurite.gc.ca/fr/blogues/faut-savoir-cookies-internet

58 www.pensezcybersecurite.gc.ca/fr/blogues/identifier-signes-arnacoeur-platformes-rencontre

59 www.pensezcybersecurite.gc.ca/fr/ressources/que-faire-si-vous-etes-victime-dune-tentative-dhameconnage

60 www.pensezcybersecurite.gc.ca/fr/mois-de-la-sensibilisation-la-cybersecurite

61 www.pensezcybersecurite.gc.ca/fr/ressources/video-chant-lhameconnage-gachez-journee-cybercriminel

62 www.pensezcybersecurite.gc.ca/fr/hameconnage

63 www.cyber.gc.ca/fr/nouvelles-evenements/partenaires-federaux-rappellent-aux-consommateurs-canadiens-detre-vigilants-envers-les-cybermenaces-au-cours-des-soldes-du-vendredi-fou-et-du-cyberlundi

64 www.pensezcybersecurite.gc.ca/fr/blogues/les-12-escroqueries-du-temps-des-fetes

65 www.pensezcybersecurite.gc.ca/fr/blogues/adoptez-des-habitudes-de-jeu-sensees-pendant-le-temps-des-fetes

66 www.pensezcybersecurite.gc.ca/fr/ressources/voici-comment-celebrer-fete-cyberdeballage

67 www.pensezcybersecurite.gc.ca/fr/blogues/stratagemes-dinvestissement-quont-fraudeurs-boites-outils

68 www.pensezcybersecurite.gc.ca/fr/blogues/harponnage

69 www.pensezcybersecurite.gc.ca/fr/blogues/escroqueries-services-quont-fraudeurs-boites-outils

70 www.pensezcybersecurite.gc.ca/fr/blogues/hameconnage-quy-t-il-boite-leurre-dun-fraudeur

71 www.pensezcybersecurite.gc.ca/fr/ressources/boite-outils-fraudeur

72 www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

73 www.cyber.gc.ca/fr/orientation/evaluations-des-cybermenaces-nationales

74 www.cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces

75 www.cyber.gc.ca/fr/

76 www.cyber.gc.ca/fr/nouvelles-evenements/cybersci

77 www.cyber.gc.ca/fr/orientation/guide-sur-les-carrieres-en-cybersecurite

78 www.cyber.gc.ca/fr/orientation/certifications-dans-le-domaine-de-la-cybersecurite

79 www.cyber.gc.ca/fr/orientation/guide-sur-les-carrieres-en-cybersecurite

80 www.cse-cst.gc.ca/fr/mission/recherche-cst/institut-tutte-mathematiques-calcul

81 www.cse-cst.gc.ca/fr/culture-et-communaute/recherche/uniform-manifold-approximation-and-projection-umap

82 news.artnet.com/art-world/refik-anadol-moma-ai-unsupervised-2213039

83 www.cse-cst.gc.ca/fr/mission/recherche-cst/recherche-appliquee

84 www.cyber.gc.ca/fr/outils-services/chaine-montage-assemblyline

85 www.cse-cst.gc.ca/fr/mission/recherche-cst/centre-recherche-vulnerabilites

86 www.cse-cst.gc.ca/fr/ressources-et-information/annonces/cadre-de-gestion-du-partage-des-nouvelles-capacites-du-cst

87 www.canada.ca/fr/commissaire-renseignement/rapportannuel.html

88 www.cse-cst.gc.ca/fr/renseignements-organisationnels/mandat

89 pm.gc.ca/fr/nouvelles/communiques/2023/03/06/prendre-de-nouvelles-mesures-contre-lingerence-etrangere-et

90 www.canada.ca/fr/institutions-democratiques/services/rapporteur-special-independant/avis.html

91 www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

92 www.canada.ca/fr/commissaire-renseignement.html

93 www.nsicop-cpsnr.ca/index-fr.html

94 nsira-ossnr.gc.ca/fr/

95 www.cse-cst.gc.ca/fr/reddition-de-comptes/respect-de-la-vie-privee

96 www.cse-cst.gc.ca/fr/ressources-et-information/fiches-des-renseignements/proteger-linformation-nominative-sur-un#DCSESI

97 Avant la présente année financière, le CST tenait un fichier des erreurs procédurales mineures distinct. Depuis 2022, les erreurs procédurales font maintenant partie du Dossier relatif aux incidents liés à la vie privée (PIF pour *Privacy Incidents File*).

98 www.cse-cst.gc.ca/fr/reddition-de-comptes/surveillance#DDP

99 www.canada.ca/fr/services/defense/securitenationale/engagement-transparence-securite-nationale.html

100 www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports

101 www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/divulgation-proactive

102 open.canada.ca/fr

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

104 www.tbs-sct.canada.ca/pses-saff/2022/results-resultats/fr/bq-pq/index/89

Notes en fin de texte

105 www.cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/un-cst-integre-un-cadre-pour-lequite-la-diversite-et-linclusion
106 www.canada.ca/fr/conseil-prive/organisation/a-propos-appel-action.html
107 talent.canada.ca/fr/indigenous-it-apprentice
108 www.cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/groupes-affinite
109 www.youtube.com/watch?v=wCZ9o4y2sZg
110 cse-cst.gc.ca/fr/carrieres
111 www.canada.ca/fr/gouvernement/fonctionpublique/dotation/modele-travail-hybride-commun-fonction-publique-federale.html
112 www.cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion
113 www.cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/un-cst-integre-un-cadre-pour-lequite-la-diversite-et-linclusion
114 www.cse-cst.gc.ca/fr/accessibilite/plan-accessibilite-cst-2022-2025
115 cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/un-cst-integre-un-cadre-pour-lequite-la-diversite-et-linclusion#pc
116 www.cse-cst.gc.ca/fr/accessibilite/processus-retroaction-accessibilite-centre-securite-telecommunications
117 www.cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/groupes-affinite
118 www.cse-cst.gc.ca/fr/ressources-information/nouvelles/visite-historique-visant-promouvoir-lutte-contre-racisme-cst-gchq
119 www.cse-cst.gc.ca/fr/etre-noire-au-canada-une-entrevue-avec-jonathan-et-marie-collegues-du-cst
120 www.canada.ca/fr/secretariat-conseil-tresor/services/innovation/prix-reconnaissance-evenements-speciaux/pefp-2021.html#toc-6
121 www.cse-cst.gc.ca/fr/culture-et-communaute/la-vie-au-cst/accent-mis-sur-les-employes
122 reviews.canadastop100.com/top-employer-communications-security-establishment?lang=fr#Jeunes
123 reviews.canadastop100.com/top-employer-communications-security-establishment?lang=fr
124 www.canada.ca/fr/campagne/charite/evenement-appreciation-ccmtgc/ccmtgc-coupe-president.html
125 cse-cst.gc.ca/fr/carrieres