Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

ISSN 2564-0488
CAT D95-11F-PDF

Centre de la sécurité des télécommunications

RAPPORT ANNUEL 2023 2024

Canada

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

ISSN 2564-0488
CAT D95-11F-PDF

Table des matières

À propos du CST

Le Centre de la sécurité des télécommunications Canada (CST) est l'organisme national de cryptologie du Canada responsable du renseignement électromagnétique étranger, de la cybersécurité et des cyberopérations étrangères. Le CST est un organisme autonome qui relève de la ou du ministre de la Défense nationale.

Le CST chapeaute le Centre canadien pour la cybersécurité (ou Centre pour la cybersécurité), qui est l'organe opérationnel et technique du gouvernement fédéral pour la cybersécurité.

Le mandat du CST est détaillé dans la *Loi sur le Centre de la sécurité des télécommunications* (*Loi sur le CST*[1]) et comporte cinq volets :

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

Le CST fait partie de la collectivité des cinq : l'alliance d'échange de renseignement la plus ancienne et la plus soudée au monde. La collectivité des cinq comprend les agences de renseignement électromagnétique et de cybersécurité du Canada, de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.

L'effectif du CST est composé de 3 529 employées et employés permanents à temps plein. Les autorités totales du CST pour 2023 à 2024 étaient de tout juste plus d'un milliard de dollars[2].

Le présent rapport est un sommaire non classifié des activités qu'a mené le CST du 1er avril 2023 au 31 mars 2024. À moins d'indication contraire, « cette année » fait référence à l'année financière 2023 à 2024.

Avant-propos du ministre

Le Canada fait face à de nouvelles menaces de sécurité comme à des menaces prenant de nouvelles formes, et au nombre desquelles figurent les changements climatiques et leur incidence sur l'Arctique, la cybercriminalité, l'extrémisme violent et les menaces de la Russie, de la Chine et d'autres États à l'encontre des règles internationales qui nous protègent toutes et tous. Mais le travail qu'accomplit le CST dans l'ensemble des volets de son mandat contribue de manière significative à protéger le Canada contre ces menaces, que ce soit actuellement ou dans l'avenir.

C'est avec plaisir que nous vous présentons ce rapport annuel, qui fait état des succès remportés par le CST dans la lutte contre la cybercriminalité et les menaces émergentes auxquelles le Canada et le monde entier font face. Le rapport met en lumière ce que le Canada a réalisé au cours de l'année écoulée. Pour un gouvernement ouvert et responsable, les rapports comme celui-ci revêtent une importance cruciale et contribuent à renforcer la confiance du public à l'égard des institutions.

En avril 2024, le premier ministre et moi-même avons publié la nouvelle politique de défense du Canada, intitulée *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*. Y étaient prévus d'importants investissements pour le CST à l'appui des cyberopérations étrangères et des capacités de collecte de renseignement étranger. Comptabilisés dans le budget 2024, ces investissements comprennent 917 millions de dollars pour les cinq prochaines années, et représentent un total de 2,83 milliards de dollars sur 20 ans.

Les investissements proposés traduisent le fait que le mandat du CST jouera un rôle crucial pour contrer les menaces en constante évolution qui guettent le Canada. Le CST a une feuille de route exemplaire pour ce qui est de produire des résultats qui contribuent à protéger la sécurité nationale, la prospérité économique et les valeurs démocratiques du Canada, de même que la sécurité des Canadiennes et des Canadiens. Ces investissements iront soutenir le travail du CST afin qu'il puisse continuer à protéger le Canada.

Le CST rassemble des fonctionnaires dévouées et dévoués qui continueront de veiller à la réalisation de la mission de l'organisme, et de travailler sans relâche afin de protéger les Canadiennes et les Canadiens.

L'honorable Bill Blair, CP, COM, député
Ministre de la Défense nationale

Message de la chef

À la lecture du présent rapport, il est difficile de croire à l'ampleur de ce qui a été accompli en tout juste un an. Je suis quotidiennement impressionnée par l'ardeur au travail et l'ingéniosité que les employées et employés du CST consacrent à la réalisation de notre mission, mais la possibilité d'en saisir la portée en un coup d'œil ne fait que confirmer ce que j'observe et dont je suis témoin chaque jour.

Le présent rapport n'en brosse même pas un portrait exhaustif, étant donné que tout ce que nous faisons ne peut être partagé dans un rapport public, mais ceci ne veut pas dire que nous agissons sans supervision ni examens externes. Ce que nous pouvons ou non effectuer est décrit très clairement dans la *Loi sur le CST*, et les organismes d'examen externe sont là pour examiner minutieusement le travail que nous menons pour le compte des Canadiennes et des Canadiens.

En fait, les activités du CST n'ont jamais été scrutées d'aussi près, particulièrement dans le contexte de l'Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques du gouvernement fédéral. Le CST salue le fait que l'on considère l'ingérence étrangère avec autant de sérieux. Il s'agit d'une question au sujet de laquelle nous effectuons publiquement des mises en garde depuis 2017, y compris, récemment, dans le rapport intitulé Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023[3]. Comme le démontre ce rapport, l'intelligence artificielle hisse la menace à un niveau inédit en raison de sa capacité à répandre la désinformation et la méfiance. La section Activités d'États hostiles et ingérence étrangère du présent rapport décrit le travail qu'accomplit le CST afin de contrer ces menaces, mais il faudra, pour les surmonter, des efforts soutenus à l'échelle du gouvernement et de la société tout entière.

Quoique les sources de préoccupation soient nombreuses, le CST a remporté plusieurs succès dignes de mention pendant l'année. Il a contribué à la lutte contre la cybercriminalité en conduisant sa toute première opération défensive, et une série de cyberopérations actives lui a permis d'attaquer la cybercriminalité à la base. Pendant ce temps, le Centre pour la cybersécurité du CST a émis des mises en garde précoces, avant que le mal puisse être fait, au sujet de la possible compromission par rançongiciel de plus de 250 organisations canadiennes. Le nombre d'organisations du secteur des infrastructures essentielles qui font affaire avec le CST a continué de croître, et la majorité des institutions fédérales, dont des sociétés d'État, ont maintenant au moins un de nos capteurs pour les aider à détecter les cybermenaces.

Il ne s'agit là que de quelques-uns des nombreux exemples que vous pourrez découvrir dans le présent rapport et qui mettent en lumière les façons dont nous nous sommes acquittés de notre mission cette année, de façon systématique et efficace. Toutefois, il y a toujours davantage à accomplir. Le CST continue d'innover grâce à de nouveaux partenariats et à l'emploi de nouvelles technologies pour répondre aux exigences croissantes d'aujourd'hui et de demain.

Avant tout, ce sont celles et ceux qui œuvrent au CST qui rendent possible l'atteinte de ces résultats. Comme le démontre la section intitulée Personnes, le CST est une organisation qui place ses employées et employés au premier rang. Nous n'adoptons pas cette approche uniquement parce qu'il s'agit de la bonne chose à faire ou que cela rend le travail plus agréable (bien que ce soit vrai dans les deux cas), mais bien parce qu'il s'agit de **« la »** façon d'obtenir des résultats hors du commun.

Le CST connaît une évolution rapide. Notre effectif a enregistré une croissance importante au cours de l'année écoulée, et les investissements annoncés dans le cadre de la nouvelle politique de défense du Canada et dans le budget 2024 favoriseront un essor plus grand encore. Au fil de ces changements, nous continuerons d'engager des efforts en vue de faire du CST un milieu de travail où toutes et tous se sentent valorisés, respectés et habilités.

Dans l'environnement de menace en évolution rapide qui est le nôtre, le travail du CST n'a jamais été aussi crucial. Le Canada a confiance en nous pour donner le meilleur de nous-mêmes, et je peux affirmer sans crainte de me tromper que nous sommes plus prêtes et prêts que jamais à relever le défi.

Caroline Xavier (elle)
Chef du CST

Manière dont s'imbriquent les différents volets du mandat du CST

Les mandats du CST en matière de cybersécurité, de renseignement étranger et de cyberopérations fonctionnent en synergie afin de produire une gamme de résultats qui bénéficient aux Canadiennes et aux Canadiens. Le fait que tous ces mandats soient pris en charge au sein d'un même organisme procure au CST et au Canada des avantages uniques.

L'exemple qui suit se fonde sur une cyberopération passée du CST dans le cadre de la campagne qu'il mène en permanence contre la cybercriminalité.

Cyberincident

Une organisation canadienne comptant au nombre des infrastructures essentielles signale au Centre pour la cybersécurité une attaque par rançongiciel.

Cybersécurité (criminalistique numérique)

L'équipe d'intervention en cas d'incident du Centre pour la cybersécurité identifie un groupe bien connu d'attaques par rançongiciel comme coupable.

Renseignement étranger

Le CST recueille du renseignement électromagnétique étranger sur le groupe et avertit plusieurs clients gouvernementaux, de même que la haute direction. Le renseignement en question est également mis à profit pour mener des cyberopérations et pour favoriser la cyberrésilience.

Cyberopérations étrangères

Le CST et ses partenaires de la collectivité des cinq conduisent des cyberopérations pour perturber les activités du groupe et empêcher d'autres incidents.

Cybersécurité (cyberrésilience)

Le Centre pour la cybersécurité utilise la criminalistique numérique **et** le renseignement étranger pour améliorer les capacités de cyberrésilience et de cyberdéfense du Canada. Il fournit également des avis et conseils aux propriétaires d'infrastructures essentielles afin de les aider à se défendre contre de futures attaques.

Renseignement électromagnétique étranger

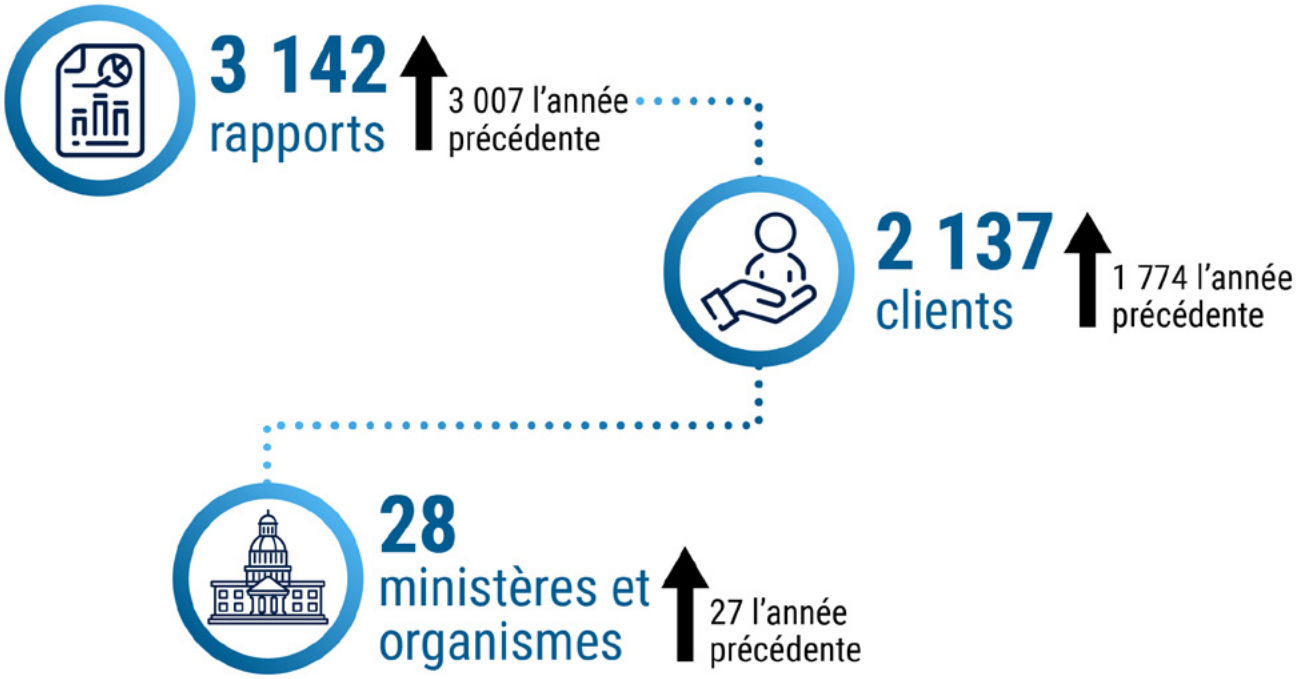
Le CST recueille du renseignement électromagnétique étranger (ou SIGINT) afin de procurer au gouvernement du Canada de l'information au sujet des menaces étrangères. Le SIGINT peut englober tout type de communication électronique, allant des messages texte aux signaux satellite. Aux termes de la *Loi sur le CST*, les activités de collecte de renseignement étranger ne doivent pas cibler la population canadienne ou les personnes en sol canadien.

Priorités en matière de renseignement étranger

Cette année, le CST a fourni des rapports de renseignement étranger en fonction des priorités du gouvernement du Canada, dont :

- les activités d'États hostiles, notamment :
  - → la désinformation,
  - → l'espionnage,
  - → l'ingérence étrangère et l'influence néfaste,
  - → le contre-espionnage,
  - → le vol de propriété intellectuelle,
  - → les activités de cybermenace;
- le terrorisme et l'extrémisme violent;
- le cybercrime;
- l'invasion de l'Ukraine par la Russie;
- la République populaire de Chine et la stabilité de la région indo-pacifique;
- la guerre entre Israël et le Hamas;
- l'instabilité en Haïti;
- la souveraineté dans l'Arctique;
- le soutien aux opérations des Forces armées canadiennes;
- l'enlèvement de Canadiennes et Canadiens à l'étranger;
- les menaces pour les Canadiennes et Canadiens partout dans le monde;
- les événements urgents et les nouveaux événements mondiaux.

Rapports de renseignement étranger du CST pour l'année 2023 à 2024



Soutien aux Forces armées canadiennes

Les Forces armées canadiennes (FAC) constituent l'un des plus importants partenaires fédéraux du CST. Le soutien fourni par le CST aux FAC comprend :

- renseignement électromagnétique;
- sécurité des communications;
- cybersécurité;
- assistance et collaboration dans le cadre de cyberopérations étrangères;
- soutien linguistique.

Cette année, le CST a collaboré étroitement avec les FAC à l'appui d'activités comme :

- la protection des missions des FAC à l'étranger;
- la défense de la souveraineté du Canada dans l'Arctique;
- l'appui à la défense continentale de l'Amérique du Nord;
- la réponse aux besoins des FAC en matière de renseignement, y compris concernant le conflit en Ukraine (opérations Unifier et Reassurance);
- le soutien aux opérations des forces spéciales;
- l'appui aux FAC déployées dans le cadre d'opérations comme le départ assisté de Canadiennes et de Canadiens se trouvant à l'étranger.

Réponse opérationnelle 24/24, 7/7

Le CST est un organisme constamment sur le qui-vive. Lorsque se produisent des situations de crise qui comportent des menaces pour le Canada ou pour les Canadiennes et Canadiens à l'étranger, le CST est prêt à répondre aux besoins urgents du gouvernement du Canada en conformité avec son mandat.

Le Centre opérationnel de production et de coordination du CST, le COPCC, travaille jour et nuit pour coordonner les efforts engagés par le CST en réaction aux cyberincidents critiques et aux crises internationales. Cette année, le COPCC a fourni en temps opportun de l'information aux hautes et hauts responsables au sujet d'une série d'événements survenus à l'échelle internationale comportant une incidence sur le Canada (voir la section Renseignement électromagnétique étranger). Le COPCC a aussi collaboré avec Affaires mondiales Canada et les FAC afin d'appuyer l'évacuation de ressortissantes et ressortissants canadiens du Soudan et d'Israël.

Toujours vigilant, le COPCC assure une veille permanente pour s'assurer que le CST peut fournir au gouvernement du Canada l'information voulue au moment crucial.

Assistance technique et opérationnelle

Le mandat confié au CST lui permet d'appuyer ses partenaires fédéraux en matière de sécurité, d'application de la loi et de défense, sur demande de leur part et en vertu des pouvoirs juridiques qu'ils détiennent.

En 2023 à 2024, le CST a reçu 45 demandes d'assistance technique et opérationnelle de la part de partenaires fédéraux, et a fourni son aide dans 43 de ces cas.

Les demandes d'assistance en chiffres

- 2023 à 2024
  → Reçues : 45
  → Approuvées : 43
- 2022 à 2023
  → Reçues : 62
  → Approuvées : 59

Méthodes de partage du renseignement

Les rapports de renseignement du CST ne peuvent être lus que par les utilisatrices et utilisateurs autorisés à l'échelle du gouvernement du Canada et de la collectivité des cinq. Le CST a institué de robustes mécanismes pour s'assurer que cette information de nature très délicate parvient à ses destinataires sans tomber entre de mauvaises mains.

Diffusion électronique

Le CST exploite le Réseau canadien Très secret (RCTS). Il s'agit d'un réseau informatique sécurisé utilisé pour collaborer et communiquer au niveau Très secret. Par exemple, le RCTS permet à ses clientes et clients répartis à l'échelle du gouvernement du Canada et de la collectivité des cinq d'avoir accès aux rapports de renseignement du CST. Ce réseau prend aussi en charge les appels audio et vidéo de niveau Très secret.

Les personnes autorisées peuvent consulter les rapports de renseignement du CST et de la collectivité des cinq en ouvrant une session dans le RCTS pour accéder à la base de données des rapports du CST. Ces rapports demeurent dans la base de données; le système ne permet pas aux clientes et clients de copier, de sauvegarder ou d'envoyer les rapports à d'autres personnes. Il enregistre et fait le suivi de l'information, notamment sur qui lit un rapport donné et à quel moment.

Agentes et agents des relations avec la clientèle

Les agentes et agents des relations avec la clientèle (ARC) sont des membres du personnel du CST intégrés dans les institutions du gouvernement du Canada. Ces personnes transmettent des copies papier de rapports de renseignement du CST aux utilisatrices et utilisateurs autorisés, par exemple des ministres du Cabinet et des hautes et hauts fonctionnaires. Les ARC ont la responsabilité de faire le suivi du lectorat et de détruire toute copie papier des rapports de renseignement.

Agente ou agent de diffusion du SIGINT

Les agentes et agents de diffusion SIGINT (ADS) sont des membres d'autres ministères du gouvernement du Canada qui ont accès à la base de données des rapports de renseignement par l'intermédiaire du RCTS. Ces personnes sont accréditées par le CST pour partager les rapports de renseignement étranger avec les clientes et clients autorisés de leur ministère d'attache. Les ADS utilisent les mêmes outils que les ARC du CST pour faire le suivi du lectorat et en journaliser les activités.

Améliorations

En mai 2023, le Rapport du très honorable David Johnston, rapporteur spécial indépendant sur l'ingérence étrangère[4] préconisait un meilleur suivi du renseignement au sein du gouvernement du Canada. En réponse à cette recommandation, la collectivité de la sécurité et du renseignement a apporté divers changements à la manière dont les produits classifiés sont diffusés. Parmi les efforts engagés par le CST, notons :

- un accroissement du nombre d'ARC et d'ADS afin d'appuyer davantage de hautes et hauts fonctionnaires;
- la prestation d'appui aux sous-ministres et aux ministres du Cabinet dans le cadre de nouveaux forums de sensibilisation et de partage du renseignement;
- l'élargissement à la collectivité plus vaste de la sécurité et du renseignement de l'accès au système de diffusion électronique du renseignement du CST, afin de systématiser le suivi et la journalisation des activités.

Importantes mises à jour au Réseau canadien Très secret

Durant l'année financière, le CST a effectué une refonte complète du RCTS et en a amélioré la sécurité, la capacité et la fiabilité. Parmi les nouveautés figurent la vidéo haute définition et le chiffrement de bout en bout. Cette mise à jour a permis au CST de commencer à consolider plusieurs fonctions qui existaient à la fois sur le RCTS et sur le réseau interne du CST, ce qui a réduit les dédoublements et permis des économies.

RCTS
RÉSEAU CANADIEN TRÈS SECRET

Cybersécurité

Le Centre pour la cybersécurité est l'autorité opérationnelle et technique du Canada en matière de cybersécurité. En tant que partie intégrante du CST, il fournit des conseils et des services de pointe en vue d'aider à prévenir les cyberincidents et à faire en sorte que les services critiques demeurent fonctionnels et accessibles.

Le mandat du Centre pour la cybersécurité s'applique aux institutions fédérales et aux systèmes d'importance, ce qui englobe les infrastructures essentielles. Aux termes de la *Loi sur le CST*, le Centre pour la cybersécurité peut aussi venir en aide à toute autre entité désignée par la ou le ministre de la Défense nationale comme étant d'importance pour le gouvernement du Canada. Des exemples, cette année, comprennent la prestation de services de cyberdéfense aux territoires du Canada (voir la section Sécuriser le Nord) et une aide à l'Ukraine et à la Lettonie en matière de cybersécurité (voir la section Assistance à la Lettonie et à l'Ukraine en matière de cybersécurité).

Institutions fédérales

Le Centre pour la cybersécurité collabore avec Services partagés Canada, le Secrétariat du Conseil du Trésor du Canada et d'autres partenaires fédéraux en vue de protéger les biens de TI du gouvernement du Canada. Le Centre pour la cybersécurité coopère également, de manière ponctuelle, avec des sociétés d'État et d'autres institutions fédérales qui n'appartiennent pas au réseau central.

Capteurs

Les capteurs sont des outils logiciels qui permettent de détecter les cyberactivités malveillantes sur les dispositifs, sur le périmètre du réseau et au sein du nuage. Ils comptent parmi les instruments les plus cruciaux que détient le Centre pour la cybersécurité pour défendre les réseaux du gouvernement du Canada.

Le Centre pour la cybersécurité met à profit l'apprentissage automatique pour l'aider à détecter les anomalies dans les données des capteurs et à bloquer automatiquement les activités suspectes ou malveillantes.

Cette année, le Centre pour la cybersécurité a bloqué en moyenne 6,6 milliards d'activités malveillantes par jour, comprenant aussi bien des analyses de routine que des tentatives d'intrusion sophistiquées.

Le nombre d'institutions fédérales participant au programme de capteurs du Centre pour la cybersécurité a continué d'augmenter cette année. Parmi celles-ci, davantage de sociétés d'État et de ministères et organismes de petite taille, demandant de leur propre initiative à y prendre part.

Le Centre pour la cybersécurité a aussi déployé des capteurs pour aider à protéger les cybersystèmes d'un petit nombre d'institutions non fédérales prioritaires. Cette année, il a amorcé le déploiement de capteurs dans les systèmes des gouvernements des Territoires du Nord-Ouest, du Nunavut et du Yukon (voir la section Sécuriser le Nord).

Déploiement des capteurs en date de mars 2024

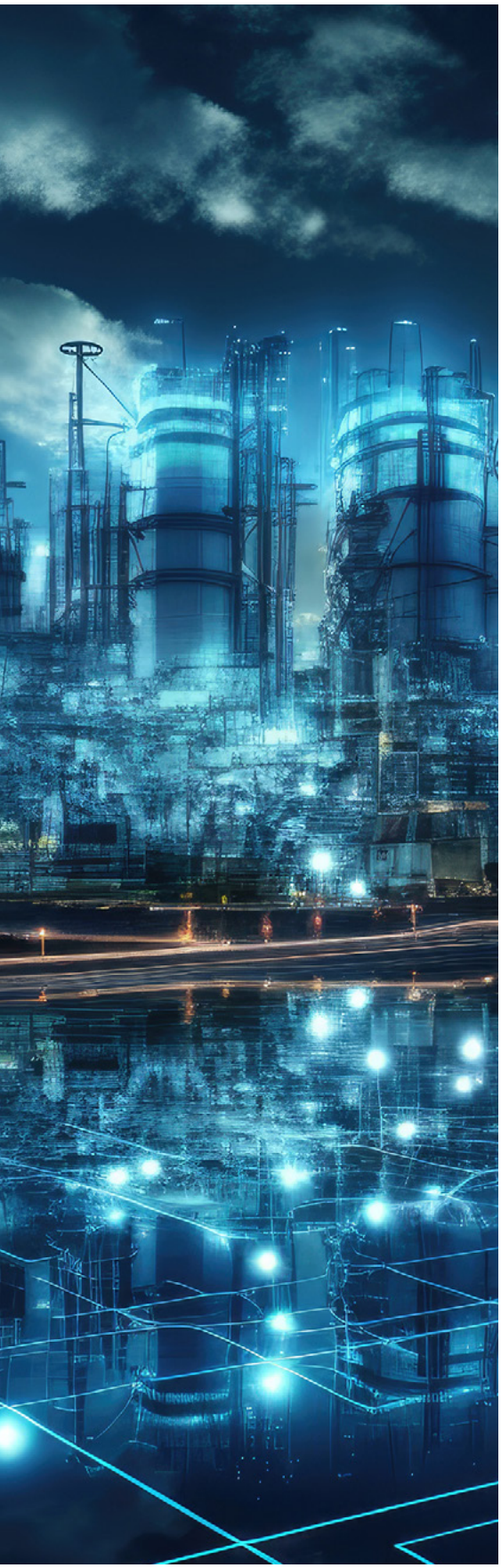
- Capteurs au niveau de l'hôte (HBS pour *Host Based Sensors*) : 102 institutions fédérales (comparativement à 85 l'année précédente)
- Capteurs au niveau du nuage (CBS pour *Cloud Based Sensors*) : 80 institutions fédérales (comparativement à 72 l'année précédente)
- Capteurs au niveau du réseau (NBS pour *Network Based Sensors*) : 84 institutions fédérales tirent profit des capteurs déployés en périmètre de réseau (aucun changement)
- Capteurs virtuels au niveau du réseau : 5 institutions fédérales (aucun changement)

Déploiement des capteurs par type d'institution

En date de mars 2024, le nombre d'institutions dotées d'au moins un capteur se présentait comme suit :

- 167 institutions fédérales sur 217, dont :
  → 23 sociétés d'État sur 46 (comparativement à 11 en 2023),
  → 42 petits ministères et organismes sur 43 (comparativement à 26 en 2023) [5];
- 4 institutions non fédérales.

Le programme de capteurs en un coup d'œil



Protection des dispositifs mobiles du gouvernement du Canada

Cette année, le Centre pour la cybersécurité s'est doté d'une nouvelle capacité pour améliorer la cybersécurité des dispositifs mobiles du gouvernement du Canada. Le Centre pour la cybersécurité a mis en place une connexion sécurisée pour récupérer les données de cybersécurité des serveurs de gestion des appareils mobiles (serveurs MDM pour *Mobile Device Management*). Le Centre pour la cybersécurité traite les données au moyen de divers modèles de menaces fondés sur le renseignement et modèles d'analyse en vue de déceler des vulnérabilités et des signatures d'activités de cybermenace sur les dispositifs fournis par le gouvernement. Le Centre pour la cybersécurité transmet les résultats de ses analyses aux opératrices et opérateurs MDM, qui peuvent les utiliser pour atténuer les menaces. Ces personnes pourraient, par exemple, s'en servir pour effectuer des mises à jour ou pour supprimer des applications interdites.

Infrastructures essentielles

Cette année, le Centre pour la cybersécurité a échangé avec près de 1 900 organisations responsables d'infrastructures essentielles (IC) afin d'accroître la cyberrésilience du Canada dans tous les secteurs.

Les organisations responsables des infrastructures essentielles sont considérées comme des systèmes d'importance parce qu'elles sont cruciales pour le fonctionnement du Canada. Les secteurs clés comprennent :

- les institutions démocratiques;
- l'éducation;
- l'énergie;
- les finances;
- l'alimentation;
- la santé;
- les technologies de l'information et les communications;
- le secteur manufacturier;
- les gouvernements fédéral, provinciaux et territoriaux, et les gouvernements autochtones;
- le transport;
- l'eau.

Le secteur de l'énergie

Cette année, le Centre pour la cybersécurité a accentué ses efforts de collaboration avec le secteur canadien de l'énergie en vue d'accroître la cyberrésilience de ce dernier.

En juin 2023, le Centre pour la cybersécurité a publié une évaluation des cybermenaces contre le secteur pétrolier et gazier[6]. Selon ce rapport, les rançongiciels constituent la principale menace pouvant affecter l'approvisionnement en pétrole et en gaz du Canada, et il est fort probable que les cyberactivités parrainées par des États et ciblant ce secteur se poursuivent.

Ceci inclut aussi bien le cyberespionnage que les activités visant à se positionner pour pouvoir déployer des cyberattaques destructives contre le Canada et son infrastructure pétrolière et gazière.

Parallèlement à la publication de ce rapport, le CST a eu des séances de breffage classifiées dans des installations sécurisées partout au pays afin de donner aux cadres du secteur pétrolier et gazier des informations supplémentaires de nature trop délicate pour pouvoir les rendre publiques. Le CST a pris cette mesure exceptionnelle en raison de l'importance de ce secteur pour la sécurité nationale du Canada.

Au fil de l'année, le CST a inscrit trois partenaires de plus du secteur pétrolier et gazier à certains de ses services par abonnement, notamment les notifications en matière de cybersécurité et les flux automatisés de données sur les menaces du Centre pour la cybersécurité.

Le Programme de la flamme bleue[7], mené en partenariat avec l'Association canadienne du gaz (ACG), a doublé le nombre de ses membres, passé de quatre à huit organisations. En juillet 2023, le Centre pour la cybersécurité a organisé un atelier avec l'ACG afin de cerner des manières d'améliorer le partage de l'information et les services offerts aux entreprises participant au Programme de la flamme bleue.

Cette année, le Centre pour la cybersécurité est devenu un membre gouvernemental du Energy Security Technical Advisory Committee[8] (en anglais seulement) nouvellement constitué. Ce groupe d'échange d'information et de collaboration a été établi à l'initiative de l'ACG et rassemble des partenaires de l'industrie et du gouvernement en vue d'amener le secteur à une plus grande maturité en matière de cybersécurité.

> **« Il est difficile d'exagérer l'importance du secteur pétrolier et gazier pour la sécurité nationale. »**
>
> - Centre canadien pour la cybersécurité, Cybermenaces contre le secteur pétrolier et gazier du Canada

Provinces et territoires

Renforcer la collaboration avec les provinces et les territoires a constitué une des grandes priorités du Centre pour la cybersécurité cette année (voir aussi la section Sécuriser le Nord).

En mai 2023, le Centre pour la cybersécurité a accueilli sa première table ronde sur la cybersécurité, consacrée en totalité à la collaboration entre les dirigeantes et dirigeants fédéraux, provinciaux et territoriaux à ce chapitre. L'atelier de deux jours s'est concentré sur les façons dont le Centre pour la cybersécurité pouvait le mieux appuyer les provinces et territoires sur les plans des services de cyberdéfense, du soutien aux interventions en cas d'incident et du renforcement de la résilience en matière de cybersécurité.

En novembre 2023, à partir de la rétroaction obtenue lors de la table ronde, le Centre pour la cybersécurité a mis en place des capacités de communication sécurisée pour des hautes et hauts fonctionnaires provinciaux et territoriaux. Cette plateforme chiffrée de bout en bout permet des communications sécurisées avec les hautes et hauts responsables du Centre pour la cybersécurité en cas de cyberincident.

Entrepreneures et entrepreneurs de la Défense

En juin 2023, le gouvernement du Canada a annoncé un nouveau programme de certification de cybersécurité afin de protéger la chaîne d'approvisionnement du Canada en matière de défense[9]. Pour remporter des contrats d'approvisionnement gouvernementaux en matière de défense, les entreprises devront prouver que leur posture de sécurité répond à des normes précises. Le programme applique les mêmes exigences que les États-Unis, de sorte qu'il suffira aux entreprises menant des activités dans les deux pays d'obtenir la certification une seule fois.

En août 2023, le Centre pour la cybersécurité a mis sur pied une nouvelle équipe pour aider les entrepreneures et entrepreneurs de la Défense à se préparer à répondre aux nouvelles exigences techniques.

Séances de breffage et engagements

Cette année, les spécialistes du Centre pour la cybersécurité ont continué de partager l'information exploitable en matière de cybersécurité avec les partenaires responsables d'infrastructures essentielles de tous les secteurs dans le cadre de :

- 23 séances de breffage sur les cybermenaces;
- 7 présentations « Passons à l'action » sur divers sujets dont :
  - → le cybercrime,
  - → les menaces contre la chaîne d'approvisionnement,
  - → le développement de systèmes d'intelligence artificielle sécurisés;
- environ 230 conférences.

Outils et services

Le Centre pour la cybersécurité partage ses outils et ses services afin d'aider les responsables de la cyberdéfense à accomplir leur travail. Certains de ces outils et services ne sont proposés qu'aux partenaires gouvernementaux et aux partenaires responsables des infrastructures essentielles. D'autres sont accessibles au public.

Flux automatisé de données sur les menaces

Le Centre pour la cybersécurité a continué de partager des données sur les cybermenaces par l'intermédiaire d'Aventail, son flux automatisé de renseignements sur les menaces. Cette année, Aventail a transmis plus de 30 700 indicateurs de compromission, au total, pour aider les organisations à repérer les activités malveillantes sur leurs réseaux. Cela correspond à l'envoi d'environ 84 indicateurs par jour.

- Mars 2024
  - → Nombre total d'organisations inscrites à Aventail : 230
    - Institutions fédérales : 57
    - Infrastructures essentielles : 173
- Mars 2023
  - → Nombre total d'organisations inscrites à Aventail : 152
    - Institutions fédérales : 20
    - Infrastructures essentielles : 132

Analyse de maliciels

Les partenaires peuvent soumettre des fichiers suspects à Assemblyline[10], la plateforme de détection et d'analyse de maliciels du Centre pour la cybersécurité. Cette dernière leur indiquera rapidement si un fichier est malveillant, et recommandera des mesures d'atténuation précises pour le type de maliciel concerné. Il s'agit d'une capacité particulièrement utile pour les courriels que l'on soupçonne de constituer des tentatives d'hameçonnage, ou lors d'une intervention en réponse à un cyberincident.

Assemblyline exploite l'apprentissage automatique (une branche de la technologie de l'intelligence artificielle [IA]) pour optimiser ses capacités d'analyse. En date de février 2024, Assemblyline a ajouté plusieurs options facultatives, alimentées par des modèles de langage de grande taille (une branche de l'IA générative).

Les utilisatrices et utilisateurs peuvent maintenant :

- créer un sommaire de l'analyse de maliciels;
- produire un rapport imprimable offrant une analyse plus détaillée;
- analyser des parties de code et obtenir une explication de ce que le maliciel effectue;
- interagir avec un agent conversationnel intelligent pour naviguer dans Assemblyline et poser des questions de suivi.

Cette année, Assemblyline a analysé plus d'un milliard de fichiers suspects. Le nombre d'organisations qui utilisent le service a augmenté de 35 %.

- Mars 2024
  - → Nombre total de partenaires : 308
    - Gouvernement du Canada : 58
    - Infrastructures essentielles : 250
- Mars 2023
  - → Nombre total de partenaires : 228
    - Gouvernement du Canada : 45
    - Infrastructures essentielles : 183

Tableau de bord de la posture de sécurité

ObservationDeck est un tableau de bord interactif qui permet aux ministères du gouvernement du Canada de détecter les vulnérabilités potentielles que présentent leurs biens de TI. Il combine l'information issue des capteurs du Centre pour la cybersécurité avec des données de source ouverte afin de mettre en relief les facteurs de risque potentiels et les vecteurs d'attaque.

Le nombre de ministères du gouvernement du Canada qui utilisent ObservationDeck est passé de 57 à 70 cette année.

Plateforme de triage d'alertes

Cette année, le Centre pour la cybersécurité a créé Howler, une nouvelle plateforme destinée aux équipes du Centre des opérations de sécurité (COS). Cette plateforme a été rendue publique en avril 2024. Howler est une plateforme de triage d'alertes, ce qui signifie qu'elle aide les analystes à trier et à filtrer d'importantes quantités d'alertes de cybersécurité. Ces alertes sont produites en grand nombre par les systèmes automatisés de détection des menaces. Howler permet aux analystes du triage de faire ce qui suit :

- automatiser les tâches répétitives;
- éliminer certains scénarios;
- réduire le nombre de fausses alertes;
- personnaliser l'information qu'ils reçoivent.

Toutes ces options aident les analystes à identifier les cyberincidents et à y répondre, le tout plus rapidement.

Pour en savoir plus au sujet de Howler[11], consultez le site Web.

Projet pilote de détection des menaces

Le Centre pour la cybersécurité explore les façons d'aider les organisations du secteur des infrastructures essentielles à améliorer leurs capacités de détection des cybermenaces. Cette année, le Centre pour la cybersécurité a travaillé, en collaboration avec un partenaire du secteur de l'énergie, à un projet pilote appelé SSAJS (pour Service de surveillance et d'analyse des journaux de sécurité).

Comme une organisation offrant des services sur mesure, le Centre pour la cybersécurité a ajusté les capacités génériques d'analyse de menaces du partenaire en fonction de son environnement opérationnel propre. Les premiers résultats suggèrent que cette approche a le potentiel de réduire le nombre de faux positifs de même que la désensibilisation aux alertes qui peut en résulter. Le Centre pour la cybersécurité mène actuellement une analyse exhaustive du projet pilote. Les résultats de cet examen alimenteront les futurs produits de cybersécurité destinés aux partenaires responsables des infrastructures essentielles.

Notifications en matière de cybersécurité

Le Centre pour la cybersécurité a continué d'avertir la collectivité de la cybersécurité des problèmes potentiels tout au long de l'année. Différents types de notifications sont utilisés pour différentes situations. Chaque type comporte des détails techniques et des directives à l'intention des propriétaires de systèmes sur les façons d'atténuer la menace.

Avis et alertes

Le Centre pour la cybersécurité publie des avis et des alertes sur son site Web et dans ses médias sociaux. Les avis sont utilisés pour les problèmes courants de cybersécurité, tandis que les alertes se rapportent à des menaces urgentes ou présentant des risques élevés.

Cyberflashs

Les cyberflashs sont des alertes qui contiennent de l'information sensible ne pouvant être rendue publique. Les cyberflashs sont partagés directement avec les partenaires du Centre pour la cybersécurité.

Notifications prioritaires

Des notifications prioritaires sont envoyées directement aux partenaires inscrits au Service national de notification de cybermenace (SNNC) du Centre pour la cybersécurité. Ce service analyse un ensemble de flux de menaces en vue d'y repérer des références aux actifs identifiés par ses abonnés. Le SNNC peut envoyer des notifications prioritaires en même temps que des alertes ou des cyberflashs, pour aviser des partenaires que leurs réseaux sont exposés.

Tableaux de bord

Les tableaux de bord fournissent un résumé mensuel des données du SNNC qui compare les données d'une ou un abonné avec celles de ses pairs anonymisés dans son secteur, afin de favoriser une amélioration de sa posture de sécurité.

Notifications en 2023 à 2024

- 779 avis
- 20 alertes
- 10 cyberflashs
- 18 notifications prioritaires
- Plus de 1 100 abandonnées et abonnés au SNNC
- Plus de 175 000 notifications du SNNC
- 267 abonnées et abonnés aux tableaux de bord

Notifications de signes avant-coureurs d'une attaque par rançongiciel

Cette année, le Centre pour la cybersécurité a commencé à envoyer des notifications de signes avant-coureurs d'une attaque par rançongiciel, en se fondant sur la détection précoce de certaines souches de rançongiciels. La section Cybercriminalité contient davantage d'information au sujet des notifications de signes avant-coureurs d'une attaque par rançongiciel.

Gestion des incidents

Lorsque des cyberincidents se produisent, réagir rapidement et prendre les mesures appropriées peut réduire considérablement les dommages et accélérer le processus de rétablissement.

Cette année, le Centre pour la cybersécurité a aidé à répondre à 2 192 cyberincidents à l'échelle du gouvernement et des infrastructures essentielles du Canada. Ce nombre est légèrement supérieur à celui de l'an dernier.

La définition fournie par le Centre pour la cybersécurité d'un cyberincident[12] couvre une vaste gamme de tentatives malveillantes, **qu'elles aient réussi ou non**.

Dossiers de cyberincidents ouverts par le Centre pour la cybersécurité

- 2023 à 2024
  → Total de dossiers : 2 192
  - Institutions fédérales : 1 017
  - Infrastructures essentielles : 1 175
- 2022 à 2023
  → Total de dossiers : 2 089
  - Institutions fédérales : 957
  - Infrastructures essentielles : 1 132

Renseignement sur les cybermenaces

Le CST recueille du SIGINT sur les groupes parrainés par des États étrangers ou alliés à des États étrangers et sur les groupes cybercriminels qui représentent une menace pour le Canada. Le renseignement recueilli porte sur leurs tactiques, leurs techniques et leurs procédures (TTP), sur l'infrastructure qu'ils utilisent et sur les auteures et auteurs de menaces comme tels.

Cette année, le CST a identifié des cyberactivités menées par des États étrangers ou par des groupes alliés à des États étrangers qui ciblaient le Canada, et a mis en place des moyens de défense et d'atténuation des cybermenaces dirigées contre le Canada et ses partenaires.

Le CST a également fourni des informations sur la manière dont les groupes cybercriminels opèrent, et a relevé des liens concrets entre les groupes et leurs partenaires et associés ciblant les infrastructures essentielles. Ce renseignement a contribué aux efforts engagés par le Canada et ses alliés pour perturber, saper et contrer les capacités des groupes cybercriminels (voir la section Cyberopérations étrangères pour lutter contre les cybercrimes). Il a également servi à aider les gouvernements alliés à formuler des accusations et à émettre des sanctions.

En outre, ce renseignement aura permis de contribuer à améliorer les activités menées par le Centre pour la cybersécurité en vue d'aider le gouvernement du Canada, de même que ses partenaires responsables des infrastructures essentielles et d'autres systèmes d'importance, à atténuer les cybermenaces. Par exemple, le SIGINT a appuyé la production d'alertes et l'évaluation de menaces par le Centre pour la cybersécurité, et lui a procuré des milliers d'indicateurs de compromission pour alimenter Aventail, son flux automatisé de données sur les menaces.

Renseignement sur les cybermenaces : étude de cas

En début d'année 2023, le renseignement étranger a permis au Centre pour la cybersécurité de réagir à un incident susceptible d'occasionner de graves dommages à la propriété et de poser un danger à la vie humaine. Les activités de renseignement ont permis de découvrir qu'une ou un auteur de cybermenaces allié à un État avait mené une cyberattaque contre une IE du Canada dans le but d'en perturber les activités et, potentiellement, de lui infliger des dommages majeurs.

L'auteure ou auteur de menaces, qui était allié à un État, a réussi à accéder au réseau et, avec des intentions malveillantes, à le configurer afin que son fonctionnement soit perturbé en profitant d'un dispositif relié à Internet et mal protégé. Le renseignement étranger recueilli par le CST a permis de mettre au jour ces activités, et son Centre pour la cybersécurité a collaboré avec ses partenaires en matière de sécurité et de renseignement, dont la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRC), pour informer les responsables de la sécurité publique. Ces responsables ont ensuite travaillé avec les fournisseurs d'infrastructures essentielles pour faire en sorte d'atténuer la menace avant que des dommages ne surviennent.

Bien qu'il n'ait pas été établi que cette activité a été commanditée par un État, cette situation démontre l'aggravation des menaces contre les systèmes les plus cruciaux de notre pays, et le rôle et la position uniques du CST pour s'y attaquer en mettant à profit son mandat en matière de renseignement étranger. Cela souligne aussi l'importance d'appliquer et de mettre en œuvre les avis et conseils dispensés par le Centre pour la cybersécurité en vue d'accroître la cyberrésilience.

Partenaires internationaux en matière de cybersécurité

Le Centre pour la cybersécurité collabore avec d'autres organismes de cybersécurité à l'échelle mondiale en vue de mettre en place une défense commune contre les cybermenaces.

Appui conjoint des membres de la collectivité des cinq

Lorsque les membres de la collectivité des cinq et leurs alliés partageant les mêmes valeurs s'expriment d'une seule voix, le message est amplifié partout sur la planète. Cette année, le CST et le Centre pour la cybersécurité ont appuyé un nombre record de publications conjointes sur des questions suscitant des préoccupations communes, dont :

- les activités de cybermenace parrainées par des États qui ciblent des infrastructures essentielles;
- les activités cybercriminelles;
- l'adoption de lignes directrices sur le développement et l'utilisation sécurisés de l'IA (voir la section Intelligence artificielle).

On peut consulter les 14 documents qui ont fait l'objet d'une publication conjointe cette année sur le site Web du Centre pour la cybersécurité, sous les rubriques nouvelles et événements[13] .

« Le Canada a été à nos côtés en tête de peloton en matière de cybersécurité, et nous entretenons avec lui une relation extrêmement étroite et approfondie à cet égard. C'est là en fait que notre collaboration se démarque le plus au sein de la collectivité des cinq, et le Canada est à l'origine de certains des principes que nous utilisons, y compris en ce qui a trait aux façons de surveiller les menaces à l'échelle du gouvernement; nous leur rendons d'ailleurs la pareille en partageant à notre tour. À mon avis, le Canada fait réellement preuve d'une excellente capacité d'adaptation, et mise beaucoup sur la cybersécurité. »

- Éloges de nos partenaires du Royaume-Uni, Government Communications Headquarters (GCHQ) – Rapport du Comité du renseignement et de la sécurité du Royaume-Uni[13] (en anglais seulement). Décembre 2023.

Transmission ultrarapide de données sur les menaces

Depuis sa mise sur pied en 2018, le Centre pour la cybersécurité a partagé de l'information sur les cybermenaces avec ses partenaires internationaux au moyen de courriels, par le truchement de portails Web et à l'aide d'autres outils de collaboration.

En mars 2023, le Centre pour la cybersécurité a inauguré une nouvelle plateforme destinée à l'échange ultrarapide de données de grande valeur sur les cybermenaces avec ses partenaires de confiance à l'échelle internationale. Cette plateforme est multidirectionnelle. Les indicateurs de compromission partagés par un partenaire sont accessibles à tous les autres partenaires participants en conformité avec leur mandat.

En mars 2024, huit pays utilisaient cette plateforme, y compris le Canada. Le Centre pour la cybersécurité envisage une augmentation du nombre de membres au cours de l'année à venir.

Conférence FIRST

Le Forum des équipes de sécurité et d'intervention en cas d'incident (*Forum of Incident Response and Security Teams* ou FIRST) est une association internationale sans but lucratif qui réunit les équipes d'intervention en cybersécurité de plus de 100 pays. Fondée en 1990, cette association fournit aux responsables de la cyberdéfense un forum inestimable pour échanger des idées, des outils et des pratiques exemplaires afin d'améliorer la cybersécurité à l'échelle mondiale.

En juin 2023, le Centre pour la cybersécurité a accueilli à Montréal la 35e conférence annuelle FIRST[15] (en anglais seulement), dont il a assuré la présidence. Le thème de cette conférence était « Donner le pouvoir aux collectivités ». En qualité de responsable de plusieurs séances, le Centre pour la cybersécurité a partagé les leçons tirées de récentes études de cas, afin d'aider les organisations à se préparer à des cyberincidents complexes ou inhabituels. Le Centre pour la cybersécurité a aussi donné un atelier d'une journée sur Assemblyline, son outil d'analyse de maliciels phare, offert en libre accès à tous les responsables de la cyberdéfense à travers le monde.

Formation en cybersécurité

Le Centre pour la cybersécurité fournit de la formation en cybersécurité et en sécurité des communications (COMSEC) par l'entremise du Carrefour de l'apprentissage[16]. Par le passé, la formation du Carrefour de l'apprentissage n'était destinée qu'aux membres du personnel et aux professionnelles et professionnels des TI du gouvernement du Canada œuvrant dans des secteurs des infrastructures essentielles. Cette année, le Carrefour de l'apprentissage a ajouté des formations en ligne pour deux nouveaux auditoires cibles :

- Introduction à la cybersécurité pour les professionnels et professionnelles de l'éducation[17]
- Cybersécurité pour les petites et moyennes entreprises[18]

Ces nouveaux cours à rythme libre sont gratuits et ouverts à toutes et à tous. Ils offrent des connaissances pratiques visant à aider celles et ceux qui les suivent à améliorer de manière significative leur cybersécurité. Les cours à l'intention des professionnelles et professionnels de l'éducation comprennent des ressources d'apprentissage destinées à faciliter la transmission de connaissances à leurs étudiantes et étudiants.

Formation à l'intention des fonctionnaires

Afin de protéger les informations et les réseaux sensibles du gouvernement du Canada, il est crucial que toutes et tous les fonctionnaires aient une solide connaissance et compréhension de la cybersécurité.

Cette année, le Carrefour de l'apprentissage a effectué une mise à jour de sa formation intitulée Principes fondamentaux de la cybersécurité[19]. Ce cours présente une introduction aux notions de base en matière de cybersécurité ainsi qu'au paysage des cybermenaces à l'intention des membres du personnel du gouvernement du Canada qui ne sont pas des spécialistes de la cybersécurité ou de la sécurité des TI.

Le Carrefour de l'apprentissage a également produit une nouvelle série de formations sur le développement de logiciels et d'applications Web sécurisés à l'intention de l'Agence du revenu du Canada. Cette série de formations dirigée par une instructrice ou un instructeur comprend quatre cours et nécessite huit jours de travail. Elle sera mise à la disposition de tous les ministères du gouvernement du Canada en 2024.

Le Carrefour de l'apprentissage de 2023 à 2024 :

- Nombre total de participantes et de participants : 12 273 (augmentation de 146 %)
- Format :
  - → Apprentissage en ligne : 68 %
  - → Cours dirigé par une instructrice ou un instructeur : 32 %
- Public :
  - → Gouvernement du Canada : 93,5 %
  - → Autre : 6,5 %

Invasion de l'Ukraine par la Russie

Cette année, le CST a continué à tirer parti de son mandat en matière de renseignement étranger pour appuyer la résistance de l'Ukraine à son invasion injustifiable par la Russie, toujours en cours.

Par exemple, le CST a identifié des entités financières et industrielles exploitées par le gouvernement russe pour soutenir sa capacité à financer la guerre en Ukraine en contournant les sanctions internationales. Le Canada et ses alliés ont utilisé cette information pour exercer des pressions sur les entités internationales qui continuent à faire affaire avec la Russie.

En outre, le CST a produit à l'intention du gouvernement du Canada et de ses alliés du renseignement exploitable pour :

- détecter et décourager les activités malveillantes de la Russie envers l'Ukraine et d'autres alliés;
- comprendre les développements militaires, politiques et économiques liés à l'invasion;
- surveiller les campagnes de désinformation de la Russie;
- surveiller les cyberactivités malveillantes de la Russie contre le Canada et ses alliés;
- aider à protéger le personnel du gouvernement canadien et le personnel militaire allié qui se trouve en Ukraine;
- soutenir l'opération Unifier, la mission de formation menée par les FAC à l'appui de l'Ukraine.

Parallèlement, le Centre pour la cybersécurité a continué d'offrir de l'assistance à l'Ukraine et à la Lettonie en matière de cybersécurité.

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

Le Centre pour la cybersécurité a engagé des efforts pour soutenir l'Ukraine et la Lettonie au moyen de la cybersécurité depuis 2022, lorsque la ministre de la Défense nationale a désigné les cybersystèmes de ces pays comme d'importance pour le Canada.

Au cours de l'année écoulée, le Centre pour la cybersécurité a continué de partager de l'information avec la Lettonie et l'Ukraine au sujet des cybermenaces exercées contre leurs infrastructures essentielles. Cette information aborde notamment :

- les vulnérabilités en matière de cybersécurité dans les réseaux essentiels;
- les aspects techniques des menaces;
- l'accès non autorisé au réseau par des auteures et auteurs de menace malveillants.

Des équipes du Centre pour la cybersécurité ont été déployées en Lettonie six fois au total, dans le cadre d'activités concertées avec les FAC (opération Reassurance) et avec l'agence de cybersécurité de la Lettonie, CERT.LV. Les deux déploiements effectués cette année ont eu lieu à l'automne 2023 et en début d'année 2024, chacun d'eux s'étant étalé sur trois semaines environ.

Les équipes ont conduit des opérations de détection des cybermenaces couronnées de succès sur les réseaux du gouvernement letton et ceux des organisations du secteur des infrastructures essentielles de la Lettonie, et ont partagé de l'information essentielle en matière de cyberdéfense pour aider à lutter contre les auteures et auteurs de menace dotés de moyens sophistiqués.

> **« Les activités de cybermenace représentent une menace réelle et croissante contre les processus démocratiques du Canada. »**
>
> - Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023

Activités d'États hostiles et ingérence étrangère

Les activités d'États hostiles et l'ingérence étrangère revêtent un grand nombre de formes et font souvent intervenir des cyberactivités. On peut citer, à titre d'exemple, les tentatives dissimulées pour influencer le processus démocratique, la désinformation en ligne et les activités de cybermenace et d'espionnage économique parrainées par des États.

Le CST et le Centre pour la cybersécurité jouent des rôles clés lorsqu'il s'agit de surveiller et de contrer les tentatives étrangères visant à s'ingérer dans les affaires du Canada. Consultez la section Responsabilisation du présent rapport pour vous renseigner sur les Examens en matière d'ingérence étrangère.

Cybermenaces contre le processus démocratique du Canada

Les cybermenaces visant les élections connaissent une hausse à l'échelle mondiale. La désinformation en ligne est maintenant omniprésente dans les élections à travers le monde, et l'IA générative est de plus en plus utilisée pour influencer les élections.

Voilà certains des résultats clés du dernier rapport du CST sur le sujet intitulé Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023[20].

Publié en décembre 2023, le rapport prédit qu'il est plus probable que des activités de cybermenace surviennent lors de la prochaine élection fédérale canadienne que cela n'a été le cas par le passé. Ceci comprend l'utilisation « très probable » de contenu généré par l'IA pour influencer les électrices et les électeurs.

Le rapport révèle que les cybercampagnes d'influence, comme les opérations de piratage et de divulgation, sont sept fois plus fréquentes que les tentatives qui ciblent les infrastructures électorales. Il mentionne également que les auteures et auteurs de cybermenace sont de plus en plus habiles à dissimuler leurs traces.

On y souligne aussi qu'une recrudescence des tensions entre le Canada et un État hostile durant la période précédant des élections nationales aurait presque certainement pour effet d'inciter les auteures et auteurs de cybermenaces à cibler les processus démocratiques du Canada ou à perturber l'écosystème d'information en ligne du Canada. Le rapport nomme la République populaire de Chine (RPC) et la Russie comme les deux États les plus activement engagés dans des activités de cybermenace ciblant des élections, des institutions démocratiques, des représentantes et représentants de gouvernement, et des communautés de la diaspora dans le monde entier.

De plus, le rapporteur spécial indépendant sur l'ingérence étrangère, nommé en vue de vérifier l'ampleur et les répercussions de l'ingérence étrangère sur les processus électoraux au Canada, a publié en mai 2023 un rapport donnant des exemples de l'intensité des activités d'ingérence étrangère de la RPC au Canada.

Surveillance pour prévenir l'ingérence lors des élections partielles fédérales

En tant que membre du Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (GT MSRE), le CST a uni ses efforts à ceux du SCRS, de la GRC et d'Affaires mondiales Canada en vue de surveiller et de signaler les menaces à l'égard de six élections partielles fédérales ayant eu lieu cette année, ce qui constituait une première.

Le programme de renseignement électromagnétique étranger du CST a permis de surveiller les signes d'ingérence étrangère, y compris les tentatives pour affecter l'issue des élections partielles ou pour miner la confiance du public en l'intégrité du processus.

Pendant ce temps, le Centre pour la cybersécurité a aidé à assurer la cybersécurité lors des élections partielles, de la manière suivante :

- en surveillant les cyberactivités malveillantes ciblant Élections Canada;
- en renseignant les partis politiques sur les cybermenaces courantes et sur les pratiques exemplaires en matière de cybersécurité;
- en mettant en service, pour le signalement des cyberincidents, une ligne d'assistance disponible en tout temps à l'intention des partis et des candidates et candidats.

Pendant la période des élections partielles, le Groupe de travail MSRE a fourni des rapports de situation hebdomadaires au Comité des sous-ministres sur les interventions en matière de renseignement. À la suite des élections partielles, le Groupe de travail a partagé ses résultats avec le public dans des rapports non classifiés[21]. Comme indiqué dans ces rapports, le Groupe de travail n'a décelé aucune tentative d'ingérence étrangère visant les élections partielles ni aucun cyberincident qui suggérerait que des actrices et acteurs étatiques étrangers ciblaient expressément Élections Canada durant la période des élections partielles.

Le CST continue de collaborer étroitement avec ses partenaires en vue de recueillir et de diffuser le renseignement étranger requis pour effectuer le suivi des menaces et réagir adéquatement devant leur intensification en provenance d'auteures et auteurs de menaces extrêmement compétents et motivés.

Soutien à l'intégrité des élections provinciales et territoriales

L'ingérence étrangère constitue un problème pour tous les ordres de gouvernement[22]. Cette année, le Centre pour la cybersécurité a fait équipe avec les organismes de gestion des élections (OGE) afin de contrer les cybermenaces étrangères visant les élections. Par exemple, le Centre pour la cybersécurité a mené les activités suivantes :

- rétablissement d'un appel trimestriel collectif avec la communauté d'intérêts des OGE provinciaux et territoriaux;
- élaboration de directives sur les cybermenaces visant les élections;
- soutien aux initiatives provinciales et territoriales comme le groupe de travail sur l'intégrité des élections d'Elections BC;
- soutien à la formation des membres du personnel électoral canadien;
- soutien aux OGE concernant l'utilisation sécuritaire des modes de scrutin électroniques et des systèmes de registre électronique du scrutin;
- participation aux séances d'information données par des OGE à l'intention de partis politiques.

Désinformation en ligne

Des actrices et acteurs étatiques exploitent la désinformation en ligne comme outil d'ingérence étrangère. La désinformation incite également les gens à prendre des décisions qui peuvent être contraires à leurs intérêts, et par exemple à investir dans des fraudes liées à la cryptomonnaie ou à de faux produits de santé.

Les percées en IA font en sorte que des auteures et auteurs de menace peuvent maintenant créer et diffuser facilement du contenu trompeur, y compris des vidéos hypertruquées qui sont de plus en plus difficiles à identifier.

> **« La désinformation est devenue omniprésente durant les élections nationales. »**
>
> - Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023

Le CST et le Centre pour la cybersécurité ont attiré l'attention sur la menace que constitue la désinformation dans deux rapports emblématiques récents :

- Évaluation des cybermenaces nationales 2023-2024[23] (Octobre 2022)
- Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023[24]

Campagne de sensibilisation sur la désinformation en ligne

Cette année, le CST a lancé la phase 2 d'une campagne publicitaire menée pour le compte du gouvernement du Canada en vue de sensibiliser la population à la désinformation en ligne. La campagne encourage les Canadiennes et les Canadiens à se montrer vigilants à l'égard du contenu affiché en ligne, et utilise le slogan « Si ça vous fait hausser les sourcils, ça devrait soulever des questions ».

- Vidéo de la campagne de sensibilisation sur la désinformation « Si ça vous fait hausser les sourcils, ça devrait soulever des questions »[25]

Les vidéos et publicités en ligne de la campagne donnaient accès à une page Web intitulée Désinformation en ligne[26] offrant des renseignements sur les torts que peut causer la désinformation, et des astuces et des outils pour la reconnaître.

La campagne s'est déroulée de janvier à mars 2024 sur diverses plates-formes numériques y compris X (Twitter), TikTok et YouTube. Les publicités ont été affichées plus de 159 millions de fois et ont généré 12 millions de vues sur les vidéos et près de 400 000 visites sur la page Web.

Cyberactivités parrainées par des États

Le Centre pour la cybersécurité estime que « les cyberprogrammes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord sont les plus grandes cybermenaces stratégiques ciblant le Canada »[27].

Cette année, le CST et le Centre pour la cybersécurité ont continué de partager de l'information au sujet de ces menaces en recourant à une combinaison de communications publiques et de mises en garde envoyées directement aux partenaires du Centre pour la cybersécurité.

Activités de cybermenace parrainées par la République populaire de Chine

En mai 2023, le CST et le Centre pour la cybersécurité ont collaboré avec leurs partenaires de la collectivité des cinq pour lancer une mise en garde au sujet d'un ensemble d'activités de cybermenace associées à la République populaire de Chine[28] (RPC). Le bulletin publié conjointement mettait en lumière une technique appelée « attaque hors sol » difficile à détecter du fait qu'elle ressemble fortement à une cyberactivité normale. Bien que l'activité décelée ait majoritairement visé des infrastructures essentielles aux États-Unis, la même technique pourrait être employée contre toute cible à l'échelle mondiale.

En février 2024, le Centre pour la cybersécurité a appuyé la publication d'un Bulletin conjoint sur l'auteur de menace Volt Typhoon parrainé par la RPC[29] qui cible les réseaux d'infrastructures essentielles des États-Unis. Ce bulletin a été suivi, en mars, par des conseils à l'intention des cadres supérieures et supérieurs et des chefs d'organisations liées aux infrastructures essentielles[30] en rapport avec la même cyberactivité de la RPC.

Le bulletin conjoint établissait que l'activité en question visait à permettre un prépositionnement en vue d'attaques perturbatrices ou destructrices contre les infrastructures essentielles américaines en cas de crise majeure ou de conflit avec les États-Unis. Toute perturbation des infrastructures essentielles des États-Unis aurait vraisemblablement des répercussions sur le Canada, étant donné que nos infrastructures sont étroitement liées.

Les deux bulletins contenaient des conseils techniques sur la manière de reconnaître les méthodes employées et de s'en protéger.

Activités de cybermenace menées par des auteures et auteurs de menace alliés à la Russie

Le 12 avril 2023, le Centre pour la cybersécurité a publié un cyberflash pour mettre en garde nos partenaires des infrastructures essentielles au sujet d'une augmentation considérable des activités de cybermenace menées par des auteures et auteurs de menace alliés à la Russie. Au nombre de ces activités figuraient des tentatives pour compromettre les technologies opérationnelles (les systèmes utilisés pour contrôler l'équipement physique). En faisaient aussi partie des attaques par déni de service distribué (DDoS) contre des sites Web gouvernementaux et commerciaux.

Le 13 avril 2023, la ministre de la Défense nationale a renforcé le message du cyberflash en diffusant une déclaration publique au sujet des activités de cybermenaces conduites par des auteures et auteurs de menace alliés à la Russie[31]. La déclaration exhortait les organisations du secteur des infrastructures essentielles à protéger leurs systèmes, et fournissait de l'information sur les ressources du Centre pour la cybersécurité à consulter à cette fin.

En septembre 2023, le CST a publié une mise en garde additionnelle à l'intention de la collectivité canadienne de la cybersécurité[32] en prévision d'une visite officielle du président ukrainien, Volodymyr Zelenskyy.

En février 2024, le CST a de nouveau exhorté les organisations canadiennes à être vigilantes à l'occasion du deuxième anniversaire de l'invasion massive de l'Ukraine par la Russie[33].

De plus, le CST et le Centre pour la cybersécurité ont appuyé les bulletins de cybersécurité conjoints de la collectivité des cinq mettant en garde contre :

- des campagnes sophistiquées d'attaques par harponnage d'origine russe[34];
- le fait que des auteures et auteurs de menace russes adaptaient leurs tactiques pour accéder à l'infrastructure infonuagique[35].

Sécurité économique

Le CST travaille conjointement avec ses partenaires fédéraux pour mettre l'économie canadienne à l'abri des activités d'États hostiles et de l'ingérence étrangère, y compris des menaces à l'égard de la sécurité nationale, de l'espionnage économique et des risques liés à la chaîne d'approvisionnement. Les programmes de sécurité économique tirent parti des volets du mandat du CST liés au renseignement étranger et à la cybersécurité, et de son expertise en matière de technologies de pointe.

Sécurité relative à la recherche

En janvier 2024, le gouvernement du Canada a mis en place de nouvelles mesures pour protéger la recherche en technologies sensibles menée par le Canada. La Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes[36] offre des conseils en vue d'aider les chercheuses et chercheurs canadiens à éviter les liens avec des organisations qui posent un risque élevé pour la sécurité nationale du Canada. Des exemples de telles organisations comprendraient des instituts possédant des liens avec des entités gouvernementales ou militaires en Russie, en Chine et en Iran. Le CST a contribué à établir la liste des domaines de recherche en technologies sensibles et la liste des organisations suscitant des préoccupations.

Intégrité de la chaîne d'approvisionnement

Le CST conduit des évaluations des risques pour des clients du gouvernement du Canada cherchant à se procurer de l'équipement de TI. Ces évaluations prennent en compte un grand nombre de facteurs, dont les vulnérabilités techniques des produits, les pratiques d'affaires, la cybermaturité et la question de la propriété étrangère relativement aux fournisseurs. Le CST travaille de plus en plus, concernant les risques liés à la chaîne d'approvisionnement, avec des partenaires qui ne font pas partie du gouvernement fédéral et sont rattachés aux provinces ainsi qu'au secteur privé. Cette année, le CST a mené 1 291 évaluations des risques liés à la chaîne d'approvisionnement.

Protection de l'infrastructure des télécommunications du Canada

Les Canadiennes et les Canadiens dépendent de la connectivité dans leur vie quotidienne. Cette année, le CST a continué de collaborer avec les opérateurs de réseau mobile (ORM) en vue d'améliorer la sécurité et la résilience des réseaux 4G et 5G, en veillant à :

- identifier et atténuer les risques en matière de sécurité et les risques liés à la chaîne d'approvisionnement;
- partager l'information concernant les menaces et les pratiques exemplaires.

Par exemple, des auteures et auteurs de menace comme des auteures et auteurs de menace étatiques et des cybercriminelles et cybercriminels peuvent exploiter la signalisation des réseaux mobiles pour géolocaliser des utilisatrices et utilisateurs de téléphones cellulaires. Le CST a mis à profit le renseignement sur les menaces visant l'industrie pour alerter les ORM à la présence de ce type d'activités de menace sur leurs réseaux. Il a également fourni aux ORM des conseils techniques sur la façon d'optimiser leurs défenses réseau en vue de contrer cette menace précise.

Normes internationales

Les auteures et auteurs de menace peuvent avoir une influence sur la sécurité des produits dans le cadre du processus d'élaboration de normes, avant même que les produits soient conçus. Le CST collabore avec ses partenaires fédéraux et internationaux, dans cet espace de plus en plus contesté, pour faire en sorte que les normes en matière de TI et de cryptographie demeurent rigoureuses.

Cette année, le CST a continué de certifier des produits de TI commerciaux dans le cadre du Programme des Critères communs (pour ce qui touche à la cybersécurité) et du Programme de validation des modules cryptographiques (concernant l'intégrité cryptographique). Le CST collabore par ailleurs avec ses partenaires fédéraux et internationaux en vue de mettre au point des normes internationales en matière d'IA.

Examens de la sécurité nationale

Cette année, le CST a continué d'effectuer des examens de la sécurité nationale à l'appui de ce qui suit :

- *Loi sur Investissement Canada*;
- *Loi sur les licences d'exportation et d'importation*;
- Lignes directrices sur la sécurité nationale dans le cadre de partenariats liés à la recherche.

Antiterrorisme

Le CST a continué de fournir du renseignement étranger de grande valeur pour protéger les Canadiennes et les Canadiens, de même que les intérêts du Canada, contre le terrorisme et l'extrémisme violent, dont :

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

Des exemples d'EVCR comprennent Al-Quaïda et les nombreux groupes affiliés à Daech (groupe État islamique/ISIS), tandis que les menaces liées à l'EVCI englobent une vaste gamme d'idéologies extrémistes xénophobes, anti-autorité, fondées sur l'identité de genre et les récriminations personnelles. Le CST concentre ses efforts sur la mise à contribution d'outils et de techniques virtuelles pour identifier les activités d'extrémistes étrangères et étrangers constituant une menace pour le Canada ou pour les Canadiennes et les Canadiens.

Cette année, le CST a continué de collaborer avec les ministères et organismes du gouvernement du Canada en vue d'identifier et de recueillir du renseignement sur les extrémistes étrangères et étrangers qui s'efforcent de provoquer et de favoriser, au Canada, des attaques de type « loup solitaire » ou des attaques par de petites cellules. À titre d'exemple, le Canada a travaillé avec le SCRS et la GRC en vue d'identifier des extrémistes étrangères et étrangers constituant une source de préoccupation, et de fournir de l'information cruciale sur leur recrutement, leur radicalisation et leurs activités de planification d'attaques.

Le CST a également cherché à recueillir du renseignement étranger sur les menaces extrémistes étrangères contre des Canadiennes et des Canadiens ou contre les intérêts du Canada à l'étranger. L'éventail des efforts engagés par le CST à ce chef ont pu aller de l'appui du soutien aux victimes d'enlèvement à la couverture des menaces exercées contre des événements publics ou contre des ambassades et des missions du Canada, en passant par la détection de menaces extrémistes envers des nations alliées. À de multiples occasions, le renseignement fourni par le CST a aidé ses partenaires internationaux à atténuer et à contrecarrer les menaces d'extrémistes violentes et violents, contribuant ainsi potentiellement à épargner des vies.

En plus de permettre de perturber concrètement des activités d'extrémistes étrangères et étrangers, le renseignement provenant du CST a servi à étayer nos cyberopérations actives contre ces mêmes extrémistes et organisations violentes (voir la section Contrer l'extrémisme violent).

L'Arctique

La préservation de la souveraineté canadienne dans l'Arctique constitue une priorité du gouvernement du Canada et fait appel aux volets du mandat du CST liés à la fois à la cybersécurité et au renseignement étranger.

Scruter l'horizon

L'Arctique est une région riche en ressources naturelles et importante sur le plan stratégique. Les changements climatiques et les progrès technologiques facilitent l'accès à cette région. Comme l'indique le Cadre stratégique pour l'Arctique et le Nord, « [cette situation] pos[e] des défis en matière de sécurité auxquels le Canada doit être prêt à répondre »[37].

Le CST travaille en concertation avec ses partenaires nationaux et ses alliés internationaux afin de recueillir du renseignement étranger sur les activités menées dans l'Arctique par des auteures et auteurs de menace étrangers, et de comprendre les objectifs à long terme de ces derniers. Il faut pour cela produire des rapports de renseignement étranger sur les intentions politiques des États étrangers, leurs capacités militaires, leurs progrès technologiques, leurs intérêts économiques et les activités de recherche qui ont lieu dans la région.

Cette année, le CST a partagé 132 rapports de renseignement sur la sécurité dans l'Arctique avec 17 ministères du gouvernement canadien ainsi qu'avec les alliés internationaux du Canada.

Partenaires nationaux

Le CST poursuit sa collaboration avec les FAC afin de s'assurer que le gouvernement du Canada dispose du renseignement dont il a besoin pour défendre la sécurité et la souveraineté du Canada dans l'Arctique. En font partie la surveillance aérienne et maritime des navires et d'autres éléments dans la région.

Aux côtés du Bureau du Conseil privé, le CST continue de coprésider le Groupe de coordination du renseignement sur l'Arctique, qui coordonne les activités liées à la sécurité dans l'Arctique pour le gouvernement du Canada.

Alliés internationaux

Le CST a continué de participer à deux forums multinationaux de renseignement pour coordonner ses activités avec celles d'alliés partageant les mêmes valeurs en ce qui a trait à la sécurité dans l'Arctique. L'un de ces forums, présidé par le CST, est expressément consacré au renseignement électromagnétique et s'intéresse aux deux régions polaires. L'autre forum concentre le renseignement de toutes les sources et porte exclusivement sur l'Arctique.

Le CST a dirigé deux conférences internationales à l'appui de ces forums au cours de l'année écoulée. Ces événements en présentiel ont permis de définir les questions clés pour la collecte de renseignement, de s'entendre sur les priorités communes et de coordonner les efforts liés à l'Arctique.

Sécuriser le Nord

Une série de cyberincidents ciblant les institutions nordiques ont mis en relief l'importance stratégique cruciale de la cybersécurité dans le Nord.

En novembre 2022, le Centre pour la cybersécurité a effectué en urgence le déploiement de capteurs en réponse à un cyberincident touchant le gouvernement des Territoires du Nord-Ouest.

À la suite de cet incident, le Centre pour la cybersécurité a identifié deux priorités urgentes en vue de sécuriser le Nord :

- fournir aux gouvernements territoriaux les capacités voulues pour sécuriser les communications, avec l'encadrement du Centre pour la cybersécurité;
- déployer des capteurs sur les biens de TI des gouvernements territoriaux pour exercer une surveillance permanente sur les cyberactivités malveillantes.

Dès novembre 2023, le Centre pour la cybersécurité avait établi des liaisons sécurisées avec les trois territoires, et en janvier 2024, le Centre pour la cybersécurité commençait à déployer les capteurs. C'est dans ce contexte que le Centre pour la cybersécurité a déployé pour la première fois des capteurs auprès d'une organisation non fédérale de manière proactive, plutôt qu'à la suite d'un cyberincident.

Pendant toute l'année, le Centre pour la cybersécurité a continué de travailler avec ses partenaires du Nord, pour :

- améliorer les processus d'échange d'information sur les menaces;
- fournir des notifications de vulnérabilité améliorées;
- aider à gérer les risques liés à la chaîne d'approvisionnement.

Il a fallu pour cela visiter chaque territoire pour y rencontrer les fournisseurs d'infrastructures essentielles et d'autres systèmes d'importance, dont les aéroports, les fournisseurs d'énergie et les universités.

Chronologie des cyberincidents dans le Nord

Novembre 2022

Un cyberincident touche le gouvernement des Territoires du Nord-Ouest.

Janvier 2023

Des systèmes de TI sont compromis à la Qulliq Energy Corporation, dans le Nunavut.

Juillet 2023

Une base de données du gouvernement Nunatsiavut est piratée.

Septembre 2023

On enregistre une attaque par DDoS sur des sites gouvernementaux d'un bout à l'autre du Canada, y compris au Nunavut et au Yukon.

La stratégie du Canada pour l'Indo-Pacifique

En novembre 2022, le gouvernement du Canada a publié sa stratégie pour l'Indo-Pacifique, destinée à orienter les politiques et les initiatives du Canada dans cette région pendant plusieurs décennies.

La stratégie vise à améliorer les capacités que possède le Canada en matière de renseignement et de cybersécurité, afin de lui permettre de protéger les Canadiennes et les Canadiens contre des menaces comme :

- l'ingérence étrangère;
- les cybermenaces;
- les activités hostiles d'auteures et d'auteurs de menace étatiques;
- les menaces d'ordre économique pour la sécurité nationale.

La stratégie vise également à renforcer les partenariats de sécurité et les capacités en matière de cybersécurité dans la région.

Cette année, le CST a appuyé la stratégie du Canada pour l'Indo-Pacifique en donnant suite aux demandes de renseignement croissantes visant la région, et en collaborant avec les partenaires régionaux.

La République populaire de Chine et la stabilité de la région indo-pacifique

La RPC demeure un auteur de menace étatique doté de moyens sophistiqués et d'un appareil de sécurité et de renseignement efficace et de grande portée.

La RPC a manifesté un ensemble de comportements qui menacent la sécurité des Canadiennes et des Canadiens. Certains exemples vont d'interceptions non sécuritaires d'opérations déployées par les FAC dans les eaux internationales à l'appui de la Stratégie du Canada pour l'Indo-Pacifique[38], à la menace réelle et persistante des cyberactivités menées par la RPC contre le Canada et ses alliés[39]. Le Canada continue de dénoncer ce comportement en prenant note du scénario de plus en plus inquiétant des actes d'intimidation menés par la RPC dans des régions comme la mer de Chine méridionale[40].

Le CST travaille en étroite collaboration avec ses partenaires nationaux et internationaux en matière de sécurité et de renseignement ainsi qu'avec un ensemble de fournisseurs de renseignement, pour obtenir l'information dont le Canada a besoin pour comprendre, décourager et contrer les activités malveillantes du gouvernement de la RPC et de ses services de renseignement. La RPC continue de recourir à une vaste gamme de méthodes déclarées, secrètes et clandestines de promotion de ses intérêts, lesquelles méthodes ont des répercussions considérables pour le Canada et les États de l'Indo-Pacifique, et constituent une menace constante pour l'ordre international fondé sur des règles alors que la RPC tente de réinterpréter celles-ci à son avantage.

En réaction à la concurrence stratégique croissante dans la région, le CST a accru sa capacité de production de rapports de renseignement étranger à l'appui du gouvernement du Canada et de ses alliés. Les rapports produits par le CST cette année ont fourni des perspectives propres à permettre de :

- déceler et atténuer les cybermenaces de la RPC visant le Canada et ses alliés;
- surveiller les campagnes d'influence qui font la promotion des versions des faits véhiculées par le Parti communiste chinois et qui sapent la confiance à l'égard des institutions démocratiques;
- lever le voile sur des activités délibérément néfastes pour la prospérité et les intérêts économiques canadiens;
- fournir des informations sur les tendances et les événements qui constituent une menace pour la stabilité dans la région.

Appui à la cybersécurité dans la région indo-pacifique

Le Centre pour la cybersécurité a échangé de manière régulière de l'information sur les cybermenaces avec ses partenaires de la région indo-pacifique. Cette information a aidé à améliorer les directives que fournit le Centre pour la cybersécurité aux organisations responsables d'infrastructures essentielles et au gouvernement du Canada. Le Centre pour la cybersécurité continue de raffermir ses liens avec ses partenaires régionaux en participant à des événements comme :

- la Semaine internationale de la cybersécurité de Singapour;
- une conférence sur la cybersécurité organisée par l'ambassade du Canada aux Philippines;
- la rencontre annuelle du Pacific Cyber Security Operational Network.

Cyberopérations étrangères

La *Loi sur le CST* autorise ce dernier à réaliser deux différents types de cyberopérations : des cyberopérations actives, et des cyberopérations défensives. Les deux types d'opérations comportent la prise de mesures dans le cyberespace en vue de nuire aux menaces étrangères visant le Canada.

Des cyberopérations défensives (COD) peuvent être employées pour aider à protéger les systèmes d'importance et les institutions fédérales à l'occasion de cyberincidents d'envergure, lorsque les mesures de cybersécurité seules ne suffisent pas à la tâche. Des cyberopérations actives (COA) peuvent servir, de manière proactive, à perturber des menaces étrangères visant les intérêts du Canada en matière d'affaires internationales, de défense ou de sécurité.

Le CST conduit souvent des cyberopérations étrangères de concert avec ses partenaires de la collectivité des cinq, en vue de l'atteinte d'objectifs communs. Il mène également des cyberopérations conjointes avec les FAC à l'appui des objectifs liés à leur mission.

Agir en cyberpuissance responsable

La *Loi sur le CST* établit clairement certaines limites que les cyberopérations étrangères du CST ne peuvent franchir. Il est interdit au CST d'utiliser des cyberopérations pour « entraver, détourner ou contrecarrer le cours de la justice ou de la démocratie ». De la même manière, les cyberopérations ne peuvent causer des lésions corporelles à une personne physique ou la mort de celle-ci, et ne peuvent être utilisées contre des cibles étrangères que dans la mesure où « ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité ».

En vertu de la *Loi sur le CST*, les cyberopérations étrangères doivent être autorisées par la ou le ministre de la Défense nationale. En outre, la ou le ministre des Affaires étrangères doit approuver les cyberopérations actives ou en avoir fait la demande, et faire l'objet de consultations avant la mise en place de cyberopérations défensives.

Le CST a un cadre de gouvernance bien établi pour le guider en matière de cyberopérations étrangères et s'assurer qu'elles sont conformes à la *Loi sur le CST* et aux autorisations ministérielles émises. Ceci exige des consultations étroites avec Affaires mondiales Canada (AMC) afin d'évaluer les répercussions des cyberopérations envisagées sur le plan de la politique étrangère et sur le plan juridique. Ces évaluations tiennent compte à la fois des lois canadiennes et du droit international applicable dans le cyberespace[41].

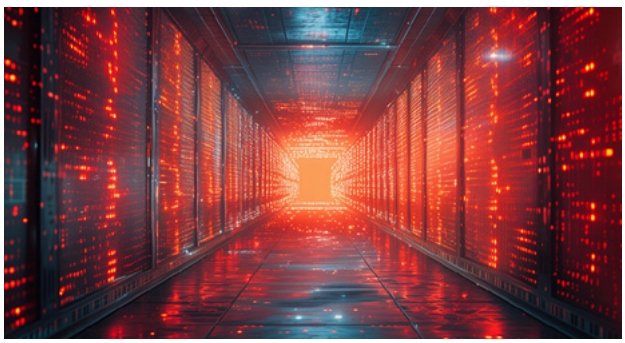
Contrer les activités d'États hostiles

Cette année, le CST a continué de faire appel à ses capacités de COA pour lutter contre les activités hostiles d'actrices et acteurs étatiques étrangers. Ces opérations ont perturbé des menaces à l'étranger, avant même qu'elles puissent affecter la sécurité des Canadiennes et des Canadiens. Ces menaces comprennent :

- de l'ingérence étrangère et de l'influence néfaste ciblant le Canada et ses alliés;
- des opérations de désinformation;
- des activités de cybermenace malveillantes;
- de l'espionnage.

Contrer la cybercriminalité

Le CST mène une campagne permanente pour perturber les activités des groupes cybercriminels. Consultez la section Cybercriminalité pour obtenir des précisions sur l'usage par le CST des cyberopérations étrangères pour lutter contre la cybercriminalité.



Contrer l'extrémisme violent

Le CST a continué de mener des cyberopérations actives pour lutter contre la diffusion en ligne de contenu extrémiste violent. Cette année, le CST a utilisé les COA pour contrer les initiatives de groupes étrangers impliqués dans des activités relevant tant de l'extrémisme violent à caractère idéologique que de l'extrémisme violent à caractère religieux.

Ces extrémistes ont recours à des vidéos et à des images empreintes de violence pour diffuser leurs idéologies et pour recruter et radicaliser leurs adeptes. En nuisant à leurs activités de propagande en ligne, le CST porte atteinte à leur crédibilité et à leur capacité d'influencer d'autres personnes en ligne.

Raisons qui nous empêchent d'en dire davantage

Le CST cherche à faire preuve de la plus grande transparence possible tout en protégeant l'information classifiée. En règle générale, le CST ne peut diffuser aucune information susceptible de :

- permettre à la cible d'une cyberopération d'identifier le CST comme source de la perturbation;
- donner de l'information sur les techniques ou les capacités employées par le CST;
- révéler l'étendue de la capacité du CST à conduire des cyberopérations.

La diffusion de toute information de cet ordre pourrait occasionner un préjudice grave aux intérêts nationaux du Canada, et justifie que nous ne puissions fournir de détails sur les cibles précises visées, les procédés utilisés ou le moment où les activités ont eu lieu. Nous ne privilégions pas le secret pour le plaisir de le faire. Nous préservons ces capacités pour la prochaine occurrence où nous en aurons besoin pour défendre les Canadiennes et les Canadiens.

Cybercriminalité

Les organisations canadiennes continuent d'être la cible de cybercrimes, qui gagnent en audace et en sophistication. En effet, une étude de 2023 suggère qu'une organisation canadienne sur trois a été touchée par les rançongiciels, dont le montant moyen de la rançon est de plus d'un million de dollars canadiens[42].

Le Centre pour la cybersécurité désigne les rançongiciels comme étant « la forme la plus perturbatrice de cybercriminalité à laquelle est confronté le Canada » en raison de leurs potentielles répercussions sur les services essentiels dont dépendent les Canadiennes et les Canadiens[43]. Des exemples très médiatisés en sont la preuve, comme l'attaque par rançongiciel contre le système de santé de Terre-Neuve-et-Labrador qui a touché plus d'une personne sur dix dans la province, ainsi que les activités ayant ciblé cinq hôpitaux ontariens en 2023.

La lutte contre la cybercriminalité est une des principales priorités du CST et elle touche chacun des volets de son mandat.

Cyberopérations étrangères pour lutter contre les cybercrimes

En 2023, le CST a utilisé ses capacités de COD pour la première fois contre un groupe étranger à l'origine de rançongiciels qui ciblait un grand nombre d'organisations du secteur canadien des infrastructures essentielles. Tandis que le Centre pour la cybersécurité prenait des mesures pour atténuer la compromission au Canada, l'équipe responsable des cyberopérations étrangères s'activait dans le cyberespace. La COD a visé les serveurs à l'étranger des cybercriminelles et cybercriminels, de sorte à diminuer l'efficacité et la rentabilité de leurs activités. Surtout, les actions du CST ont permis de réduire les conséquences de l'incident sur les victimes.

À la suite de cette première COD, le CST a continué de mener d'autres COD au cours de l'année. Il a notamment mené une opération dont l'objectif était de contrer un groupe de cybercriminelles et cybercriminels qui ciblaient des institutions fédérales canadiennes et des organisations du secteur des infrastructures essentielles au moyen d'attaques par DDoS.

De plus, le CST a continué sa campagne actuelle de cyberopérations actives en vue de perturber les activités de groupes étrangers à l'origine de rançongiciels. En collaboration avec ses partenaires de la collectivité des cinq, le CST a entrepris des COA en vue de décourager les activités des groupes étrangers à l'origine de rançongiciels et de dégrader les outils virtuels qu'ils utilisent. Ces opérations en continu font en sorte qu'il est plus difficile pour les cybercriminelles et cybercriminels de lancer des attaques par rançongiciel contre les organisations canadiennes et de tirer profit du vol de données canadiennes. Le CST fixe la priorité de ses opérations en fonction des groupes à l'origine de rançongiciels qui représentent la plus grande menace pour le Canada selon les évaluations du Centre pour la cybersécurité.

Incidence durable

Lors de la dernière année financière, le CST a dirigé une campagne multinationale de cyberopérations étrangères contre un groupe étranger à l'origine de rançongiciels. Le groupe avait été lié à des cyberincidents qui avaient touché les systèmes de santé et d'autres secteurs essentiels au Canada et dans les pays alliés. Le CST a dirigé cette opération en collaboration avec ses partenaires de la collectivité des cinq afin de perturber les infrastructures techniques utilisées par le groupe. Il s'agissait de la première opération multinationale que dirigeait le CST. À la suite de l'opération, il semble que le groupe se soit séparé et ait cessé ses activités. À ce jour, le CST n'a pas constaté que le groupe se soit reconstitué ou qu'il ait effectué d'autres activités de menace au Canada.

Prix d'excellence de la fonction publique

En 2023, l'équipe chargée de la lutte contre la cybercriminalité du CST s'est vu décerner un prix d'équipe dans le cadre des Prix d'excellence de la fonction publique 2022 en récompense de ses efforts visant à minimiser les effets de la cybercriminalité sur les organisations canadiennes. Ce prix reconnaît les innovations et les contributions exceptionnelles de l'équipe dans la lutte mondiale contre la cybercriminalité.

> **« Grâce à ses innovations et à ses contributions exceptionnelles, l'équipe a démontré que le Canada s'investissait pleinement dans la lutte mondiale contre la cybercriminalité. »**
>
> - Prix d'excellence de la fonction publique 2022

Notifications de signes avant-coureurs d'une attaque par rançongiciel

En mai 2023, le Centre pour la cybersécurité a lancé une nouvelle initiative pilote dans la lutte contre les rançongiciels. Les notifications de signes avant-coureurs d'une attaque par rançongiciel avertissent rapidement les victimes potentielles à l'étape d'accès initial d'un incident lié à un rançongiciel. Elles permettent aux responsables de la défense des réseaux de localiser précisément la compromission et de la contrecarrer avant que ne survienne le chiffrement ou le vol des données.

Les notifications de signes avant-coureurs d'une attaque par rançongiciel se fondent sur trois principales sources d'information :

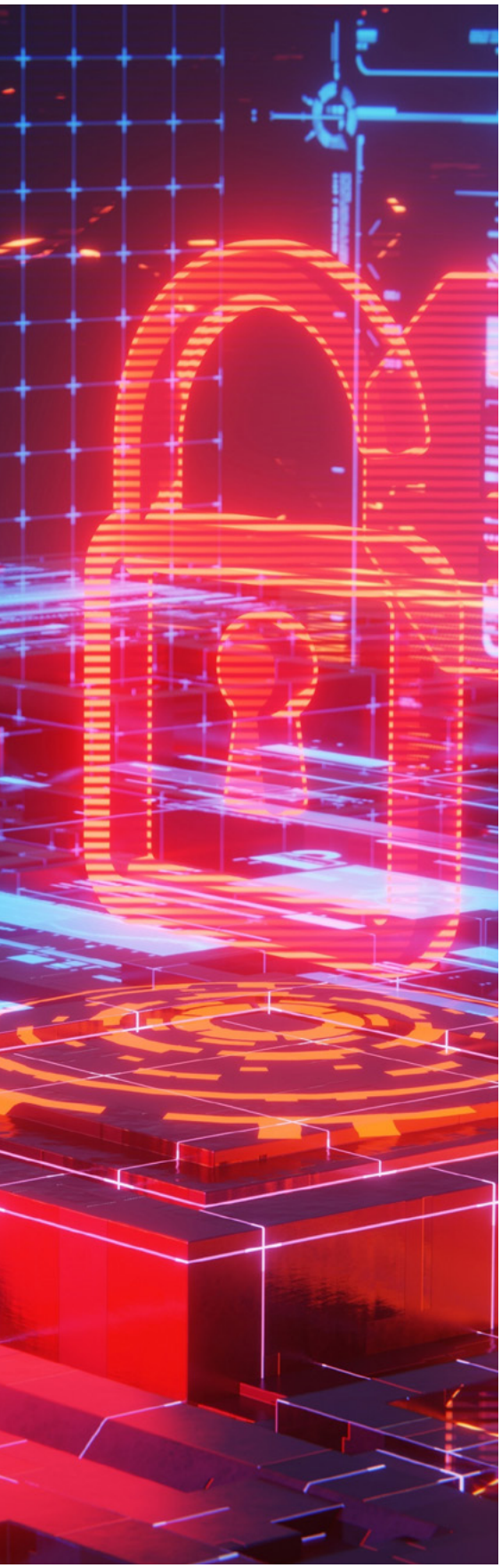
- les recherches du Centre pour la cybersécurité sur les comportements des maliciels et des infrastructures connexes;
- la collaboration avec les partenaires de confiance de l'industrie;
- la collaboration avec le Joint Ransomware Task Force, dirigée par les États-Unis.

Depuis le lancement de l'initiative pilote, le Centre pour la cybersécurité a envoyé des notifications de signes avant-coureurs d'une attaque par rançongiciel à plus de 250 organisations canadiennes. Les cibles se trouvaient à tous les échelons des gouvernements et dans des secteurs clés, comme le secteur manufacturier et les secteurs de la santé, de l'énergie, des finances et de l'éducation.

Le Centre pour la cybersécurité a également travaillé avec 10 de ses partenaires internationaux, y compris la Cybersecurity and Infrastructure Security Agency (CISA), afin d'envoyer de telles notifications à des organisations à l'extérieur du Canada.

Bien qu'elles soient utiles dans la lutte contre les rançongiciels, ces notifications ne font toutefois pas des miracles. Les rançongiciels demeurent une menace persistante et omniprésente. Pendant que les auteures et auteurs de menace continueront d'adapter leurs tactiques, le Centre pour la cybersécurité continuera d'entretenir des partenariats avec des organisations canadiennes et internationales, dans le but d'atténuer les répercussions des rançongiciels et d'accroître la résilience des cybersystèmes. Communiquez avec le Centre pour la cybersécurité[44] pour obtenir des conseils sur la manière de renforcer vos défenses.

Notifications de signes avant-coureurs d'une attaque par rançongiciel de 2023 à 2024



Publications en lien avec la cybercriminalité

En août 2023, le Centre pour la cybersécurité a publié une évaluation intitulée Évaluation des menaces de base : Cybercriminalité[45]. Le rapport détaille l'évaluation de la cybercriminalité et évalue les répercussions actuelles sur le Canada.

Le rapport soutient que « [l]es cybercriminelles et cybercriminels […] continueront presque certainement de cibler les organisations attrayantes dans les secteurs des infrastructures essentielles au Canada et partout dans le monde » et que la Russie et l'Iran agissent comme des « havres pour la cybercriminalité ». Le rapport montre qu'il ne ressort aucune tendance dans les organisations canadiennes qui ont été victimes de rançongiciel. Aucun secteur n'est à l'abri.

Cette année, le Centre pour la cybersécurité a produit des profils pour six groupes cybercriminels. Ces six profils ont été transmis aux responsables de la cyberdéfense. En outre, pour la toute première fois, deux profils ont été publiés en ligne.

- Profil : Rançongiciel ALPH/BlackCat[46]
- Profil : Rançongiciel CL0P / TA505[47]

Le Centre pour la cybersécurité a également contribué à deux bulletins de cybersécurité conjoints avec ses partenaires de la collectivité des cinq :

- Bulletin de cybersécurité conjoint sur le maliciel Truebot[48]
- Bulletin de cybersécurité sur le rançongiciel LockBit[49]

Le Centre pour la cybersécurité a continué de créer des produits de classement des menaces par rançongiciel et d'autres rapports classifiés visant à déterminer les occasions de dissuasion et de perturbation.

Sécurité des communications

La sécurité des communications (COMSEC pour *Communications Security*) est essentielle à la mission du CST. C'est la manière dont le CST protège les données et les communications les plus sensibles du gouvernement du Canada pour éviter que les adversaires en prennent connaissance ou les modifient.

Encore cette année, le CST a offert des solutions COMSEC au gouvernement du Canada et aux partenaires de l'industrie, notamment du matériel informatique sécurisé, des logiciels et des clés cryptographiques.

Le CST continue de donner des avis et des conseils aux institutions fédérales et aux organisations du secteur des infrastructures essentielles en matière de solutions de communications sécurisées.

Préparation à la cryptographie post-quantique

La cryptographie est un fondement de la cybersécurité, et elle est essentielle pour protéger les données et les communications. Cependant, on s'attend à ce que les ordinateurs quantiques deviennent assez gros pour casser la cryptographie qui est actuellement utilisée dans le monde, et ce, dès les années 2030.

Cette année, le CST a continué de contribuer au processus de normalisation international à l'appui de la cryptographie post-quantique. Le CST a fourni des commentaires publics sur trois normes proposées par le National Institute of Standards and Technology des États-Unis.

En même temps, le CST a travaillé avec des partenaires fédéraux afin de planifier la mise en œuvre de la cryptographie post-quantique au sein du gouvernement du Canada, lorsque les normes internationales seront finalisées.

De plus, le CST a fourni des dizaines de séances d'information sur la menace quantique et la préparation à la transition post-quantique aux partenaires des gouvernements et des infrastructures essentielles. Ces séances abordaient notamment l'importance d'utiliser la cryptographie normalisée et validée afin de prévenir des vulnérabilités informatiques évitables.

Autonomisation des Canadiennes et Canadiens

Le CST et le Centre pour la cybersécurité contribuent à autonomiser les Canadiennes et Canadiens en communiquant de l'information et en collaborant avec des partenaires afin que le Canada soit en un endroit où il est sécuritaire de vivre et de travailler en ligne.

Évaluations des menaces

Le Centre pour la cybersécurité publie régulièrement des évaluations des menaces afin de favoriser une meilleure compréhension des cybermenaces qui guettent le Canada, et des façons de les contrer, auprès de son lectorat. Les évaluations aident également à fixer les priorités relatives à la mission du CST. Au cours de l'année, le Centre pour la cybersécurité a publié quatre principales évaluations des menaces :

- Cybermenaces contre le secteur pétrolier et gazier du Canada[50]
- Évaluation des menaces de base : Cybercriminalité[51]
- Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023[52]
- La menace posée par les générateurs de texte basés sur des modèles de langage de grande taille[53]

Également, le Centre pour la cybersécurité a publié deux profils de groupes cybercriminels précis (voir la section Publications en lien avec la cybercriminalité).

Documents d'orientation

Le Centre pour la cybersécurité publie des documents d'orientation à l'intention de divers publics, d'un lectorat général à des gestionnaires, ainsi qu'à des cadres et à des praticiennes et praticiens des TI.

Cette année, le Centre pour la cybersécurité a publié 34 nouvelles publications d'orientation et en a mis à jour 14. Parmi les sujets d'intérêt figuraient :

- les technologies émergentes, comme l'IA;
- les tactiques de piratage psychologique, comme l'hameçonnage;
- les privilèges d'administrateur et l'authentification;
- les mesures d'atténuation contre les tactiques et techniques avancées des auteures et auteurs de menace.

Consultez le catalogue complet des documents d'orientation sur la cybersécurité[54] du Centre pour la cybersécurité.

Campagne Pensez cybersécurité

Le CST communique des conseils en matière de cybersécurité directement à la population canadienne par l'entremise de sa campagne de sensibilisation publique Pensez cybersécurité. Pensez cybersécurité offre des conseils simples et pratiques pour aider la population à se protéger au fil de ses activités en ligne.

Cette année, Pensez cybersécurité a produit plus de 40 nouvelles ressources sur une grande variété de sujets, comme sécuriser les appareils personnels et éviter les cyberfraudes.

Consultez toutes les ressources sur le site de Pensez cybersécurité[55].

Pensez cybersécurité pour les petites entreprises

Aucune entreprise, même la plus petite, n'est à l'abri des cybercriminelles et cybercriminels. Cependant, il n'est pas toujours réaliste pour un grand nombre de petites entreprises d'investir dans des solutions de cybersécurité coûteuses ou complexes.

Afin de pallier cette lacune, Pensez cybersécurité a produit, au début de 2024, une série de ressources pour les propriétaires de petites entreprises, et a mis à jour son guide rapide de la cybersécurité pour les petites entreprises.

Consultez les ressources de Pensez cybersécurité pour les petites entreprises[56].

Pensez cybersécurité a également lancé une campagne publicitaire sur les rançongiciels, dont le principal public cible était les petites entreprises. De février à mars 2024, les publicités ont été affichées plus de 49 millions de fois et ont généré 3,8 millions de vues sur les vidéos et près de 49 000 visites sur le site Web de Pensez cybersécurité.

Pensez cybersécurité pour les publics autochtones

Toutes les ressources de Pensez cybersécurité sont accessibles en anglais et en français. Afin de mieux joindre les communautés autochtones, Pensez cybersécurité a commencé cette année à traduire ses ressources les plus téléchargées en différentes langues autochtones. Les infographies suivantes sont maintenant accessibles en ojibwé, en cri, en inuktitut et en mi'kmaq :

- Les 7 signaux d'alarme de l'hameçonnage[57]
- L'authentification multifactorielle : votre cybersécurité vous appartient[58]
- Avez-vous un plan de sauvegarde pour vos données?[59]

Mois de la sensibilisation à la cybersécurité

En octobre, Pensez cybersécurité dirige le Mois de la sensibilisation à la cybersécurité (mois de la cybersécurité) au Canada. Cette année, le thème était « Mettez-vous en cyberforme » et des dizaines de ressources ont aidé les Canadiennes et Canadiens à se faire des cybermuscles. Les ressources comprenaient des graphiques téléchargeables sur les médias sociaux, des fonds d'écran pour les réunions virtuelles, un jeu-questionnaire interactif[60] et une vidéo d'entraînement sur la cybersécurité[61]. Extrait des paroles : « Le prochain pas est très tendance. Contre les rançongiciels, il faut garder la cadence. »

Des partenaires nationaux, comme HabiloMédias et l'Association des banquiers canadiens, ont aidé à créer et à transmettre le contenu du mois de la cybersécurité. Pendant ce temps, plus de 360 organisations ont partagé le contenu du mois de la cybersécurité avec leur public. Au cours du mois de la cybersécurité, le contenu de Pensez cybersécurité a été vu plus de 293 000 fois.

Apprenez-en davantage sur le site Web du Mois de la sensibilisation à la cybersécurité[62].

Médias sociaux

L'équipe responsable des médias sociaux du CST publie le contenu à l'intention de la population canadienne sur cinq plateformes : X (Twitter), Facebook, LinkedIn, YouTube et Instagram. Il y a au total 17 comptes ciblant différents publics, y compris les comptes en anglais et ceux en français du CST, du Centre pour la cybersécurité et de Pensez cybersécurité.

Cette année, le nombre d'abonnements, tous comptes confondus, est passé de 184 000 à 198 000. Le nombre total de publications a été de 5 580. Ces contenus ont été vus plus de 4 millions de fois.

Les médias sociaux en chiffres

Mesures d'atténuation

Les auteures et auteurs de menace utilisent des domaines malveillants pour héberger des sites Web et des courriels frauduleux. Les noms de domaine ressemblent souvent beaucoup à ceux d'organisations légitimes dans le but de tromper l'internaute et de l'inciter à donner des renseignements personnels ou à télécharger un maliciel. Au cours de l'année, le Centre pour la cybersécurité a collaboré avec des partenaires de confiance dans l'industrie afin de bloquer ou de retirer près de 300 000 domaines malveillants. De ce nombre, plus de 10 000 sites Web imitaient les sites Web d'institutions du gouvernement du Canada.

- 2023 à 2024
  - → Usurpation de domaines du gouvernement du Canada : 10 700
  - → Autres domaines malveillants : 284 000
- 2022 à 2023
  - → Usurpation de domaines du gouvernement du Canada : 3 167
  - → Autres domaines malveillants : 306 000

Hameçonnage par message texte

L'hameçonnage par message texte désigne les messages frauduleux envoyés par SMS (texto). Ces messages contiennent souvent des liens vers des sites Web usurpés qui imitent les sources de confiance, comme les organismes gouvernementaux, les banques, les compagnies de livraisons ou les boutiques en ligne.

Pour signaler l'hameçonnage par message texte[63], il suffit de transférer le texto au 7726 (qui épelle SPAM sur le clavier). Les fournisseurs de services de télécommunications (FST) peuvent ainsi prendre connaissance de l'hameçonnage par message texte et le bloquer pour l'ensemble de ses utilisatrices et utilisateurs. Plusieurs FST collaborent également avec le Centre pour la cybersécurité et lui fournissent le contenu anonymisé des pourriels. Le Centre pour la cybersécurité collabore aussi avec les partenaires de confiance dans l'industrie pour détecter et atténuer les répercussions des nouveaux URL (liens Web) malveillants qui se trouvent dans ce contenu.

Cette année, le Centre pour la cybersécurité a reçu plus de 1,6 million de messages d'hameçonnage par message texte provenant des FST et a pu atténuer les répercussions de plus de 37 000 nouveaux URL d'hameçonnage.

Bouclier canadien de l'ACEI

Bien souvent, les cybercriminelles et cybercriminels tentent d'inciter les gens à cliquer sur des liens qui vont injecter un maliciel sur l'appareil ou les connecter à un site Web malveillant. Le Bouclier canadien de l'Autorité canadienne pour les enregistrements Internet (ACEI)[64] est un service gratuit offert à la population canadienne qui lui permet de se protéger en utilisant les données de menace recueillies par le Centre pour la cybersécurité conjointement avec les flux commerciaux de cybersécurité.

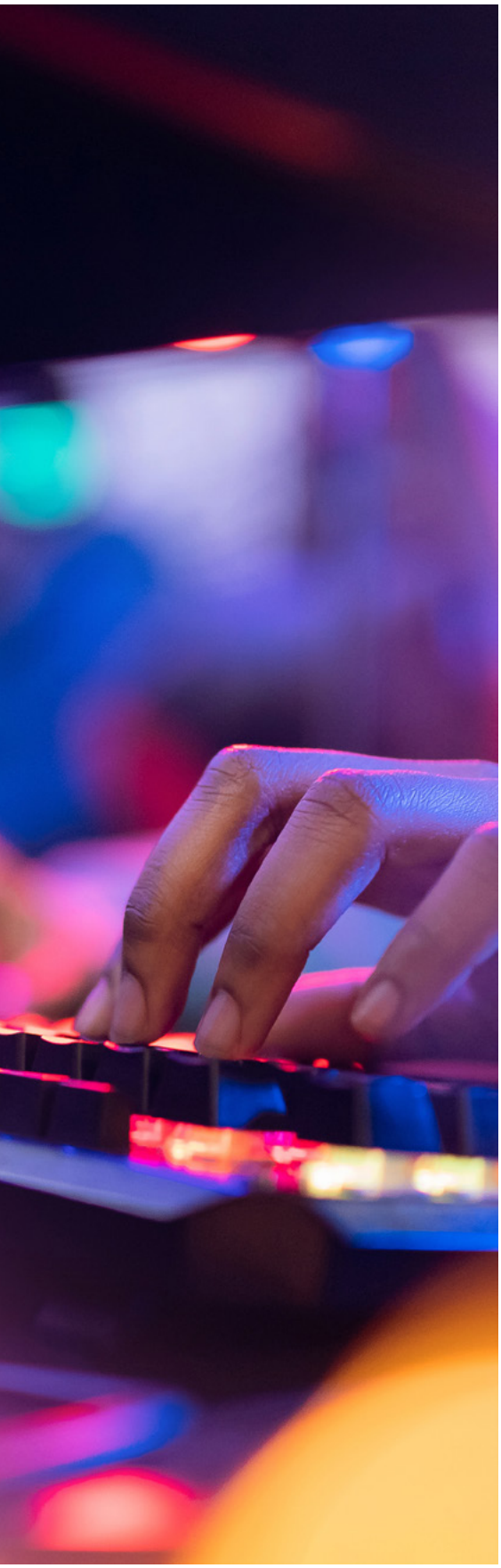
Jusqu'à maintenant, plus de 278 000 personnes se sont inscrites aux services de blocage des menaces du Bouclier canadien de l'ACEI. Ces services ont permis de bloquer plus de 500 millions de menaces au cours de l'année. C'est environ cinq connexions malveillantes bloquées par jour par personne inscrite.

Croissance de l'effectif en cybersécurité

Partout dans le monde, il manque de professionnelles et professionnels qualifiés en cybersécurité. Afin de résoudre ce problème, il faut que les gouvernements, l'industrie et le milieu universitaire collaborent. En tant que centre national d'expertise en cybersécurité, le Centre pour la cybersécurité joue un rôle de coordination afin d'appuyer et de guider ces efforts.

En avril 2023, en consultation avec les partenaires de l'industrie et du milieu universitaire, le Centre pour la cybersécurité a publié le Cadre des compétences en matière de cybersécurité du Canada[65]. Le cadre fait ressortir les lacunes actuelles dans le marché du travail au Canada et les compétences requises pour occuper différents rôles en cybersécurité.

Le Centre pour la cybersécurité continue de produire des ressources pour les enseignantes et enseignants ainsi que les élèves, dans le but de promouvoir les compétences en cybersécurité. Parmi ces ressources, il y a le nouveau cours du Carrefour de l'apprentissage à l'intention des professionnelles et professionnels de l'éducation (voir la section Formation en cybersécurité) et un cours ludique, intitulé Assurer la sécurité du Canada! Découvrir les carrières dans le domaine de la cybersécurité[66], qui porte sur les carrières en cybersécurité et est présenté sur la plateforme d'apprentissage numérique ChatterHigh.



Sensibilisation communautaire

Le CST mène une grande variété d'activités de sensibilisation visant à inspirer la prochaine génération de responsables de la cyberdéfense. Il a un intérêt tout particulier de joindre les groupes qui sont actuellement sous-représentés dans le domaine.

Cette année, afin d'intéresser encore plus de jeunes au Canada à poursuivre une carrière dans un domaine technique, le CST a renouvelé son soutien envers les partenaires suivants :

- Actua
- Black Boys Code
- Black Diplomats Academy
- CyberSci
- Cyber Titan
- Hackergal

Les bénévoles du CST ont participé aux activités suivantes :

- Sept ateliers de programmation dans trois écoles d'Ottawa
- Marathons de programmation et ateliers d'orientation professionnelle avec Hackergal et CyberTitan
- Journée d'orientation au CST avec Black Boys Code

> **« J'ai beaucoup aimé la journée, parce que j'avais l'impression de connecter avec des personnes comme moi. J'ai pu en apprendre plus sur des emplois auxquels je n'aurais jamais pensé après le secondaire. »**
>
> - Participant de la journée d'orientation de Black Boys Code au CST

Innovation

Le travail du CST a une grande incidence sur le Canada et la population canadienne, et c'est pourquoi l'organisme s'efforce d'être à l'avant-garde de l'innovation et de la recherche, en enquêtant continuellement sur les nouvelles menaces, en explorant de nouvelles capacités et en collaborant avec de nouveaux partenaires. Ce faisant, le CST garantit qu'il peut continuer de mener à bien sa mission, aujourd'hui et demain.

Lancement du nouveau secteur des Stratégies d'entreprise innovantes et du développement de la recherche

En septembre 2023, le CST a créé un nouveau secteur d'activités dont l'objectif est de promouvoir l'innovation par la collaboration avec les partenaires internes et externes. Entre autres, les priorités des Stratégies d'entreprise innovantes et du développement de la recherche viendront :

- appuyer l'élaboration d'un nouveau plan et d'une nouvelle vision stratégique du CST;
- favoriser l'engagement de l'industrie, du milieu universitaire et des partenaires provinciaux et territoriaux;
- obtenir des innovations, des capacités et des talents de l'externe pour appuyer les objectifs du CST.

La création de ce secteur montre l'importance de la recherche et de l'innovation afin de mener à bien la mission du CST.

Recherche

Les chercheuses et chercheurs du CST étudient une grande variété de sujets à l'appui du mandat de l'organisme. Des recherches sur la cryptographie, la cybersécurité, les sciences des données et les vulnérabilités, entre autres, permettent de veiller à ce que le CST ait l'expertise nécessaire pour relever les défis actuels et émergents.

Subventions CRSNG-CST à l'appui des communautés de recherche

Cette année, le CST et le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) ont collaboré afin de mettre sur pied des subventions CRSNG-CST à l'appui des communautés de recherche.

Il s'agit du premier programme de la sorte. Il propose des occasions de financement pluriannuel pour la recherche sur les technologies de pointe qui concordent avec les priorités du CST et du gouvernement du Canada. Le CST et le CRSNG financeront quatre communautés de recherche sur une période de dix ans, qui s'attarderont chacune à un sujet de recherche distinct.

Le programme a été lancé dans le cadre de l'initiative de recherche du CST, un engagement de financement envers les investissements en recherche annoncé dans le budget 2022. Cette initiative a pour but d'appuyer la recherche classifiée et non classifiée au CST.

Découvrez les subventions CRSNG-CST à l'appui des communautés de recherche[67] sur le site Web.

Des systèmes d'intelligence artificielle robustes, sûrs et sécurisés

En août 2023, le CST et le CRSNG ont annoncé le premier appel de propositions dans le cadre des subventions à l'appui des communautés de recherche, qui porte sur les systèmes d'intelligence artificielle robustes sûrs et sécurisés. La première subvention vise à :

- obtenir de nouvelles connaissances liées à des systèmes d'IA robustes, sûrs et sécurisés;
- améliorer les capacités des universités canadiennes à entreprendre de la recherche connexe;
- encourager une nouvelle génération de scientifiques et d'ingénieures et ingénieurs des données qui est au fait des enjeux touchant les systèmes d'IA robustes, sûrs et sécurisés.

Le CST a encouragé les propositions qui exploraient les **approches axées sur les données** en matière de systèmes d'IA robustes, sûrs et sécurisés, c'est-à-dire les projets de recherche qui touchaient les premières étapes du processus d'IA, comme l'amélioration de la qualité des données.

Ce sont 22 lettres d'intention provenant de 16 universités canadiennes qui ont été reçues. La proposition gagnante sera annoncé à l'été 2024.

Recherches universitaires

Au cours de la dernière année, les recherches universitaires du CST ont entraîné non seulement des innovations au CST et au sein de la communauté de recherche au Canada, mais aussi des répercussions à l'échelle mondiale.

L'Institut Tutte pour les mathématiques et le calcul[68] (ITMC) du CST a continué d'être un leader mondial dans la recherche relationnelle et sur les hypergraphes, qui a pour but de comprendre et de représenter les structures et relations complexes des données. Le travail sur les analyses vectorielles exploratoires continue d'offrir de grands avantages dans diverses recherches au sein de la collectivité canadienne de la sécurité et du renseignement, de la collectivité des cinq et de la communauté scientifique mondiale.

La recherche externe non classifiée de l'ITMC a eu également des répercussions importantes dans divers autres domaines d'études, y compris la recherche sur le cancer, l'astronomie, les neurosciences et l'analyse des médias sociaux.

Cette année, la contribution de l'ITMC à la communauté de recherche universitaire a consisté à :

- publier 14 articles de revues;
- produire 5 versions de logiciels contenant du nouveau code ou modifiant du code;
- publier 1 livre et en éditer 2 autres;
- participer à 5 discussions et à 7 présentations lors de conférences externes;
- organiser 3 séances de conférences spéciales;
- occuper des places au Conseil d'administration de la Société mathématique du Canada et présider son comité des nominations.

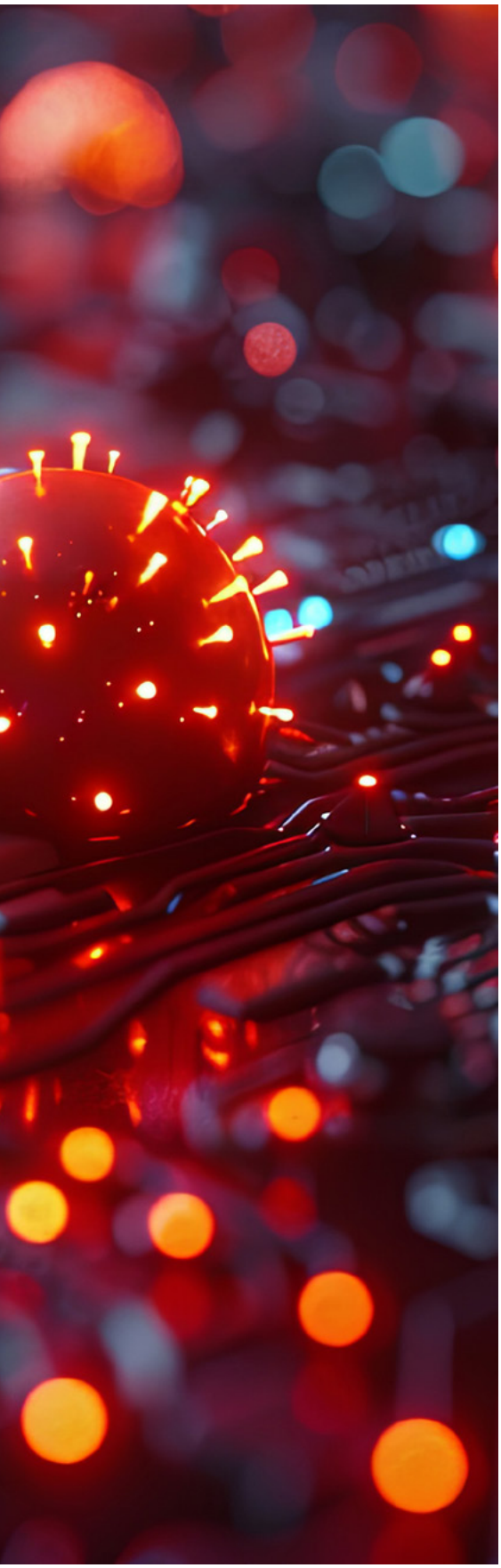
Plus de 2,5 millions de téléchargements s'effectuent chaque mois à partir des librairies logicielles de l'ITMC.

Recherche appliquée

Cette année, l'équipe chargée de la recherche appliquée[69] a mis l'accent sur l'opérationnalisation de nouveaux outils et la création de partenariats internes et externes.

À l'interne, les chercheuses et chercheurs ont collaboré étroitement avec les analystes du CST afin d'appuyer leur travail et d'accroître leurs capacités. Notamment, deux services sont passés de la recherche à la mise en service. Un d'entre eux est un outil qui utilise des techniques de la science des données pour aider les analystes à automatiser le flux de travail et à accroître l'efficacité de l'analyse des données. L'autre est un outil qui utilise l'apprentissage automatique pour traduire du contenu classifié dans plus de 100 langues (voir la section Outil de traduction alimenté par l'IA). Les chercheuses et chercheurs continuent d'aider à améliorer l'outil de traduction afin d'accroître sa rapidité et son exactitude.

À l'externe, les chercheuses et chercheurs ont contribué à sept présentations faites lors de conférences en science des données de la collectivité des cinq. Ils ont également publié un rapport technique à l'appui du programme d'Influence Campaign Awareness and Sensemaking (INCAS). L'objectif d'INCAS est de développer des techniques et des outils qui aident les analystes à détecter, à caractériser et à suivre les campagnes d'influence géopolitique.



Recherche et gestion de vulnérabilités

Le CST poursuit ses efforts de recherche appliquée des vulnérabilités à l'appui de son mandat et des mandats de ses partenaires fédéraux. Au cours de la dernière année, il a découvert de nombreuses vulnérabilités et a divulgué, de façon responsable, huit vulnérabilités aux fournisseurs touchés.

Il a également renforcé ses liens avec le milieu universitaire en entrant en contact avec deux nouvelles universités. Par exemple, à l'été 2023, le CST s'est associé à l'Université Concordia afin d'améliorer ses outils de recherche de vulnérabilités. Cette collaboration a permis de découvrir cinq vulnérabilités du jour zéro, qui ont été communiquées au fournisseur, Netgear. En février 2024, Netgear a publié un bulletin de sécurité qui reconnaissait les contributions du CST dans la découverte des vulnérabilités.

Mises à jour du Cadre de gestion du partage des nouvelles capacités

Le processus de gestion des vulnérabilités du CST est décrit dans le Cadre de gestion du partage des nouvelles capacités[70]. Ce cadre permet au CST de gérer les vulnérabilités qui sont découvertes de façon à appuyer sa mission de protection du pays.

Le cadre a été actualisé cette année afin de tenir compte du cyberespace en évolution constante et de garantir que les pratiques mettent au premier plan les intérêts du Canada et des Canadiennes et Canadiens.

La mise à jour du cadre comprend :

- l'ajout du soutien aux cyberopérations étrangères;
- la mise en évidence du rôle de la GRC et du SCRS en tant que membres officiels du Comité d'examen des actifs;
- le retrait d'un principe qui excluait les vulnérabilités uniques aux systèmes d'information et aux technologies utilisées exclusivement par une entité étrangère;
- l'ajout d'analyses environnementales comme condition à la prise de mesures ou au report de la prise de mesures par le CST suivant la divulgation d'une vulnérabilité.

Événements de collaboration

Le CST et le Centre pour la cybersécurité organisent plusieurs événements pendant l'année pour travailler intensément sur des problèmes liés à la mission. Ces ateliers sont des laboratoires d'innovation qui réunissent des participantes et participants de tout le Canada, de la collectivité des cinq, du milieu universitaire, de l'industrie et du secteur public.

GeekWeek 8

L'atelier GeekWeek 8[71] a eu lieu au Centre pour la cybersécurité en juillet 2023. Pendant les huit jours qu'a duré l'atelier, les participantes et participants ont travaillé sur des projets abordant certains des défis les plus complexes en cybersécurité.

Certains de ces projets ont exploré le potentiel de l'IA, par exemple :

- utiliser l'apprentissage automatique pour identifier les parties malveillantes d'un fichier;
- analyser de grandes quantités de données de menace;
- créer un dialogueur pour aider les analystes à gérer les cyberincidents.

Consultez le site Web pour en apprendre plus sur GeekWeek[72].

L'atelier GeekWeek 8 en chiffres

Grande exploration, 13e édition

Le CST a organisé la Grande exploration, 13e édition, sur une période de deux semaines de novembre à décembre 2023.

Cet événement classifié rassemble des participantes et participants du gouvernement du Canada, de l'industrie canadienne et des partenaires internationaux afin de développer de nouvelles solutions et capacités de cybersécurité.

Cette année, les équipes ont exploré des sujets comme :

- l'évaluation des vulnérabilités;
- la simulation de menaces;
- le renseignement sur les menaces;
- l'hameçonnage;
- l'intervention en cas d'incident.

Les modèles de langage de grande taille ont joué un rôle de premier plan dans un grand nombre de projets.

Le CST a accueilli Jen Easterly, directrice de la Cybersecurity and Infrastructure Security Agency (CISA)[73] (en anglais seulement), l'homologue américain du Centre pour la cybersécurité, qui a prononcé un discours.

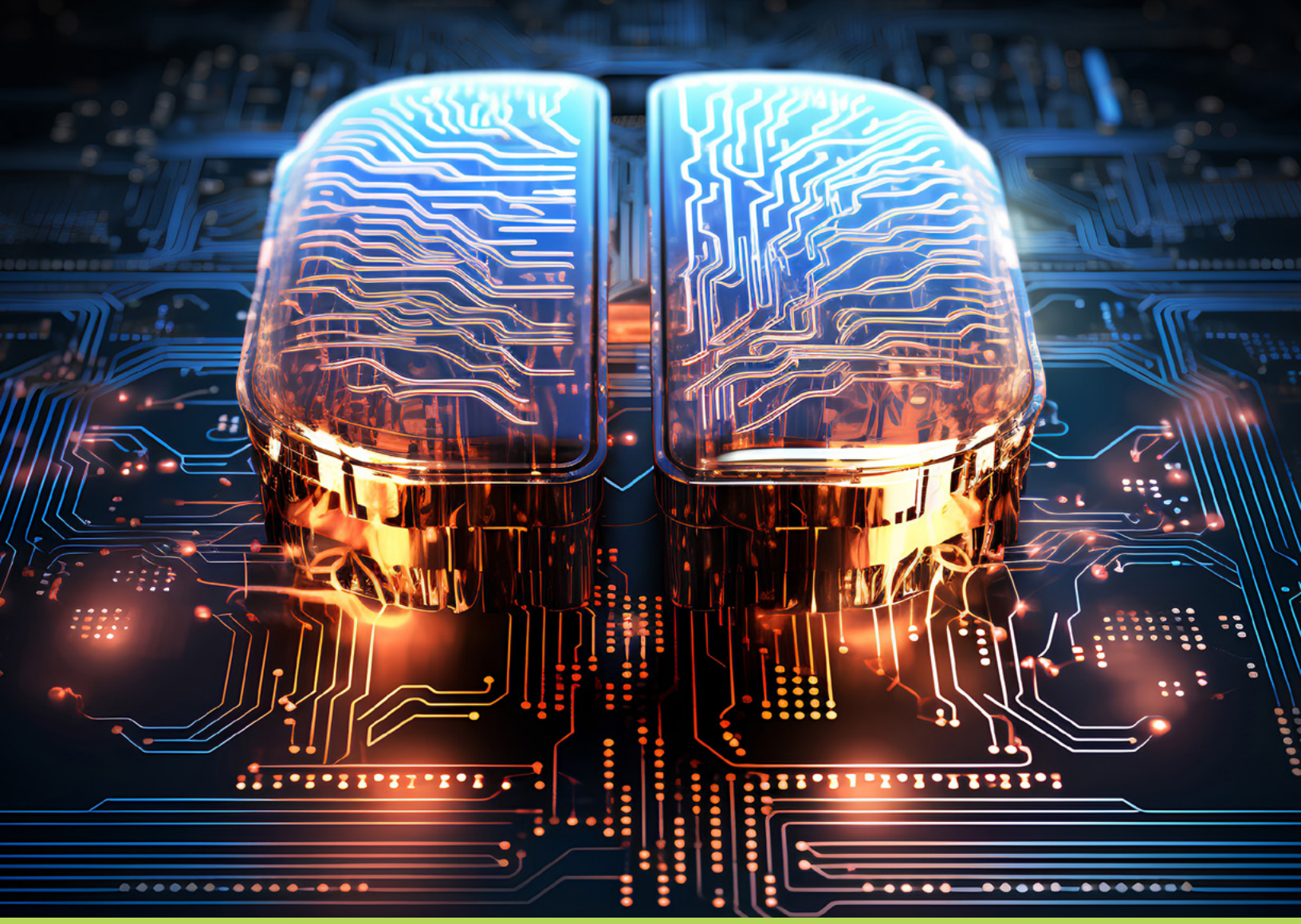
Consultez le site Web pour en apprendre plus sur la Grande exploration[74].

La Grande exploration, 13e édition, en chiffres

Projet Kickstart

Le projet Kickstart est un atelier classifié du CST axé sur le perfectionnement du savoir-faire en SIGINT. Les participantes et participants du Canada et des autres pays de la collectivité des cinq utilisent des outils à la fine pointe de la technologie pour s'attaquer aux problèmes les plus complexes du SIGINT dans un environnement classifié. Cette année, les participantes et participants de divers domaines d'expertise sont parvenus à :

- améliorer les outils SIGINT et les cyberoutils;
- explorer des techniques de la science des données en vue d'obtenir de nouveaux accès;
- réaliser des analyses des mégadonnées dans le contexte des principaux objectifs liés à la mission.



Intelligence artificielle

L'intelligence artificielle change la façon dont les Canadiennes et Canadiens travaillent, vivent, accèdent aux services et reçoivent les services. Chez les organisations, elle peut accroître la productivité et améliorer les services. L'IA est maintenant utilisée dans une grande variété d'industries partout sur le globe, et le domaine de la sécurité nationale ne fait pas exception.

Depuis longtemps, le CST est précurseur pour ce qui est d'utiliser les plus récentes technologies pour appuyer son travail et mener à bien sa mission, notamment en utilisant l'IA. Au cours des prochaines années, l'IA a le potentiel de renforcer considérablement la sécurité nationale, en contribuant à :

- améliorer et complémenter les capacités humaines;
- améliorer la capacité d'analyse des grandes quantités de données;
- appuyer la détection des nouvelles menaces, de sorte à accélérer l'intervention;
- automatiser les processus organisationnels pour accroître leur efficacité.

Bien qu'elle nous aide à mieux défendre le Canada, l'IA présente certains risques. Le CST et le Centre pour la cybersécurité sont déterminés à se servir de l'IA d'une manière responsable et éthique, tout en s'efforçant de protéger le Canada contre les menaces à la sécurité facilitées par l'IA.

Principaux termes

Intelligence artificielle

L'intelligence artificielle se rapporte aux technologies dont les comportements se manifestent à l'instar des comportements qui sont normalement associés à l'intelligence humaine, comme l'apprentissage, le raisonnement et la résolution de problèmes.

Science des données

La science des données est le processus qui consiste à adapter et à analyser les données afin d'obtenir des renseignements utiles à la prise de décisions humaine (ou automatique). La science des données atteint ces objectifs notamment au moyen de l'apprentissage automatique.

Apprentissage automatique

L'apprentissage automatique est une branche de l'IA qui permet aux machines d'apprendre comment effectuer une tâche à partir des données fournies sans avoir à programmer explicitement une solution étape par étape. Les modèles d'apprentissage automatique peuvent faire aussi bien, voire mieux, qu'un être humain pour certaines tâches, comme relever des tendances dans les données.

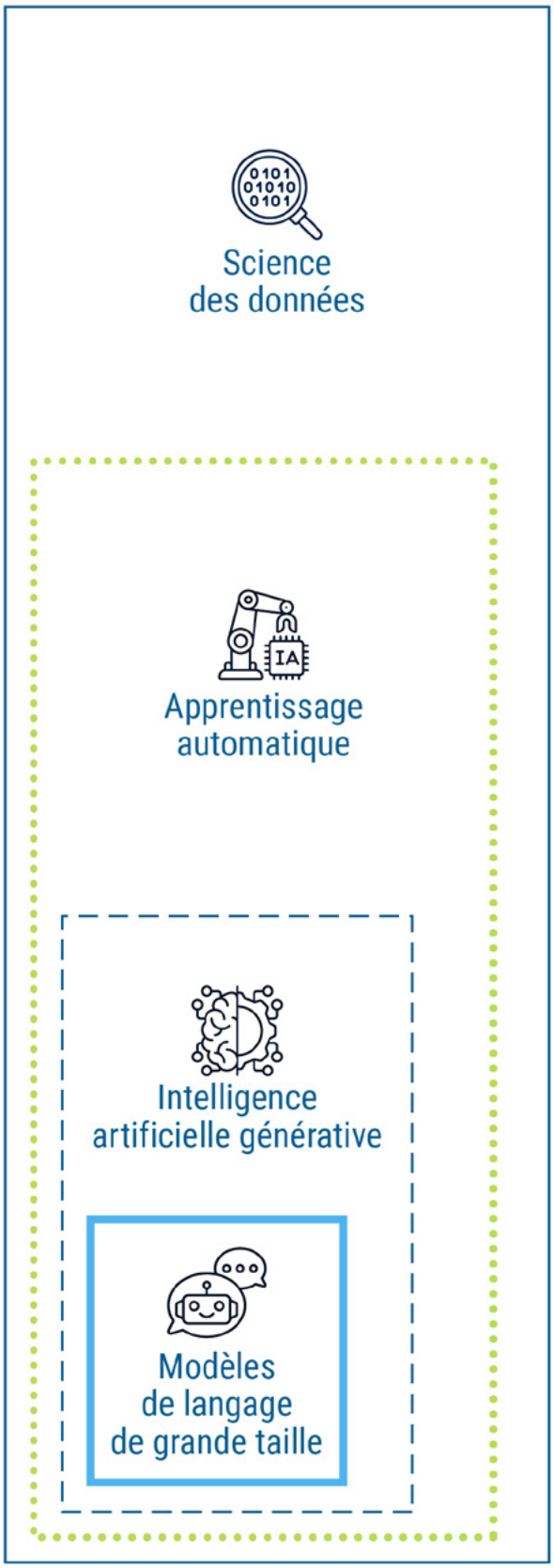
Intelligence artificielle générative

L'IA générative est une branche de l'apprentissage automatique qui génère du nouveau contenu en se fondant sur des jeux de données de grande taille, qui alimentent le modèle. L'IA générative peut créer du contenu dans divers formats, comme du texte, des images, du contenu audio ou vidéo et du code de logiciel.

Modèles de langage de grande taille

Les modèles de langage de grande taille (LLM pour *large language models*) sont un type d'IA générative entraînée sur de grands jeux de données linguistiques qui créent du langage semblable à celui de l'être humain sur un sujet donné à partir d'une requête. ChatGPT d'OpenAI et Gemini de Google sont des exemples de LLM.

Principaux termes reliés à l'IA



Sensibilisation aux menaces

Au cours des deux dernières années, l'IA générative a retenu l'attention du monde entier en raison de son accessibilité accrue et de sa capacité à générer du contenu synthétique difficile à distinguer du contenu créé par une personne.

Il y a des répercussions sur le contexte des cybermenaces au Canada, car les auteures et auteurs de menace peuvent se servir de l'IA pour accroître l'efficacité de leurs activités. Par exemple, ils peuvent utiliser les LLM pour rédiger une grande quantité de courriels d'hameçonnage qui sont difficiles à détecter, puisque les messages sont variés et semblent davantage être écrits par un être humain.

IA et menaces contre la démocratie

> **« Malgré les avantages possibles sur le plan créatif, la capacité de l'IA générative à polluer l'écosystème d'information par la désinformation menace les processus démocratiques partout dans le monde. »**
>
> - Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023

Les répercussions de l'IA générative deviennent particulièrement préoccupantes dans le contexte des processus démocratiques.

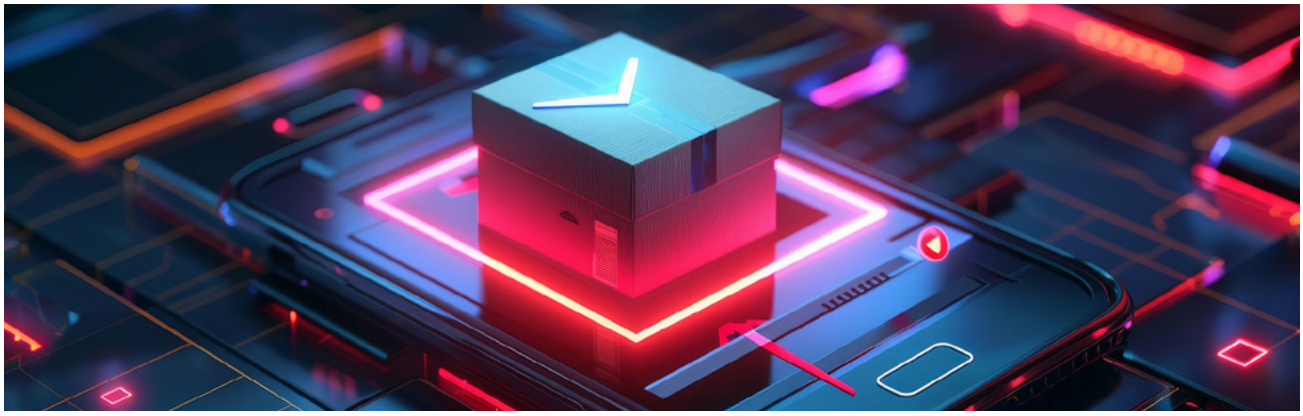
L'utilisation croissante de l'IA générative afin d'influencer les élections est une des principales tendances relevées dans un rapport du Centre pour la cybersécurité, intitulé Cybermenaces contre le processus démocratique du Canada : Mise à jour 2023[75].

Les auteures et auteurs de menace ont utilisé l'IA générative pour diffuser de la désinformation en ligne en créant des vidéos hypertruquées d'événements qui ne sont jamais arrivés. Le rapport prédit que les adversaires étrangers utiliseront probablement l'IA générative pour cibler les élections fédérales au Canada dans les deux prochaines années.

Menaces posées par les générateurs de texte basés sur des modèles de langage de grande taille

En janvier 2024, le Centre pour la cybersécurité a publié un rapport portant précisément sur la menace posée par les générateurs de texte basés sur des modèles de langage de grande taille[76].

Ce rapport détermine que les campagnes d'influence en ligne et d'hameçonnage par courriel sont des menaces probables qui découlent de ce type d'IA générative. De plus, il soulignait d'autres risques pesant sur les organisations qui utilisent des générateurs de texte basés sur les LLM, comme la sécurité des données et les risques liés à la gouvernance des données.



Adoption d'une IA sécurisée

Le CST a par ailleurs produit une vidéo éducative, intitulée Songer à la sécurité lorsqu'on adopte l'intelligence artificielle[77]. La vidéo, qui a pour principale cible la fonction publique du Canada, a été publiée par l'École de la fonction publique du Canada en mars 2024. Plusieurs dirigeantes et dirigeants d'organismes de la collectivité des cinq, de même que des spécialistes en matière d'IA du gouvernement du Canada, de l'industrie et du milieu universitaire, apparaissent dans la vidéo. Ils discutent du besoin d'agir dès maintenant pour mettre en place des cadres fondés sur les principes qui optimisent les possibles avantages de l'IA, tout en accordant la priorité à la sécurité et à la sûreté.

> **« L'IA est à la fois source de possibilités et de vulnérabilités. »**
>
> - **Caroline Xavier, chef, CST, Songer à la sécurité lorsqu'on adopte l'intelligence artificielle**

Atténuation des risques

En plus de sensibiliser aux menaces que présente l'IA, le CST cherche à les atténuer.

En juillet 2023, le Centre pour la cybersécurité a publié des conseils pour la population et les organisations canadiennes sur l'intelligence artificielle générative[78]. Le document fournit une liste de contrôle de mesures à prendre pour atténuer les risques de compromission découlant de cyberattaques facilitées par l'IA. Une autre liste de contrôle propose aux organisations des mesures dont tenir compte en lien avec l'utilisation des outils d'IA générative.

Il a également publié deux documents conjoints avec ses partenaires internationaux cette année, en vue d'offrir des conseils sur le développement et l'utilisation de l'IA. Les partenaires du Royaume-Uni ont dirigé la publication intitulée Lignes directrices pour le développement de systèmes d'IA sécurisés[79], en collaboration avec 17 autres pays, dont le Canada.

Cette publication donne des conseils en vue de développer, de déployer et d'utiliser l'IA de façon sécurisée et responsable. En janvier 2024, le Centre pour la cybersécurité s'est joint à l'Australie et à neuf autres pays pour publier un guide sur l'utilisation sécurisée des systèmes d'IA, intitulé Engaging with Artificial Intelligence[80] (en anglais seulement).

En plus de produire des documents d'orientation pour le public, le Centre pour la cybersécurité :

- a conseillé ses partenaires fédéraux quant à l'utilisation sûre des outils d'IA au gouvernement du Canada;
- a conseillé ses partenaires des infrastructures essentielles quant aux risques de cybersécurité que présente l'IA;
- a collaboré avec les partenaires de l'industrie et du milieu universitaire dans le cadre de la recherche en lien avec l'IA;
- a travaillé avec ses partenaires de la collectivité des cinq pour harmoniser les activités et les conseils donnés en matière d'IA;
- a contribué aux efforts internationaux en vue de :
  - → créer des politiques sur l'utilisation sûre et responsable de l'IA,
  - → créer des normes internationales de cybersécurité en matière d'IA;
- a co-organisé un séminaire en personne des leaders d'opinion du gouvernement, de l'industrie et du milieu universitaire afin de discuter de l'IA, plus précisément de la conception sécurisée de l'IA.

Ces efforts ne touchent pas uniquement l'IA. Même si l'IA a gagné en popularité au cours des deux dernières années, un des principaux rôles du Centre pour la cybersécurité a toujours été de collaborer avec ses partenaires afin d'améliorer la cybersécurité des technologies numériques.

Utilisation de l'IA dans le cadre de la mission du CST

Pendant toute son histoire, le CST a utilisé des technologies avancées pour aider à protéger le Canada et ses alliés. La science des données est pratiquement la mission fondamentale du CST. Ces dernières années, l'utilisation de l'IA et de l'apprentissage automatique à l'appui des activités relatives à la mission s'est ajoutée.

Le CST possède certains des ordinateurs haute performance les plus puissants au pays. Il utilise ces superordinateurs afin d'entraîner de nouveaux modèles d'IA et d'apprentissage automatique, comme son outil de traduction alimenté par l'IA. Tirer parti du pouvoir de l'IA et de l'apprentissage automatique ne signifie pas qu'on élimine l'intervention humaine du processus. L'accent est plutôt mis sur l'utilisation de la science des données et de l'apprentissage automatique dans le but de permettre aux personnes de prendre de meilleures décisions dans le cadre juridique rigoureux et les structures de reddition de comptes dans lesquels le CST mène ses activités.

Outil de traduction alimenté par l'IA

Les logiciels de traduction sont des outils puissants, et un grand nombre de versions sont largement disponibles en ligne. Toutefois, le CST ne peut pas utiliser ces outils pour traduire du renseignement électromagnétique ou du contenu classifié brut.

C'est pourquoi la Direction de la recherche du CST a développé un outil interne de traduction automatique qui utilise l'apprentissage automatique. Les analystes peuvent utiliser l'outil pour traduire du contenu à partir de plus de 100 langues. Les équipes SIGINT du CST ont rendu opérationnel l'outil à la fin de 2022 et l'ont rendu accessible aux partenaires de la collectivité des cinq en janvier 2023.

Les chiffres de la première année financière complète d'utilisation de l'outil, c'est-à-dire plus de 1 million de requêtes par mois provenant du CST et plus de 100 000 requêtes par mois provenant des partenaires de la collectivité des cinq, montrent qu'il apporte une bonne contribution à la collectivité des cinq.

L'IA au service de la cyberdéfense

Le travail du Centre pour la cybersécurité visant à protéger les systèmes du gouvernement fédéral et des infrastructures essentielles contre les cybermenaces consiste en grande partie à détecter les tendances dans une grande quantité de données. Et les outils d'apprentissage automatique conviennent particulièrement à cette tâche. Par exemple, l'apprentissage automatique permet de détecter :

- les campagnes d'hameçonnage ciblant le gouvernement du Canada;
- les cyberactivités suspectes sur les réseaux et les systèmes du gouvernement fédéral (voir la section Capteurs).

L'outil Assemblyline[81] du Centre pour la cybersécurité utilise également l'apprentissage automatique pour analyser les logiciels malveillants. Depuis cette année, cet outil a intégré des fonctions optionnelles d'IA générative (voir la section Analyse de maliciels).

Étant donné que les auteures et auteurs de menace exploitent de plus en plus l'IA afin d'éviter la détection, les outils d'apprentissage automatique joueront un rôle important pour aider les analystes à repérer et à atténuer les cybermenaces qui visent le gouvernement du Canada et les infrastructures essentielles du Canada.

Recherche sur l'IA

Le domaine de l'IA évolue rapidement. Le CST mène des recherches fondamentales et appliquées afin de mieux comprendre et exploiter le potentiel de l'IA.

Les chercheuses et chercheurs de l'ITMC du CST font progresser la science des données fondamentale qui appuie l'IA et l'apprentissage automatique, y compris l'exploration des données non structurées, ainsi que l'utilisation robuste, sûre et sécurisée de l'IA. Pendant ce temps, l'équipe du CST chargée de la recherche appliquée explore des utilisations appliquées qui concernent davantage la mission du CST, comme :

- le triage des données;
- la recherche sémantique (trouver de l'information pertinente en fonction de la signification plutôt que de mots précis).

Les chercheuses et chercheurs s'efforcent également d'intégrer les projets de recherche sur l'IA en contexte opérationnel.

Cette année, les chercheuses et chercheurs du CST ont organisé un exercice visant à évaluer manuellement la sûreté de certains LLM précis de source ouverte. Ils ont composé des requêtes pour déterminer si les modèles généreraient des réponses malveillantes qui pourraient causer du tort à des personnes. Cet exercice a aidé les chercheuses et chercheurs à mieux comprendre les exigences de sûreté de référence des modèles.

Partenariats de recherche

En plus de mener ses propres recherches, le CST a collaboré avec des partenaires du fédéral, du milieu universitaire et de l'industrie pour favoriser l'innovation en matière d'IA et mettre sur pied ses propres capacités.

Par exemple, le CST collabore actuellement avec des spécialistes de l'industrie dans le domaine des LLM afin d'explorer des façons d'utiliser les LLM pour répondre à ses besoins opérationnels.

Le CST et le CRSNG collaborent afin de favoriser le développement de technologies d'IA robustes, sûres et sécurisées. Consultez la section sur l'innovation pour en savoir plus sur les subventions CRSNG-CST à l'appui des communautés de recherche.

Afin d'assurer une utilisation éthique de l'IA au CST, ce dernier élabore des approches exhaustives visant à régir, à gérer et à surveiller l'utilisation de l'IA, et il continuera de s'inspirer des pratiques exemplaires et des échanges pour garantir que ses conseils s'appuient sur les perspectives actuelles.

Reddition de comptes

Le mandat du CST est défini dans la *Loi sur le CST*, qui donne des limites claires afin de protéger la vie privée des Canadiennes et Canadiens. Le CST surveille ses activités à l'interne, et des organes d'examen externe supervisent et examinent ses activités au nom des Canadiennes et Canadiens.

Examens externes

Les activités du CST, à l'instar de celles des autres ministères fédéraux, font l'objet d'un examen par des organes d'examen fédéraux, comme le Commissariat à la protection de la vie privée et le Bureau du vérificateur général.

Ces organes d'examen externe veillent, au nom des Canadiennes et Canadiens, à ce que les activités du CST respectent la loi. Le CST est en faveur de ces examens indépendants, puisqu'ils assurent la transparence et la reddition de comptes de son important travail. Il attache de l'importance aux commentaires qui découlent des examens et en tient compte pour améliorer ses processus.

Par ailleurs, étant donné qu'il fait partie de la collectivité de la sécurité nationale du Canada, le CST peut faire l'objet d'un examen par les organismes suivants :

- Office de surveillance des activités en matière de sécurité nationale et de renseignement[82] (OSSNR)
- Comité des parlementaires sur la sécurité nationale et le renseignement[83] (CPSNR)

Ces organes d'examen publient en ligne des rapports non classifiés de leurs examens afin d'accroître la transparence envers le public. Ils soumettent également des rapports classifiés aux ministres et à la première ministre ou au premier ministre afin de leur donner une vue d'ensemble des conclusions des rapports.

Le CST soutient activement les examens externes en breffant le personnel responsable des examens, en répondant aux questions et en donnant accès aux documents classifiés et non classifiés. Depuis mars 2023, le CST et l'OSSNR ont mis à l'essai une nouvelle solution qui donne à l'OSSNR un accès direct et indépendant au dépôt organisationnel classifié officiel du CST. Le projet pilote a été renouvelé en septembre 2023 et se poursuit.

Statistiques liées aux examens externes

Au cours de l'année, le CST :

- a contribué à 26 examens externes et rapports;
- a présenté 31 breffages aux organes d'examen;
- a répondu à 317 questions.

Le CST a répondu à 96 % des questions dans les délais requis, une hausse importante par rapport à l'année précédente.

Examens sur l'ingérence étrangère

Parmi les 26 examens externes auxquels a contribué le CST cette année, 4 étaient des examens sur l'ingérence étrangère dans les élections fédérales au Canada. Ces examens ont été effectués par l'OSSNR, le CPSNR, le rapporteur spécial indépendant[84] (RSI) et la Commission sur l'ingérence étrangère[85].

La Commission sur l'ingérence étrangère a été mise sur pied en septembre 2023 afin de procéder à l'Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux. Le CST a présenté des breffages au personnel de la Commission, a donné accès à tous les documents demandés et a fourni un espace de travail sécurisé aux fins d'examens et de discussion des documents classifiés. De plus, le CST a fourni un soutien technique, comme des téléphones sécurisés, des ordinateurs de bureau, des services de vidéoconférence et l'accès au RCTS.

Des représentantes et représentants du CST ont témoigné devant la Commission lors d'audiences à huis clos et d'audiences publiques entre janvier et avril 2024.

Le CST a remis à la Commission deux rapports institutionnels (un classifié et un non classifié) résumant le mandat et les activités du CST relativement à la lutte contre l'ingérence étrangère. La version non classifiée du rapport institutionnel du CST[86] est accessible sur le site Web de la Commission.

Le CST reconnaît l'importance des examens externes en vue d'assurer la reddition de comptes et de favoriser la transparence en matière d'ingérence étrangère. Comme énoncé dans les rapports sur les menaces, les États étrangers utilisent de plus en plus les cyberoutils pour s'ingérer dans les processus démocratiques partout dans le monde, plus du quart des élections nationales à l'échelle mondiale ayant été ciblées[87]. Le Canada doit avoir une image claire des réalités liées à l'ingérence étrangère et doit faire en sorte que ses processus démocratiques soient aussi résilients que possible. Le mandat du CST est important pour ces deux aspects, et il s'efforce de respecter ces besoins (voir la section sur les activités d'États hostiles et l'ingérence étrangère).

Le CST est toujours heureux de recevoir des conseils et des avis externes pour lui permettre de remplir son mandat de manière plus efficace. Il accordera une attention particulière aux recommandations et prendra les mesures nécessaires.

Autorisations ministérielles

En vertu de la *Loi sur le CST*[88], certaines activités doivent être autorisées par la ou le ministre de la Défense nationale. Il y a différentes autorisations selon les volets du mandat du CST.

Autorisations de renseignement étranger et de cybersécurité

Avant d'entreprendre une activité en vertu d'une autorisation de renseignement étranger ou de cybersécurité, le CST doit recevoir l'approbation de la ou du commissaire au renseignement[89], qui a une fonction de surveillance indépendante quasi judiciaire.

En 2023, le CST a soumis six autorisations auprès du commissaire au renseignement, parmi lesquelles trois ont été approuvées dans leur entièreté et trois en partie :

- Autorisations de cybersécurité visant à protéger les institutions fédérales
  → Soumises : 1
  → Approuvées dans leur entièreté : 1
- Autorisations de cybersécurité visant à protéger des institutions non fédérales
  → Soumises : 2
  → Approuvées dans leur entièreté : 2
- Autorisations de renseignement étranger
  → Soumises : 3
  → Approuvées en partie : 3

Dans le cas des autorisations partielles, le commissaire au renseignement a retiré une clause concernant des activités habilitantes en lien avec les activités de renseignement étranger. Le commissaire estimait qu'il n'avait pas suffisamment de détails pour justifier la clause.

Autorisations de cyberopérations étrangères

Le nombre d'autorisations de cyberopérations étrangères en 2023 est resté le même que l'année précédente.

- Autorisations de cyberopérations actives : 3
- Autorisations de cyberopérations défensives : 1

Les autorisations sont valides pendant un an et peuvent couvrir plusieurs opérations ou aucune. La section sur les cyberopérations étrangères présente plus d'informations sur les types d'opérations qu'a effectuées le CST.

Arrêtés ministériels

La ou le ministre de la Défense nationale signe des arrêtés ministériels pour désigner des personnes ou des organisations avec lesquelles le CST peut collaborer ou auxquelles il peut transmettre de l'information. En date du 31 mars 2024, cinq arrêtés ministériels sont en vigueur au CST :

- Arrêté désignant les destinataires d'informations nominatives sur des Canadiennes et Canadiens en vertu du volet du mandat du CST touchant le renseignement étranger;
- Arrêté désignant les destinataires d'informations qui se rapportent à une Canadienne ou à un Canadien ou à une personne se trouvant au Canada en vertu de du volet du mandat touchant la cybersécurité;
- Arrêté désignant l'information électronique et les infrastructures d'information importantes pour le gouvernement du Canada;
- Arrêté désignant l'information électronique et les infrastructures d'information du gouvernement de la Lettonie comme étant importantes pour le gouvernement du Canada;
- Arrêté désignant l'information électronique et les infrastructures d'information importantes du gouvernement de l'Ukraine comme étant importantes pour le gouvernement du Canada.

Le seul arrêté ministériel signé cette année portait sur la désignation des destinataires d'informations en vertu du volet du mandat du CST touchant la cybersécurité. Signé en juin 2023, il remplace l'arrêté précédent qui partageait le même objectif.

Divulgation d'informations nominatives sur des Canadiennes et Canadiens

Il est interdit au CST de faire porter ses activités sur des Canadiennes et Canadiens ou des personnes se trouvant au Canada. Toutefois, il est possible que de l'information qui se rapporte à une Canadienne ou un Canadien ou à une personne se trouvant au Canada soit incidemment acquise dans le cadre d'activités de renseignement étranger légitimes. Le CST dépersonnalise et supprime toute information nominative sur une Canadienne ou un Canadien (INC) de ses rapports de renseignement. Cependant, les organismes et les ministères désignés par un arrêté ministériel peuvent demander que soit divulguée de l'INC dans certaines conditions[90]. Le CST examine chaque demande au cas par cas.

En 2023, le CST a reçu 1 072 demandes de divulgation, presque 1,5 fois le nombre de 2022. Un peu plus de 13 % des demandes provenaient d'organismes de la collectivité des cinq. Dans l'ensemble, le CST a approuvé 72 % des demandes de divulgation d'INC.

- Demandes de divulgation d'INC en 2023
  - → Approuvées : 72 %
  - → Refusées : 12 %
  - → Annulées : 15 %
  - → En cours : 1 %

Conformité interne

L'équipe chargée de la conformité au CST est responsable de veiller à ce que les membres du personnel respectent les politiques internes dans leur travail. Toutes les conclusions en matière de conformité interne au CST sont accessibles aux organes d'examen externe.

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

- 15 évaluations
- 6 études
- 2 vérifications ponctuelles

En février 2024, le CST a organisé une conférence sur la conformité à laquelle ont participé les partenaires de la collectivité des cinq en vue d'échanger des pratiques exemplaires et de discuter d'enjeux communs.

Les autres activités de recherche comprenaient :

- la révision des tests de conformité du CST pour les employées et employés;
- l'organisation de la Semaine annuelle de la conformité des activités.

Incidents de conformité

Malgré tous les efforts du CST pour les éviter, des erreurs surviennent. Tout événement qui ne respecte pas les politiques internes du CST constitue un incident de conformité. Si l'incident concerne de l'information qui se rapporte à une Canadienne ou un Canadien ou à une personne au Canada, il est catégorisé comme un « incident de nature opérationnelle lié à la vie privée ». La conservation de données au-delà de la date de conservation normale ou la communication par inadvertance d'INC dans un rapport de renseignement étranger en sont des exemples. Si l'incident implique un partenaire de la collectivité des cinq, il est catégorisé comme un « incident lié à la vie privée impliquant un partenaire de deuxième part ».

En 2023, l'équipe chargée de la conformité au CST a dénombré les incidents suivants :

- 104 incidents de nature opérationnelle liés à la vie privée
- 35 incidents liés à la vie privée impliquant un partenaire de deuxième part

Dans chaque cas, le CST évalue les événements, atténue les répercussions (par exemple en supprimant les données ou en rappelant un rapport) et cherche à résoudre la cause fondamentale.

Plaintes

En janvier 2024, le CST a simplifié son processus de dépôt de plaintes[91] par l'entremise directe de son site Web pour le public. Par le passé, il n'était possible de déposer une plainte que par courrier. Le nouvel outil en ligne est plus rapide et accessible que l'option par courrier, bien qu'il soit toujours possible de procéder de cette façon. La nouvelle façon de faire aide à ce que soit produite toute l'information nécessaire afin de mener une enquête en bonne et due forme. Ce faisant, le CST devrait être en meilleure position pour répondre aux plaintes dans un délai de 60 jours.

Cette année financière, le CST a reçu 10 plaintes externes à l'intention de la chef du CST et a répondu à 5 plaintes envoyées à l'OSSNR concernant ses activités.

Transparence

Le présent rapport représente une des manières utilisées par le CST pour communiquer de l'information aux Canadiennes et Canadiens. Cette année encore, le CST a favorisé la transparence quant à ses activités en prenant part aux activités suivantes :

- discours, conférences et événements publics
- 6 témoignages parlementaires
- 4 rapports publics[92]
- 55 entrevues avec les médias
- 4 conférences de presse
- 52 publications sur le portail du gouvernement ouvert[93]
- 32 réponses à des demandes d'accès à l'information[94]
- 12 divulgations proactives[95]
- 110 réponses à des questions à inscrire au Feuilleton[96]
- 5 580 publications sur les médias sociaux

Audit, évaluation et éthique

Chaque ministère fédéral doit évaluer ses activités afin de veiller à ce qu'il se conforme aux politiques (audit) et qu'il utilise de façon responsable ses ressources (évaluation).

Les équipes chargées des audits et des évaluations donnent des conseils impartiaux fondés sur des preuves directement à la haute direction afin d'aider le CST à atteindre ses objectifs stratégiques. Cette année, le CST a réalisé deux audits et deux évaluations de programmes, en vue d'améliorer l'efficacité et l'efficience des activités opérationnelles du CST. Les audits internes du CST peuvent faire l'objet d'un examen externe afin de vérifier qu'ils sont effectués de façon indépendante et qu'ils respectent les normes.

L'équipe chargée de l'éthique[97] continue d'offrir des formations et des conseils sur une variété de sujets, des conflits d'intérêts potentiels pour le personnel aux considérations d'ordre éthique dans le cadre des activités liées à la mission.

De plus, le CST a souligné le 10e anniversaire de la Charte d'éthique du CST[98] lors d'une série d'événements se déroulant pendant une semaine, y compris des activités d'apprentissage et une présentation sur l'IA et l'éthique par un conférencier invité.

Équipe spéciale sur les valeurs et l'éthique

En septembre 2023, la chef du CST, Caroline Xavier, a été invitée, ainsi que quatre autres sous-ministres, à relancer le dialogue sur la façon dont les fonctionnaires font l'expérience des valeurs et de l'éthique dans un monde en évolution rapide. L'équipe spéciale a organisé environ 90 discussions avec des personnes, des groupes et des communautés de la fonction publique et a présenté son rapport préliminaire[99] en décembre.

> **« Notre rapport au greffier est le début de la conversation, pas la fin. »**
>
> - **Équipe spéciale de sous-ministres sur les valeurs et l'éthique, rapport préliminaire**

Beaucoup d'employées et d'employés du CST ont pris part aux discussions initiales. Les commentaires mentionnaient la nécessité de fournir une formation sur l'éthique fondée sur des scénarios et des lignes directrices claires concernant l'utilisation personnelle des médias sociaux.

Les membres du personnel ont également soulevé la nécessité que la Charte d'éthique du CST tienne compte de façon explicite des valeurs de l'organisme quant au respect des personnes, des valeurs comme l'accessibilité, la lutte contre le racisme, l'équité, l'inclusion et la réconciliation.

En réponse à ces commentaires, le CST a entamé le processus d'examen de la Charte d'éthique et de mise à jour de sa formation sur l'éthique. Ces efforts se poursuivront au cours de la prochaine année financière, en partenariat avec les employées et employés du CST et les groupes d'affinité.

Personnes

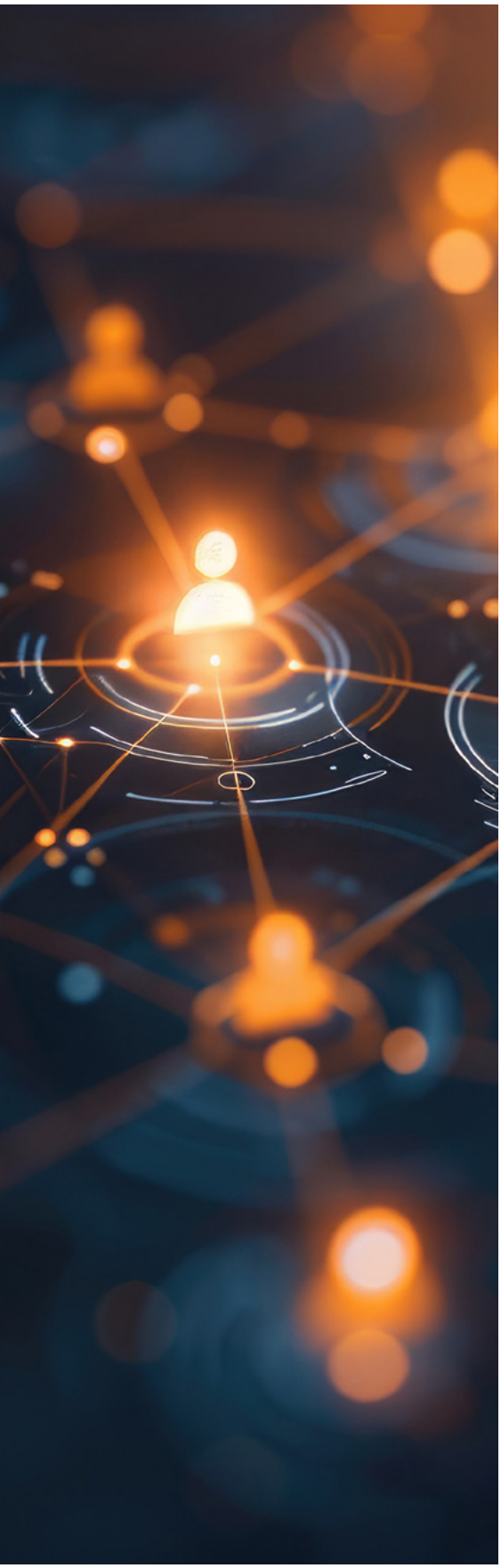
Au CST, le personnel est la plus grande force. L'effectif du CST est composé de personnes dévouées, qui prennent appui sur leurs parcours et leurs expériences uniques pour protéger le Canada, et ce, en tout temps.

Au cours de la dernière année, le CST a participé à un grand nombre d'activités afin de joindre des candidates et candidats potentiels, de recruter de nouvelles et nouveaux employés et d'appuyer sa communauté en pleine croissance.

Recrutement

Cette année, le CST a redoublé d'efforts pour attirer et embaucher les personnes dont il a besoin pour mener à bien efficacement sa mission et répondre à la demande croissante.

Il a embauché environ 465 employées et employés permanents à temps plein. L'effectif total du CST compte maintenant 3 529 employées et employés, une augmentation de 9 %.



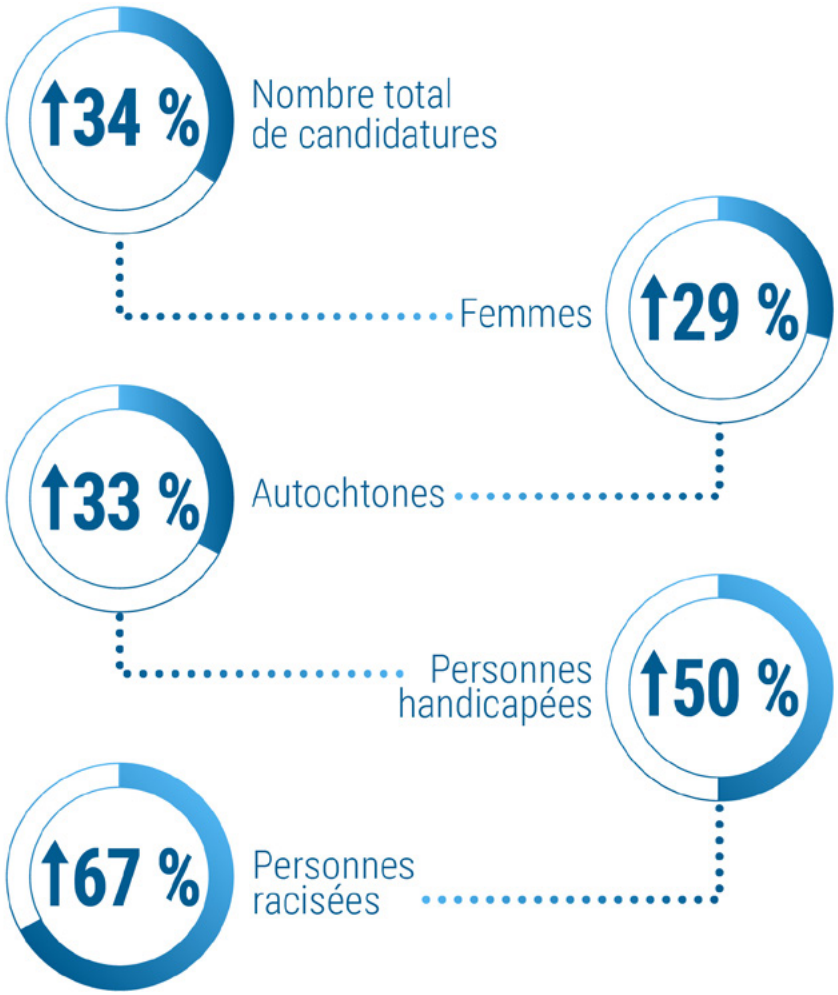
Activités de recrutement

L'équipe de recrutement a voyagé au pays pour participer à plus de 160 événements, y compris des salons de l'emploi, des marathons de programmation, des séances d'information et des événements de réseautage. Près d'un événement sur sept s'est déroulé entièrement en français, et un tiers des événements étaient axés sur l'équité, la diversité et l'inclusion et visaient précisément les personnes en recherche d'emploi provenant de communautés sous-représentées.

De plus, le CST a tiré parti de sites d'emploi précis afin d'attirer encore plus les candidatures de personnes racisées et autochtones et a mené deux campagnes publicitaires ayant pour but de joindre encore plus de candidates et candidats potentiels. Il a également effectué un examen de ses affiches de poste afin de veiller à utiliser un langage simple et inclusif, aussi exempt de préjugés que possible.

Ces efforts ont entraîné une importante augmentation du nombre de candidatures en général, en particulier chez les groupes en quête d'équité.

Candidatures au CST de 2023 à 2024[100]



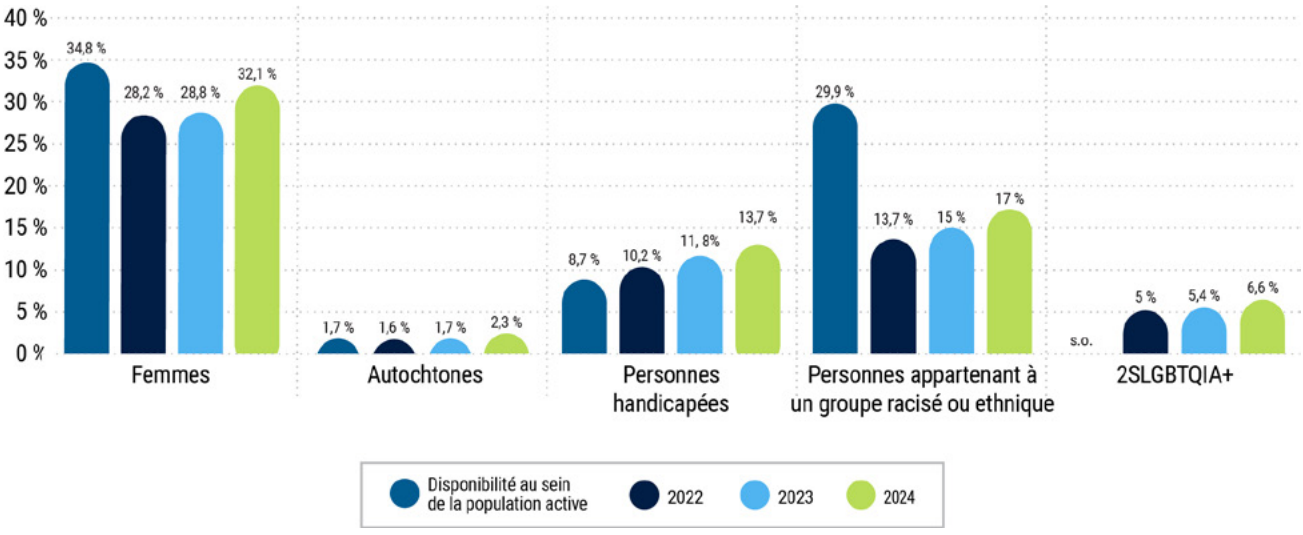
Constituer un effectif représentatif

Le CST met tout en œuvre pour constituer un effectif représentatif des différentes communautés qu'il protège. Il accorde la priorité à une plus grande représentativité à tous les échelons de l'organisme.

Comme mentionné, le CST a consacré des efforts considérables cette année afin d'accroître la représentation des groupes en quête d'équité, des efforts qui ont eu l'effet escompté.

Les derniers chiffres montrent que la diversité continue d'augmenter au CST. La représentation des Autochtones et des personnes handicapées au sein de l'effectif du CST est supérieure à la disponibilité au sein de la population active. Cependant, les femmes et les personnes racisées demeurent sous-représentées. Le CST est déterminé à changer la situation et continuera de chercher à attirer et à retenir les candidates et les candidats provenant de ces communautés par l'entremise de divers programmes adaptés.

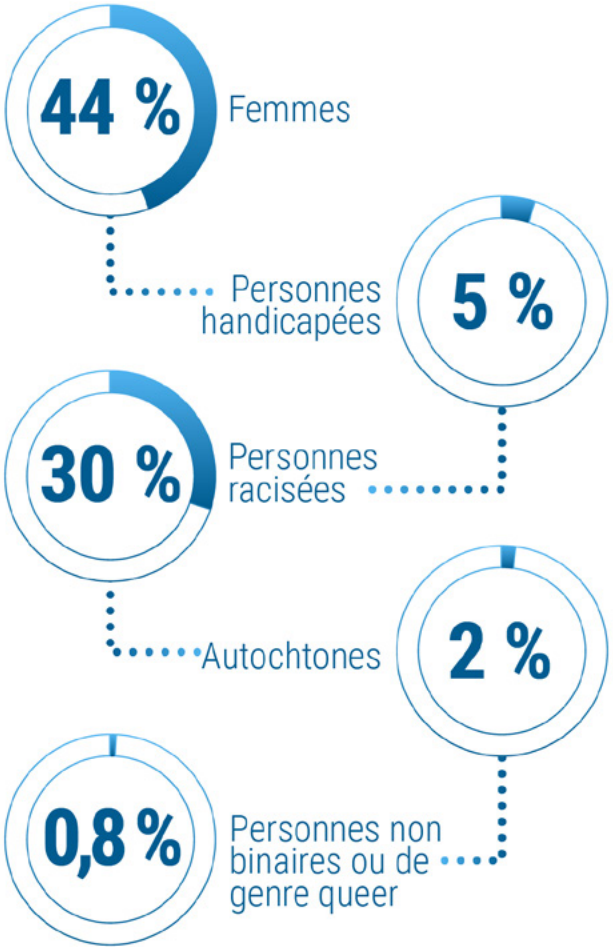
Données démographiques de l'effectif du CST pour 2022 à 2024[101] [102]



Autodéclaration des personnes nouvellement embauchées

Pour la première fois, le CST a pu recueillir une bonne quantité de données d'autodéclaration auprès des personnes nouvellement embauchées, et ces données fournissent des informations précieuses. Les données montrent que l'embauche de femmes, d'Autochtones et de personnes racisées dépassait la disponibilité au sein de la population active.

Taux d'embauche de 2023 à 2024[103]



Le CST reconnaît l'importance des données comme outil appuyant la croissance et l'augmentation de la représentativité au sein de l'effectif. Il s'efforce d'améliorer ses processus de collecte de données internes et externes, de sorte à pouvoir analyser les données désagrégées et à améliorer ses rapports. Ces initiatives lui permettent d'évaluer l'état de la situation actuelle, d'éclairer ses plans et de faire le suivi de ses efforts.

Milieu de travail hybride

À la suite d'un projet pilote fructueux, le CST a officiellement adopté un modèle de travail hybride en avril 2023 et la plupart des membres du personnel travaillent sur place au moins trois jours par semaine. Le CST demeure déterminé à assurer le succès du modèle de travail hybride et à offrir des modalités de travail souples pour appuyer son personnel et la future croissance de l'effectif.

Les personnes qui ont un travail classifié à l'appui de la mission du CST continuent de travailler sur place à temps plein.

Processus de sécurité

Au cours de la dernière année, l'équipe de Sécurité du CST a poursuivi ses consultations auprès des partenaires internes, y compris les groupes d'affinité du personnel. L'objectif de ces consultations est de trouver des façons d'accroître l'inclusion et la transparence dans le processus de sécurité, tout en maintenant son intégrité.

Ces efforts ont mené à l'approbation de deux principaux changements au processus d'embauche externe et d'habilitation de sécurité du CST en septembre 2023.

Exceptions à l'exigence de résidence canadienne

Auparavant, le CST exigeait qu'une candidate ou un candidat ait 10 ans de résidence au Canada pour obtenir une cote de sécurité Très secret approfondie. Conformément à la nouvelle politique, la dirigeante principale ou le dirigeant principal de la sécurité du CST peut accorder une exception aux personnes pour lesquelles les risques sont atténués par d'autres pratiques en place. Ce changement vise à éliminer certains des obstacles systémiques touchant les groupes sous-représentés et ainsi à faciliter le recrutement de personnes qualifiées provenant de groupes diversifiés.

Politique officielle concernant l'utilisation de drogues illicites

Le CST a clarifié, sur son site Web et les formulaires et documents connexes, que les candidates et candidats doivent s'abstenir de consommer des drogues illicites ou de faire un mauvais usage de médicaments d'ordonnance pendant au moins un an avant de présenter leur candidature au CST. Il faut également qu'ils s'en abstiennent pendant les processus d'évaluation et d'habilitation de sécurité. Ce changement vise à accroître la transparence quant au processus de sécurité en énonçant clairement les attentes en la matière.

Équité, diversité et inclusion

Depuis le lancement d'Un CST intégré : Un cadre pour l'équité, la diversité et l'inclusion[104] (EDI), le CST continue d'examiner la signification de l'EDI pour l'organisme et a trouvé de nouvelles façons d'améliorer son milieu de travail pour tout le monde.

Un CST intégré : la collection

En juin 2023, anniversaire du cadre pour l'EDI, le CST a poussé encore plus loin ses efforts en lançant le jeu *Un CST intégré : la collection*.

Le jeu *Un CST intégré : la collection* est une initiative qui encourage l'ensemble du CST à appuyer activement l'EDI dans le milieu de travail. Ce jeu virtuel reprend les principaux principes et éléments stratégiques qui se trouvent dans le cadre sous forme de « cartes » que les employées et employés peuvent jouer pour faire remporter des points à leur secteur d'activités. Les cartes présentent des exemples concrets d'actions que peuvent prendre les membres du personnel pour intégrer l'EDI dans le travail et la culture de l'organisme.

Jusqu'à présent, près du quart des employées et employés du CST ont participé au jeu et toutes les cartes ont été jouées au moins une fois.

Exemples de cartes du jeu Un CST intégré : la collection

Abeille dorée

Elle peut être jouée par une personne qui a contribué à la mission d'EDI de son secteur d'activités.

Coffre au trésor

Elle peut être jouée par une personne qui a créé un outil ou une ressource qui favorise l'EDI au CST.

Chuilà, l'assistance

Elle peut être jouée par une personne qui a participé à un événement organisé par un groupe d'affinité.

Microaffirmation

Elle peut être jouée par une personne qui souhaite reconnaître une autre personne qui a posé au moins un geste ou acte subtil d'inclusion.

Sommet de l'équité, de la diversité et de l'inclusion de la collectivité des cinq

En mars 2024, le CST a organisé le tout premier Sommet de l'EDI de la collectivité des cinq à son bureau principal à Ottawa. Il y a eu 113 participantes et participants, y compris des représentantes et représentants des organismes partenaires de l'Australie, du Royaume-Uni et des États-Unis.

Le sommet représentait une occasion pour les participantes et participants de collaborer sur cinq principaux sujets émergents, dont :

- bâtir la confiance et renforcer les liens chez les leaders;
- lutter contre les barrières qui limitent le recrutement et le maintien en poste du personnel;
- soutenir les espaces sûrs;
- promouvoir l'excellence et l'inclusivité dans le champ de la mission;
- intégrer les considérations en matière d'EDI dans les processus organisationnels.

Le sommet a également présenté des conférencières et conférenciers invités et des panels pour discuter de divers sujets, notamment les questions autochtones au Canada, l'accessibilité, l'EDI et la mission, ainsi que le fait d'être une ou un allié.

Du sommet ont découlé un ensemble exhaustif de recommandations, d'idées, de pratiques exemplaires et d'objectifs stratégiques qui éclaireront la voie collective à suivre pour favoriser des partenariats efficaces au sein de la collectivité des cinq.

Réconciliation avec les peuples autochtones

Le CST a une responsabilité envers la réconciliation avec les peuples autochtones dans le cadre de l'appel à l'action de la Commission de vérité et réconciliation[105]. C'est l'un des principaux principes du cadre pour l'EDI que le CST s'efforce de promouvoir.

Afin d'appuyer son engagement, cette année, le CST a :

- fait l'acquisition de six œuvres d'art auprès d'artistes autochtones et les a affichées bien en vue à côté d'un texte permanent de reconnaissance des territoires à l'édifice Edward-Drake;
- organisé des événements d'éducation pour le personnel sur les expériences et la culture des peuples autochtones et l'appel à l'action;
- embauché une première personne par l'entremise du Programme d'apprentissage en TI pour les personnes autochtones[106];
- lancé un processus d'embauche d'une navigatrice ou d'un navigateur de carrière autochtone en partenariat avec le Cercle du savoir sur l'inclusion autochtone[107];
- accordé plus de 5 % de la valeur totale des contrats d'approvisionnement du CST à des entreprises autochtones (ce qui excède l'exigence fixée par la *Directive sur la gestion de l'approvisionnement* du SCT);
- favorisé la cyberrésilience par l'entremise du Centre pour la cybersécurité en collaboration avec les leaders et les communautés autochtones.

Programme pilote de parrainage

Le programme pilote de parrainage du CST a pris fin en mars 2024. Au cours de l'année, 15 participantes et participants (les protégées et protégés) provenant des communautés noires, autochtones et racisées ont eu des occasions pour :

- créer des liens avec leur parrain ou marraine;
- se faire encadrer;
- explorer des façons de faire progresser leur carrière.

À la fin du projet pilote, plus de la moitié des protégées et protégés avaient atteint les objectifs de leur programme. Ces objectifs portaient sur une combinaison de promotions, de déplacements latéraux et d'accès à la formation linguistique qui aideront les participantes et participants à passer à l'étape supérieure de leur carrière. Le CST envisage maintenant des façons d'établir le parrainage comme initiative organisationnelle et d'étendre le programme à d'autres communautés.

« Le programme de parrainage est arrivé au moment où je commençais à perdre espoir. Je ne sentais pas que j'allais progresser dans ma carrière, car, malgré mes compétences et mon expérience professionnelle, je n'avais personne en position d'autorité pour défendre mes intérêts. Grâce à ce programme, j'ai eu de nouvelles occasions et une plus grande visibilité, en plus d'avoir appris à connaître une marraine qui se souciait réellement de ma personne et de ma progression de carrière. Je suis reconnaissante de cette occasion précieuse qui m'a été accordée en tant que femme marginalisée. »

- Nora (elle), employée du CST et participante du programme de parrainage

« On me demande pourquoi je participe au programme, et c'est simplement parce que d'autres personnes m'ont tellement aidé dans ma carrière que je veux redonner aux autres. Rencontrer des gens qui ont des histoires captivantes et qui ont été confrontés à autant d'obstacles, écouter leurs idées et voir leur énergie… C'est une expérience gratifiante! Quand on redonne, on reçoit beaucoup en retour aussi. »

- Darrell Schroer (il), cadre champion du programme pilote de parrainage du CST et parrain

Améliorer l'accessibilité au CST

En décembre 2023, le CST a publié le Rapport d'étape 2023 sur le Plan d'accessibilité du CST[108].

Ce rapport a été publié conformément aux engagements énoncés dans le Plan d'accessibilité 2022-2025 du CST[109]. Son objectif est de souligner les efforts réalisés pendant l'année, en vue de cerner et d'éliminer les obstacles à l'accessibilité et à l'inclusion.

Il s'agit d'un premier rapport et d'autres suivront. Le CST continuera de veiller à ce que ses espaces, ses outils, ses systèmes et ses processus soient accessibles, de sorte que personne ne soit laissé de côté.

Nouveaux groupes d'affinité

Les groupes d'affinité jouent un rôle essentiel au CST afin d'appuyer les efforts en matière d'EDI et de défendre les intérêts des différentes communautés. Cette année, cinq nouveaux groupes ont été créés :

- Groupe d'affinité des minorités audibles
- Cercle des employées et employés noirs (CEN)
- Cercle des transmetteurs en code (groupe d'affinité autochtone)
- Groupe Moyen-Orient et de l'Afrique du Nord (MENA)
- Groupe d'affinité musulman

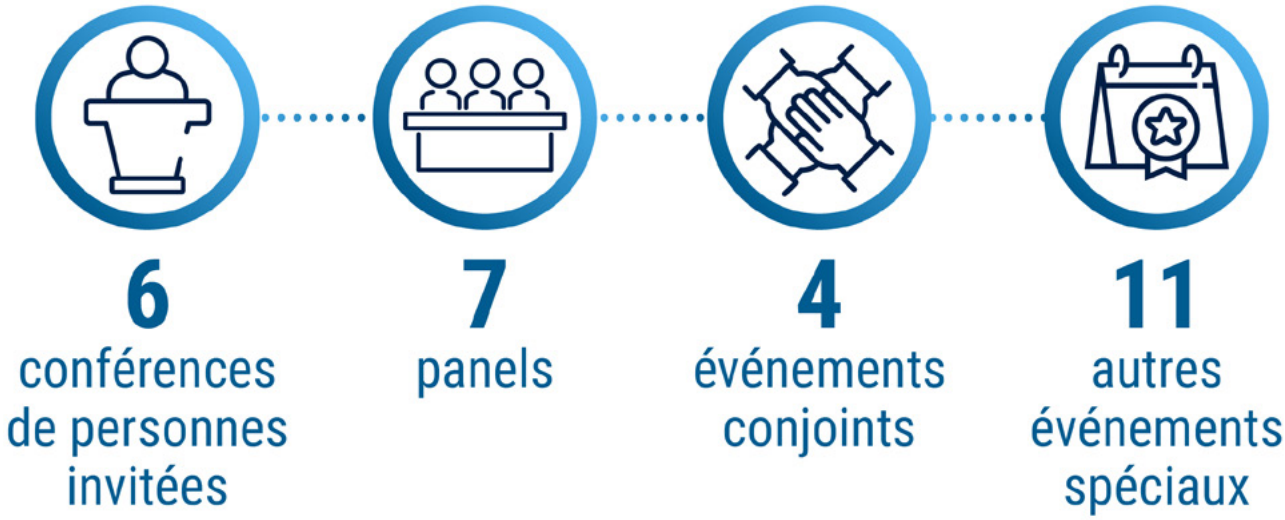
Ces groupes offrent aux employées et employés un endroit sûr où ils peuvent échanger à propos de leurs expériences et contribuer à façonner des politiques et des initiatives au CST. Pendant l'année, les groupes ont organisé des événements afin de sensibiliser le personnel à leurs réalités et de favoriser un milieu de travail inclusif.

Apprenez-en plus sur les groupes d'affinité[110] sur le site Web.

Commémorations et événements liés à l'EDI

Pendant l'année, le CST a organisé 28 événements et commémorations afin de sensibiliser le personnel sur des questions liées à l'EDI et de reconnaître des journées importantes. Les groupes d'affinité ont dirigé et organisé un grand nombre de ces événements, souvent en collaboration avec des partenaires au Canada et à l'étranger afin de joindre un plus grand public.

Types de commémorations et d'événements organisés de 2023 à 2024



Cérémonie de citoyenneté

En octobre 2023, le CST et Immigration, Réfugiés et Citoyenneté Canada ont organisé une cérémonie de citoyenneté à l'édifice de Vanier. Au cours de la cérémonie, 45 Néo-Canadiennes et Néo-Canadiens, originaires de 14 pays différents, ont prêté le serment de citoyenneté. Le ministre de la Défense nationale y a prononcé un discours afin d'accueillir officiellement les nouvelles citoyennes et les nouveaux citoyens du Canada. Il s'agissait de la première fois que des membres du public sans lien avec nos activités étaient invitées et invités dans les installations du CST. Il s'agit d'un jalon capital dans nos efforts visant à faire du CST un organisme plus ouvert, inclusif et transparent.

Nouvelle salle de toilettes neutres

En janvier 2024, le CST a ouvert sa première salle de toilettes neutres à l'édifice Edward-Drake. L'espace existant a été rénové afin d'installer des cabines allant du sol au plafond, des miroirs privés et des indications quant à l'inclusivité. La présence d'une salle de toilettes neutres à son bureau principal permet au CST de faire un pas important afin de créer des espaces accueillants pour tout son personnel.

> **« Plus précisément, c'est la communauté transgenre et non binaire qui est la plus touchée. Ces toilettes nous permettent de les utiliser librement sans craindre de subir des représailles, voire d'être démasquées ou démasqués, comme c'est le cas dans les toilettes plus traditionnelles. »**
>
> - Membre du Réseau de la fierté du CST

Langues officielles

Le CST a continué d'encourager la dualité linguistique et les langues officielles (LO) au travail dans le cadre de plusieurs initiatives, comme :

- communiquer des pratiques exemplaires en matière de LO avec le personnel;
- offrir de la formation aux nouvelles et nouveaux superviseurs sur leurs obligations en matière de LO;
- ajouter des attentes en matière de LO dans les ententes de rendement;
- passer en revue toutes les identifications linguistiques des postes afin d'en assurer l'exactitude et la conformité;
- soutenir les activités du groupe d'affinité du Réseau franco.

Cette année, l'équipe interne de services linguistiques du CST a traduit plus de 3,1 millions de mots et a veillé à ce que toutes les communications et les rapports de l'organisme respectent les exigences en matière de langue officielle. Parmi les cartes du jeu *Un CST intégré : la collection* se trouvaient trois cartes concernant les LO afin d'encourager le personnel à utiliser davantage sa seconde langue officielle au quotidien.

Bien-être du personnel

Le Programme de mieux-être des employées et employés et de l'organisme propose du soutien et les ressources nécessaires pour prospérer aux membres du personnel et aux leaders.

Nouvelle stratégie en matière de santé mentale

Cette année, le CST a créé un plan pluriannuel axé sur la santé mentale des employées et employés ainsi que le bien-être organisationnel. Le plan détaille une série d'objectifs et d'activités dont la mise au point se poursuivra dans la prochaine année.

Cette année, le CST a également mis en œuvre des initiatives visant à :

- sensibiliser;
- appuyer les membres du personnel pour qu'elles et ils prennent soin de leur santé mentale;
- offrir de la formation sur la santé mentale aux leaders.

L'équipe des Services d'orientation professionnelle a continué d'offrir des programmes de perfectionnement psychométrique et d'encadrement aux employées et employés ainsi qu'aux leaders. Il y a entre autres eu un programme d'intelligence émotionnelle, qui joue un rôle crucial dans la prise de conscience de soi et la compréhension des autres.

Prévention du harcèlement et de la violence

Cette année, le Programme de prévention du harcèlement et de la violence a lancé plusieurs initiatives ayant pour but d'appuyer le mieux-être du personnel, y compris des initiatives visant à :

- établir, des lignes directrices liées à la lutte contre la violence familiale en milieu de travail;
- créer une trousse de prévention du harcèlement et de la violence à l'intention des gestionnaires;
- offrir de la formation sur l'intervention des témoins en milieu de travail à l'intention de tout le personnel.

Espace de traitement et de ressourcement

La nature du travail au CST expose certaines et certains employés à du matériel et à des images qui peuvent être difficiles à gérer et à traiter. Afin d'aider ces personnes à préserver une bonne santé mentale et un bon rendement, le CST a créé un espace de traitement et de ressourcement à son bureau principal de l'édifice Edward-Drake.

Dans cet espace, les employées et employés ont accès à des activités, à des ressources et à des outils éprouvés qui atténuent les effets de l'exposition à du matériel perturbant. C'est un endroit sûr où les membres du personnel peuvent s'éloigner de leur poste de travail pour refaire le plein d'énergie et décompresser.

Prix des meilleurs employeurs

Le CST était fier d'être à nouveau reconnu comme un des meilleurs employeurs pour les jeunes canadiens[111] (2024) et d'être nommé comme l'un des meilleurs employeurs de la région de la capitale nationale[112] (2024).

Principaux chiffres

Au cours de l'année 2023 à 2024, le CST :

- a produit 3 142 rapports de renseignement étranger;
- a divulgué 8 vulnérabilités aux fournisseurs touchés;
- a approuvé 43 demandes d'assistance de partenaires fédéraux;
- a contribué à 26 examens externes et rapports;
- a répondu à 96 % des questions posées dans le cadre d'examen dans les délais impartis;
- a traduit 3 infographies de Pensez cybersécurité en 4 langues autochtones;
- a fait 5 580 publications sur les médias sociaux;
- a accru son effectif de 9 %.

Le Centre pour la cybersécurité :

- a bloqué 6,6 millions d'activités potentiellement malveillantes par jour;
- a pris des mesures contre près de 300 000 domaines malveillants;
- a échangé avec près de 1 900 organisations canadiennes en charge d'infrastructures essentielles;
- a analysé plus de 1 milliard de fichiers suspects pour détecter les maliciels;
- a communiqué 84 indicateurs de compromission uniques par jour;
- a appuyé l'intervention lors de 2 192 cyberincidents;
- a utilisé des capteurs pour protéger les réseaux du trois quarts des institutions fédérales;
- a publié :
  - → 4 évaluations des menaces,
  - → 34 nouvelles publications d'orientation sur la cybersécurité,
  - → 40 nouvelles ressources de Pensez cybersécurité,
  - → 250 notifications de signes avant-coureurs d'une attaque par rançongiciel,
  - → 779 avis,
  - → 20 alertes,
  - → 10 cyberflashs.

Notes en fin de texte

1 https://laws-lois.justice.gc.ca/fra/lois/c-35.3/page-1.html#h-1170321

2 Les autorités totales du CST pour 2023 à 2024 ont atteint 1 039 192 674 $.

3 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023

4 https://www.canada.ca/fr/institutions-democratiques/services/rapports/premier-rapport-david-johnston-rapporteur-special-independent-ingerence-etrangere.html

5 Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR). « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques ». 2022. https://nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-fr.pdf

6 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-secteur-petrolier-gazier-canada

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

8 https://www.cga.ca/e-stac/ (en anglais seulement)

9 Ministère de la Défense nationale. « Discours de la ministre Anand à l'occasion de CANSEC 2023 ». Le 5 juin 2023. https://www.canada.ca/fr/ministere-defense-nationale/nouvelles/2023/06/discours-du-ministre-anand-a-loccasion-de-cansec-2023.html

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

11 https://www.cyber.gc.ca/fr/outils-services/howler

12 https://www.cyber.gc.ca/fr/glossaire#c

13 https://www.cyber.gc.ca/fr/nouvelles-evenements

14 https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-International-Partnerships.pdf (en anglais seulement)

15 https://www.first.org/conference/2023/ (en anglais seulement)

16 https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage

17 https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage/cours/623-introduction-cybersecurite-professionnels-professionnelles-leducation

18 https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage/cours/625-cybersecurite-pour-petites-moyen-entreprises

19 https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage/cours/107-principes-fondamentaux-cybersecurite

20 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023

21 Institutions démocratiques. « Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections - Rapports et publications ». 2024. https://www.canada.ca/fr/institutions-democratiques/services/rapports.html

22 SCRS. Menaces d'ingérence étrangère visant les processus démocratiques du Canada. 2021. https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/menace-dingerence-etrangere-visant-les-processus-democratiques-du-canada.html

23 https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024#a10

24 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023#generative_ai

25 https://youtu.be/3ZOy8UtBlYk?si=5M9gkxgX-EHRzSka

26 https://www.canada.ca/fr/campagne/desinformation-enligne.html#1

27 Centre canadien pour la cybersécurité. « Évaluation des cybermenaces nationales 2023-2024 ». Octobre 2023. https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

28 https://www.cyber.gc.ca/fr/nouvelles-evenements/cst-centre-canadien-cybersecurite-publient-bulletin-cybermenace-parrainee-republique-populaire-chine

29 https://www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-conjoint-auteures-menace-parrainees-rpc-compromettant-infrastructures-essentielles-americaines-etablir-acces-permanent-conseils-identifier-attenuer-attaques-hors-sol

30 https://www.cyber.gc.ca/fr/nouvelles-evenements/conseils-lintention-cadres-superieurs-chefs-dorganisations-liees-infrastructures-essentielles-protection-infrastructures-fonctions-essentielles-contre-cyberactivites-menees-rpc

31 https://www.canada.ca/fr/securite-telecommunications/nouvelles/2023/04/declaration-de-la-ministre-de-la-defense-nationale--cybermenaces-ciblant-les-infrastructures-essentielles.html

32 https://www.cse-cst.gc.ca/fr/ressources-information/annonces/cst-exhorte-collectivite-canadienne-cybersecurite-redoubler-vigilance

33 https://www.cyber.gc.ca/fr/nouvelles-evenements/cst-exhorte-collectivite-canadienne-cybersecurite-etre-vigilante-loccasion-deuxieme-anniversaire-linvasion-massive-lukraine-russie

34 https://www.cse-cst.gc.ca/fr/ressources-information/nouvelles/bulletin-cybersecurite-conjoint-signaler-campagnes-harponnage-contre-cibles-dinteret-lechelle-mondiale

35 https://www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-cybersecurite-conjoint-visant-signaler-que-auteures-auteurs-menace-russie-adaptaient-tactiques-acceder-linfrastructure-infonuagique

36 https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/recherche-technologies-sensibles-affiliations-preoccupantes/politique-recherche-technologies-sensibles-affiliations-preoccupantes

37 Relations Couronne-Autochtones et Affaires du Nord Canada. « Cadre stratégique pour l'Arctique et le Nord : Chapitre sur la sécurité et la défense ». Septembre 2019. https://www.rcaanc-cirnac.gc.ca/fra/1562939617400/1562939658000

38 Ministère de la Défense nationale. « Déclaration des Forces armées canadiennes concernant l'interception non sécuritaire d'un hélicoptère de l'Aviation royale canadienne ». Le 3 novembre 2023.https://www.canada.ca/fr/ministere-defense-nationale/nouvelles/2023/11/declaration-des-forces-armees-canadiennes-concernant-linterception-non-securitaire-dun-helicoptere-de-laviation-royale-canadienne.html

39 Centre canadien pour la cybersécurité. « Bulletin conjoint sur des auteures et auteurs de menace parrainés par la RPC compromettant les infrastructures essentielles américaines pour établir un accès permanent, et conseils pour identifier et atténuer les attaques hors sol ». Le 7 février 2024. https://www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-conjoint-auteures-menace-parrainees-rpc-compromettant-infrastructures-essentielles-americaines-etablir-acces-permanent-conseils-identifier-attenuer-attaques-hors-sol

40 Affaires mondiales Canada. « Déclaration sur les mesures prises par la République populaire de Chine contre des navires philippins en mer de Chine méridionale ». Le 12 décembre 2023. https://www.canada.ca/fr/affaires-mondiales/nouvelles/2023/12/declaration-sur-les-mesures-prises-par-la-republique-populaire-de-chine-contre-des-navires-philippins-en-mer-de-chine-meridionale0.html

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

42 Palo Alto Networks. « 2023 Palo Alto Networks Canada Ransomware Barometer ». Le 7 décembre 2023. https://www.paloaltonetworks.com/content/dam/CF/Canada%20Ransomware%20Whitepaper%202023.pdf (en anglais seulement)

43 Centre canadien pour la cybersécurité. « Évaluation des menaces de base : Cybercriminalité ». Le 28 août 2023. https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite

44 https://www.cyber.gc.ca/fr/contactez-centre-cybersecurite

45 https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite

46 https://www.cyber.gc.ca/fr/orientation/profil-rancongiciel-alphvblackcat

47 https://www.cyber.gc.ca/fr/orientation/profil-rancongiciel-cl0p-ta505

48 https://www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-cybersecurite-conjoint-maliciel-truebot

49 https://www.cyber.gc.ca/fr/nouvelles-evenements/centre-securite-telecommunications-partenaires-internationaux-publient-bulletin-cybersecurite-rancongiciel-lockbit

50 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-secteur-petrolier-gazier-canada

51 https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite

52 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023

53 https://www.cyber.gc.ca/fr/orientation/menace-posee-generateurs-texte-bases-modeles-langage-grande-taille

54 https://www.cyber.gc.ca/fr/orientation

55 https://www.pensezcybersecurite.gc.ca/fr/ressources

56 https://www.pensezcybersecurite.gc.ca/fr/campagnes/cybersecurite-petites-entreprises

57 https://www.pensezcybersecurite.gc.ca/fr/ressources/les-7-signaux-dalarme-de-lhameconnage

58 https://www.pensezcybersecurite.gc.ca/fr/ressources/lauthentification-multifactorielle

59 https://www.pensezcybersecurite.gc.ca/fr/ressources/avez-vous-un-plan-de-sauvegarde-pour-vos-donnees

60 https://www.pensezcybersecurite.gc.ca/fr/ressources/recherche/jeu-questionnaire-cyberforme

61 https://www.pensezcybersecurite.gc.ca/fr/ressources/video-ameliorez-cyberforme

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

63 https://www.pensezcybersecurite.gc.ca/fr/blogues/signaler-messages-textes-indesirables-numero-7726

64 https://www.cira.ca/fr/bouclier-canadien-de-cira/

65 https://www.cyber.gc.ca/fr/education-communaute/collaboration-milieu-education-developpement-cybercompetences/cadre-competences-matiere-cybersecurite-canada

66 https://resources.chatterhigh.com/fr/d%C3%A9couvrir-les-carri%C3%A8res-dans-le-domaine-de-la-cybers%C3%A9curit%C3%A9

67 https://www.cse-cst.gc.ca/fr/cst-crsng-communautes-subvention

68 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/institut-tutte-mathematiques-calcul

69 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/recherche-appliquee

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

71 https://www.cyber.gc.ca/fr/geekweek/geekweek-8

72 https://www.cyber.gc.ca/fr/geekweek

73 https://www.cisa.gov/ (en anglais seulement)

74 https://www.cyber.gc.ca/fr/nouvelles-evenements/grande-exploration

75 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023

76 https://www.cyber.gc.ca/fr/orientation/menace-posee-generateurs-texte-bases-modeles-langage-grande-taille

77 https://www.csps-efpc.gc.ca/video/ai-security-fra.aspx

78 https://www.cyber.gc.ca/fr/orientation/lintelligence-artificielle-generative-itsap00041

79 https://www.cyber.gc.ca/fr/nouvelles-evenements/lignes-directrices-developpement-systemes-dia-securises

80 https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/engaging-with-artificial-intelligence (en anglais seulement)

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

82 https://nsira-ossnr.gc.ca/fr/

83 https://nsicop-cpsnr.ca/index-fr.html

84 https://www.canada.ca/fr/institutions-democratiques/services/rapporteur-special-independant.html

85 https://commissioningerenceetrangere.ca/

86 https://commissioningerenceetrangere.ca/fileadmin/commission_ingerence_etrangere/Documents/Preuves_et_Presentations/Rapports_sommaires_et_institutionnels/CAN.DOC.000006.pdf

87 Centre canadien pour la cybersécurité. « Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023 ». Le 6 décembre 2023. https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023

88 https://laws-lois.justice.gc.ca/fra/lois/c-35.3/page-2.html#docCont

89 https://www.canada.ca/fr/commissaire-renseignement.html

90 Les conditions à respecter pour que le CST divulgue des informations nominatives sur des Canadiennes et Canadiens sont détaillées à la page Protéger l'information nominative sur un Canadien dans le cadre du volet du mandat du CST touchant le renseignement étranger du site Web du CST. https://www.cse-cst.gc.ca/fr/ressources-et-information/fiches-des-renseignements/proteger-linformation-nominative-sur-un#DACRD

91 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/surveillance#DDP

92 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports

93 https://open.canada.ca/fr

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

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

96 https://www.noscommunes.ca/procedure/notre-procedure/questions/c_g_questions-f.html#3

97 https://www.cse-cst.gc.ca/fr/culture-et-communaute/ethique#disclosure

98 https://www.cse-cst.gc.ca/fr/culture-et-communaute/ethique

99 https://www.canada.ca/fr/conseil-prive/services/publications/rapport-equipe-speciale-sous-ministres-valeurs-ethique-adresse-greffier-conseil-prive.html

100 Les chiffres se fondent sur l'autodéclaration volontaire durant le processus de candidature.

101 Les niveaux de référence relatifs à la disponibilité au sein de la population active sont basés sur les données relatives à la disponibilité sur le marché du travail tirées du recensement de 2016 et tiennent compte d'autres critères tels que la citoyenneté, l'emplacement et des comparaisons fondées sur les codes de la Classification nationale des professions.

102 Les données relatives à la disponibilité au sein de la population active pour les groupes 2SLGBTQIA+ n'est pas disponible, étant donné qu'ils ne sont pas désignés comme groupe d'équité en matière d'emploi en vertu de la *Loi sur l'équité en matière d'emploi*.

103 Les chiffres se fondent sur l'autodéclaration volontaire. Ce sont 90 % des personnes nouvellement embauchées de 2023 à 2024 qui ont rempli une autodéclaration.

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

105 https://www.rcaanc-cirnac.gc.ca/fra/1524494530110/1557511412801

106 https://talent.canada.ca/fr/indigenous-it-apprentice

107 https://www.canada.ca/fr/gouvernement/fonctionpublique/mieux-etre-inclusion-diversite-fonction-publique/diversite-equite-matiere-emploi/cercle-savoir.htmll

108 https://www.cse-cst.gc.ca/fr/accessibilite/rapport-detape-2023-plan-daccessibilite-centre-securite-telecommunications

109 https://www.cse-cst.gc.ca/fr/accessibilite/plan-accessibilite-cst-2022-2025

110 https://www.cse-cst.gc.ca/fr/culture-et-communaute/diversite-inclusion/groupes-affinite

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

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