Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

ISSN 2564-0488
CAT D95-11F-PDF

Centre de la sécurité des télécommunications Canada

Rapport annuel 2025–2026

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

Introduction

Depuis 80 ans, le Centre de la sécurité des télécommunications Canada (CST) protège le Canada et les Canadiennes et Canadiens au moyen de son expertise dans le renseignement électromagnétique. À l'instar des technologies, le rôle du CST évolue. Par l'intermédiaire du Centre canadien pour la cybersécurité (Centre pour la cybersécurité), il fournit aujourd'hui des avis et conseils techniques et pratiques qui font autorité pour aider les Canadiennes et Canadiens, les entreprises canadiennes, divers échelons de gouvernement et les infrastructures essentielles à se protéger contre les cybermenaces. Ensemble, ils forment la première ligne de défense numérique du Canada.

Le Canada est à l'ère de concurrence géopolitique féroce et de perturbations technologiques soutenues. Les cybermenaces gagnent en ampleur et en complexité, et les adversaires ciblent de plus en plus les systèmes et les services essentiels dont les Canadiennes et Canadiens dépendent au quotidien. Dans ce contexte, le CST joue un rôle crucial afin de faire progresser les intérêts stratégiques du Canada et de protéger la sécurité, la souveraineté et la prospérité de la nation.

En réponse, le CST a amélioré sa façon de collaborer avec ses partenaires au Canada et ailleurs dans le monde. Il examine les questions communes de sécurité et renforce la résilience et la préparation collectives, en étroite collaboration avec ses partenaires de la collectivité des cinq et ses autres partenaires de confiance. En combinant ses connaissances découlant du renseignement étranger et son expertise en cybersécurité, le CST est bien placé pour détecter les menaces rapidement et proactivement et y répondre rapidement avec précision. L'effectif et les capacités grandissent également pour répondre à la hausse des demandes. Tandis que le gouvernement du Canada fait avancer ses priorités en matière de défense, de sécurité et d'économie, le CST entre dans une ère durable de croissance et de transformation. Elles se veulent le reflet des investissements accrus dans les infrastructures numériques, la cyberdéfense et les technologies émergentes, qui permettent au CST d'établir l'ampleur de ses opérations et d'avoir une incidence marquée sur les Canadiennes et Canadiens.

Cette année fut décisive pour le CST. Il a amélioré ses opérations, ses partenariats et ses capacités pour mieux mener à bien son mandat dans l'environnement mondial de sécurité complexe et contesté. L'organisme vise à accroître l'intégration en réunissant les points de vue diversifiés, en favorisant la créativité et en concertant les efforts pour appuyer la sécurité du Canada aujourd'hui et demain.

Ce rapport non classifié résume les activités entreprises par le CST entre le 1er avril 2025 et le 31 mars 2026. À moins d'indication contraire, « cette année » fait référence à la période visée par le présent rapport.

RENSEIGNEMENT ÉLECTROMAGNÉTIQUE ÉTRANGER	ASSISTANCE OPÉRATIONNELLE ET TECHNIQUE	CYBEROPÉRATIONS ACTIVES	CYBEROPÉRATIONS DÉFENSIVES	CYBERSÉCURITÉ ET ASSURANCE DE L'INFORMATION
Capacité du CST à recueillir du renseignement électromagnétique étranger à l'aide de techniques avancées.	Fournir une assistance aux organismes fédéraux chargés de l'application de la loi et de la sécurité, aux Forces armées canadiennes et au ministère de la Défense nationale.	Contrer les cyberactivités étrangères qui menacent le Canada.	Intervenir en ligne en cas de cybermenaces étrangères visant les réseaux canadiens importants.	Défendre les réseaux canadiens importants.
Acquérir de l'information à partir de l'infrastructure mondiale d'information non canadienne ou par l'entremise de celle-ci, notamment en mobilisant des entités étrangères situées à l'extérieur du Canada ou en interagissant avec celles-ci.	Avoir recours à des techniques avancées pour soutenir les activités de nos partenaires, y compris des cyberopérations dans le cadre de missions autorisées par le gouvernement.	Intervenir en ligne afin de réduire, d'interrompre, d'influencer ou de contrecarrer les cybercapacités et les cyberactivités étrangères dans la mesure où elles se rapportent aux affaires internationales, à la défense ou à la sécurité.	Défendre les systèmes d'importance pour le gouvernement du Canada.	Fournir des avis, des conseils et des services pour protéger les réseaux importants de partout au pays, les institutions fédérales, l'information électronique et les infrastructures d'importance pour le gouvernement du Canada.

Avant-propos du ministre

Le contexte de menace évolue rapidement. En plus des menaces en mer, dans les airs et sur la terre, les adversaires étrangers œuvrent de plus en plus dans le cyberespace. Le monde est plus connecté que jamais, et le Canada doit demeurer vigilant pour défendre ses systèmes et services essentiels, dont les Canadiennes et Canadiens dépendent chaque jour.

Depuis 80 ans, le Centre de la sécurité des télécommunications Canada (CST) joue un rôle clé pour assurer la protection et la sécurité de la population canadienne. En tant qu'organisme national de cryptologie, il conjugue le renseignement électromagnétique étranger, la cybersécurité, les cyberopérations et l'assistance technique et opérationnelle aux partenaires fédéraux. Son expertise et ses capacités combinées sont indispensables pour assurer la sécurité, la souveraineté, la prospérité et la résilience du Canada dans un monde complexe et contesté.

Le présent rapport annuel montre l'ampleur des contributions du CST dans la prise de décision et les opérations du gouvernement. Le CST travaille étroitement avec les Forces armées canadiennes, le ministère de la Défense nationale, la Garde côtière canadienne et d'autres ministères et organismes fédéraux pour appuyer les efforts de défense et de sécurité au pays et ailleurs. Son aide appuie la prise de décision, améliore la préparation et permet à ses partenaires de mener à bien leur mandat dans l'environnement de sécurité qui se complexifie.

En 2025, le gouvernement du Canada a accordé des investissements historiques visant à renforcer la défense nationale et la sécurité, dont une importante part relève du CST. Les capacités du CST aident le Canada à faire progresser ses objectifs de défense et contribuent à ses engagements envers ses alliés. Ces investissements ont permis au Canada d'atteindre l'objectif de dépenses en défense de 2 % de l'Organisation du Traité de l'Atlantique Nord (OTAN) en 2025-2026 et pavent la voie à l'engagement des alliés quant aux investissements en défense de 5 % d'ici 2035.

Les capacités du CST positionnent également le Canada en tant que partenaire fort et fiable à l'échelle mondiale. Son expertise technique, son expérience opérationnelle et ses partenariats de confiance appuient la collaboration internationale en matière de défense, de renseignement et de cybersécurité, notamment par le biais de son partenariat avec les membres de la collectivité des cinq. Ce rôle se traduit dans le mandat du CST par le Centre canadien pour la cybersécurité, qui fournit des conseils importants aux partenaires fédéraux, aux petites et moyennes entreprises, aux secteurs des infrastructures essentielles et aux Canadiennes et Canadiens. En renforçant la sensibilisation, la résilience et la préparation partout au pays, le Centre pour la cybersécurité veille à ce que le Canada soit en position de force.

Derrière tout ce travail, il y a les fonctionnaires qui, chaque jour, consacrent leur expertise et leur dévouement au service de leur pays. Leur travail est souvent accompli en arrière-plan, mais il touche tous les échelons de gouvernement d'un bout à l'autre du pays. Je suis reconnaissant de leur service continu et du rôle important qu'elles et ils jouent pour protéger le Canada d'aujourd'hui et de demain.

L'honorable David J. McGuinty (il)
Ministre de la Défense nationale

Message de la chef

Je suis heureuse de présenter ce rapport annuel aux Canadiennes et Canadiens à la suite d'une année importante pour le CST dans une période d'instabilité et de changements considérables dans le monde.

L'environnement de sécurité auquel est confronté le Canada s'est complexifié. Les cyberopérations contre les infrastructures essentielles, les campagnes de désinformation contre les institutions démocratiques et la sophistication accrue des adversaires qui prennent pour cible les intérêts du Canada mettent en évidence le besoin de continuer à faire preuve de vigilance et de prendre des mesures.

Ces menaces ne cessent pas à la nuit tombée, en cas de mauvais temps ou pendant les jours fériés. Au fur et à mesure que l'intérêt envers nos biens numériques croît, le mandat du CST continue sans arrêt, sur tous fuseaux horaires, chaque jour de l'année, et ce, afin de renforcer la posture de cybersécurité du Canada et d'anticiper les attaques contre notre pays. Nous avons une motivation qui nous est propre : nous sommes la première ligne de défense numérique du Canada.

Dans le budget 2025, le gouvernement du Canada a accordé des investissements historiques en défense qui montrent la confiance accordée aux capacités du CST et à son important travail dans la sécurité du Canada. Ce rapport présente comment le CST met cette confiance au service de la sécurité, des intérêts stratégiques et de la prospérité du Canada.

L'année 2025 en était une de progrès pour le CST. Nous avons fait avancer le travail qui appuie l'engagement du Canada envers les cibles de dépense en défense de l'Organisation du Traité de l'Atlantique Nord, avons concrétisé les investissements majeurs en actions et avons renforcé les capacités et les partenariats qui soutiennent la sécurité du Canada. Dans tous les volets de notre mandat, nous avons continué de lier le renseignement aux opérations et de traduire les observations en actions, au moyen d'une intégration rapprochée entre le renseignement étranger, la cybersécurité et les cyberopérations. Cette approche intégrée accroît l'autonomie du Canada dans le domaine numérique et sous-tend les efforts élargis de sécurité en Amérique du Nord, qui s'étendent aux systèmes de sécurité du Nord et de l'Arctique canadiens, tout en renforçant les relations avec les communautés autochtones, les premiers gardiens de ces terres. Partout où des progrès ont été réalisés, nous visons désormais à poursuivre ces efforts avec rigueur, ambition et une orientation stratégique claire au service de la population canadienne.

Les opérations de renseignement électromagnétique étranger du CST appuient son importante mission visant à défendre la sécurité nationale du Canada, tout en protégeant l'information du gouvernement du Canada. Cette responsabilité donne lieu à notre soutien envers l'industrie et le milieu universitaire au Canada et envers nos alliés d'ailleurs dans le monde qui ont le même mandat de sécurité et de cybersécurité. Cette année, nous avons également accru notre utilisation de l'intelligence artificielle de façon responsable pour améliorer les efforts dans le cadre de notre mission. Elle a aidé les membres du personnel à analyser efficacement les données complexes, a accéléré la prise de décisions et a renforcé les mesures de cyberdéfense contre des menaces plus sophistiquées que jamais.

En parallèle, nos chercheuses et chercheurs apportent des contributions à la collectivité de source ouverte et au milieu universitaire, qui permet au CST de se tailler une place de choix dans le domaine de l'innovation en cybersécurité. Nous continuons de croître en élargissant les partenariats avec le secteur privé, les communautés autochtones et les organisations internationales, afin d'améliorer la résilience à long terme du Canada et d'établir les fondements des futures générations de talents en cybersécurité.

En plus d'exiger de la rapidité et de la souplesse, notre mission demande aussi de la confiance. C'est pourquoi le CST est déterminé à demeurer transparent et responsable. C'est notre fierté d'œuvrer sous le regard d'organes d'examens externes et indépendants qui nous soumettent à des normes élevées. Nous améliorons continuellement les cadres de conformité pour tenir compte de l'évolution constante de notre travail et des technologies que nous utilisons.

Cette année, le CST célèbre 80 années de service. Notre mission première n'a pas changé : analyser les menaces, protéger les infrastructures numériques, soutenir les opérations militaires canadiennes et les partenaires du domaine de la sécurité et, plus important encore, protéger les Canadiennes et Canadiens.

Au cours de ces huit décennies, c'est notre effectif qui a eu le plus grand effet positif, lui qui est composé de personnes ayant des expériences, des expertises et des points de vue diversifiés, mais qui partage une même mission. Le CST est déterminé à éliminer les obstacles en milieu de travail et à favoriser un environnement où chaque personne peut pleinement contribuer et s'épanouir. La diversité de l'effectif est essentielle pour assurer l'excellence opérationnelle. Toutes les formes de diversité sont un atout pour la mission, car elles amplifient notre capacité à anticiper les menaces, éliminent les angles morts, résolvent des problèmes complexes et produisent des résultats pour les Canadiennes et Canadiens.

Le regard orienté vers son prochain chapitre, le CST se concentre sur le renforcement des fondements numériques qui sous-tendent la sécurité et la résilience du Canada. Notre travail contribue au fonctionnement, à la croissance et à la protection du pays dans le monde numérique en évolution. Au fur et à mesure que le contexte mondial évolue, le CST s'adaptera pour que le Canada soit prêt à relever les défis émergents en toute confiance. Il le fera en tant qu'un CST intégré.

Caroline Xavier (elle)
Chef du CST

Faits saillants en 2025-2026

L'effectif en 2025-2026

Effectif total	4 178[1]
Taux d'attrition	2,8 %[2]
Augmentation de l'effectif	337 (8,1 %)
Représentation au sein de l'effectif (par auto-identification)	
↳ Femmes	33,9 %
↳ Personnes handicapées	14,1 %
↳ Personnes racisées	17,9 %
↳ Autochtones	2,6 %
↳ Personnes 2ELGBTQIA+	6,4 %

Alertes et notifications émises pour protéger contre les activités malveillantes en 2025-2026

Demandes générales reçues par le Centre pour la cybersécurité	14 700 (augmentation de 9 %)
Interventions aux incidents de cybersécurité	
↳ Gouvernement du Canada	1 528
↳ Entités canadiennes	1 688
De ces 3 216 incidents	
↳ le Centre pour la cybersécurité a avisé l'organisation et offert du soutien dans	2 282 cas (1 094 touchant des institutions fédérales; 1 188 touchant des entités canadiennes)
↳ le Centre pour la cybersécurité a reçu des rapports d'incidents et offert du soutien dans	934 case (434 provenant d'institutions fédérales; 500 provenant d'entités canadiennes)
Alertes du Centre pour la cybersécurité	25
Avis du Centre pour la cybersécurité	995
Notifications de signes avant-coureurs d'une attaque par rançongiciel	67 notifications envoyées à 67 organisations canadiennes
Alertes du Système national de notification de cybermenace (SNNC)	Plus de 97 000 alertes de sécurité envoyée à 1 363 organisations inscrites
Évaluations des risques liés à la chaîne d'approvisionnement	1 772

Renseignement électromagnétique étranger en 2025-2026

Rapports	3 976
Ministères clients	30
Clientes et clients particuliers	3 332
Demandes d'assistance	55

Rapports, publications et conseils diffusés en 2025-2026

Documents d'orientation sur la cybersécurité	41
Publications conjointes	28
Bulletins et évaluations de menaces non classifiés	7

Interactions avec d'autres ministères et des industries des infrastructures essentielles en 2025-2026

Réunions avec des partenaires des infrastructures essentielles	522
Présentations	120
Kiosques du Centre pour la cybersécurité	5
Séances d'information sur la préparation à la menace que l'informatique quantique fait peser sur la cryptographie	13
Exercices de simulation	4
Séances d'information bimensuelles sur les menaces pour les professionnelles et professionnels de la sécurité des technologies de l'information (TI)	23
Séances « Passons à l'action »	8

Interactions avec le public et les médias en 2025-2026

Demandes des médias	169
Entrevues	20
Conférences de presse nationales	6
Témoignages devant un comité parlementaire	11
Réponses aux questions inscrites au Feuilleton	97
Inscriptions aux cours offerts par le Carrefour de l'apprentissage	6 585

[1] Ce chiffre inclut les emplois d'une durée indéterminée, déterminée ou occasionnelle, à temps plein ou à temps partiel.
[2] Ce chiffre n'inclut pas les emplois d'une durée déterminée et les départs à la retraite.

Responsabilisation, transparence et conformité en 2025-2026

Autorisations ministérielles	
↳ Par l'entremise du commissaire au renseignement	9
↳ Pour mener des cyberopérations étrangères	4
Arrêtés ministériels en vigueur	6
Directives ministérielles	1
Examens externes	
↳ Collaborations aux examens et aux rapports	26
↳ Séances d'information offertes aux organes d'examen	24
↳ Réponses aux questions	454
Incidents de conformité opérationnelle	
↳ Concernant de l'information qui se rapporte à une Canadienne ou à un Canadien	186
↳ Ne concernant pas de l'information qui se rapporte à une Canadienne ou à un Canadien	14
Plaintes externes	
↳ Transmises à la chef du CST	7
↳ Transmises à l'OSSNR	Aucune
Téléversements sur le portail du gouvernement ouvert	
↳ Ensembles de données	5
↳ Ressources informationnelles	56
Demandes présentées en vertu de la *Loi sur l'accès à l'information*	85
Divulgations proactives	4 cahiers de comité
Documents déposés	3
Audits internes	
↳ Audits d'assurance	3
↳ Audits consultatifs	1

LA PREMIÈRE LIGNE DE DÉFENSE NUMÉRIQUE DU CANADA

Le contexte mondial de sécurité évolue rapidement, en fonction de l'instabilité géopolitique, des nouvelles formes de conflit et de l'accélération des changements technologiques. Ces dynamiques redéfinissent la façon dont les États se font concurrence, collaborent et protègent leurs intérêts.

Le CST ajuste ses opérations en conséquence de l'intensification de ces pressions. Grâce à des investissements historiques en défense en 2025, le CST fortifie la première ligne de défense numérique et les avantages stratégiques du Canada en intégrant le renseignement aux cyberopérations et en collaborant étroitement avec ses partenaires au pays et à l'étranger.

C'est dans ce contexte que le CST joue un rôle essentiel dans la protection de la population, des infrastructures et de la souveraineté canadiennes. Le renseignement électromagnétique étranger est l'un des principaux actifs de sécurité nationale du pays, car il fournit de l'information opportune et des signes avant-coureurs qui appuient la prise de décisions et de mesures efficaces contre les menaces émergentes.

Afin de mener à bien son mandat, le CST travaille étroitement avec ses partenaires du gouvernement du Canada et de la collectivité des cinq et ses alliés internationaux de confiance.

Il se concentre sur les priorités qui importent le plus pour le Canada et ses alliés, dont la protection de l'Arctique, la lutte contre l'ingérence étrangère et l'élargissement des opérations de cyberdéfense.

Ensemble, le CST et ses partenaires réduisent les risques, améliorent la résilience et aident à faire en sorte que les Canadiennes et Canadiens puissent se fier à des services sécurisés et ininterrompus dans un monde toujours plus numérique.

Le CST se concentre sur la création de capacités qui définiront la sécurité numérique du Canada dans les prochaines années, notamment l'intelligence artificielle (IA), la cryptographie post-quantique et l'approfondissement des partenariats avec les secteurs public et privé, y compris divers partenaires étrangers. Il s'agit d'une vision à long terme vers un Canada numérique sécurisé, résilient et souverain.

Détecter, perturber et dissuader les menaces étrangères et s'en protéger

Le CST ne travaille pas en vase clos. Ses opérations sont explicitement autorisées par la *Loi sur le CST* et sont guidées par les priorités du Canada en matière de renseignement, lesquelles font office de plan opérationnel et garantissent que le travail du CST répond directement aux intérêts de la nation.

Le renseignement électromagnétique (SIGINT pour *Signals Intelligence*) étranger est au cœur du mandat du CST. Il lui permet de comprendre les menaces étrangères et d'offrir des avis stratégiques en appui à la prise de décision du gouvernement sans cibler les Canadiennes et Canadiens ou les personnes se trouvant au Canada. Ce renseignement soutient directement les intérêts du Canada en matière de sécurité, de défense et de prospérité économique dans un environnement complexe et en constante évolution.

Le SIGINT a considérablement changé en 80 ans. Au lendemain de la Seconde Guerre mondiale, les efforts liés au SIGINT se concentraient sur l'interception de signaux radio et le décryptage de dispositifs électromécaniques. Les puissantes capacités SIGINT actuelles sont utilisées pour intercepter, décrypter et analyser les communications électroniques et les signaux numériques dans l'infrastructure mondiale de l'information (IMI) au moyen de techniques sophistiquées et classifiées. Le CST continue d'investir dans de nouvelles capacités et intègre de plus en plus l'IA afin de transformer la détection des menaces étrangères et l'intervention.

Cyberopérations étrangères

La *Loi sur le CST* autorise deux types de cyberopérations étrangères, soit les cyberopérations défensives et les cyberopérations actives. Ces opérations, parfois nommées cyberopérations offensives ou cybereffets, peuvent être utilisées pour contrer les menaces étrangères visant le Canada, faire progresser les intérêts du Canada en matière d'affaires internationales, de défense, de sécurité ou d'économie ou bien aider à protéger les systèmes et l'information électronique, selon le type et la portée de l'opération.

- Les **cyberopérations défensives** aident à protéger les systèmes désignés comme étant d'importance par le gouvernement lors de cyberincidents majeurs, si d'autres mesures ne suffisent pas.
- Les **cyberopérations actives** visent à perturber les menaces étrangères avant qu'elles ne puissent nuire aux intérêts du Canada en matière d'affaires internationales, de défense ou de sécurité.

Ces opérations sont régies de façon stricte par la loi et sont décrites dans la *Loi sur le CST*. Elles ne peuvent pas cibler les Canadiennes et Canadiens au Canada ou à l'étranger ni toute personne se trouvant au Canada. De même, les cyberopérations actives ne doivent pas interférer avec le cours de la justice ou de la démocratie ou entraîner la mort ou des lésions corporelles, que ce soit de façon délibérée ou par négligence criminelle. Elles ne peuvent viser que des cibles étrangères pertinentes sur le plan des affaires internationales, de la défense ou de la sécurité, y compris les intérêts économiques.

Les cyberopérations étrangères sont approuvées grâce à un système « à deux niveaux ». Toutes les cyberopérations doivent être approuvées par la ou le ministre de la Défense nationale. Les cyberopérations actives doivent également être approuvées par la ou le ministre des Affaires étrangères, tandis que les cyberopérations défensives doivent faire l'objet d'une consultation auprès de cette ou ce ministre. Pour ce faire, il faut entretenir une collaboration étroite avec Affaires mondiales Canada (AMC) pour évaluer les répercussions sur la politique étrangère et les répercussions juridiques des cyberopérations proposées, en tenant compte du droit canadien et du droit international applicable dans le cyberespace[1].

La mission du CST quant aux cyberopérations étrangères est menée en étroite coopération avec le Commandement Cyber des Forces armées canadiennes (COMCYBERFAC). Cet important partenariat permet à bon nombre de membres d'intégrer les opérations du CST afin de défendre et de faire progresser les intérêts du Canada, tout en permettant au pays d'établir des capacités agiles et efficaces de cyberopérations étrangères.

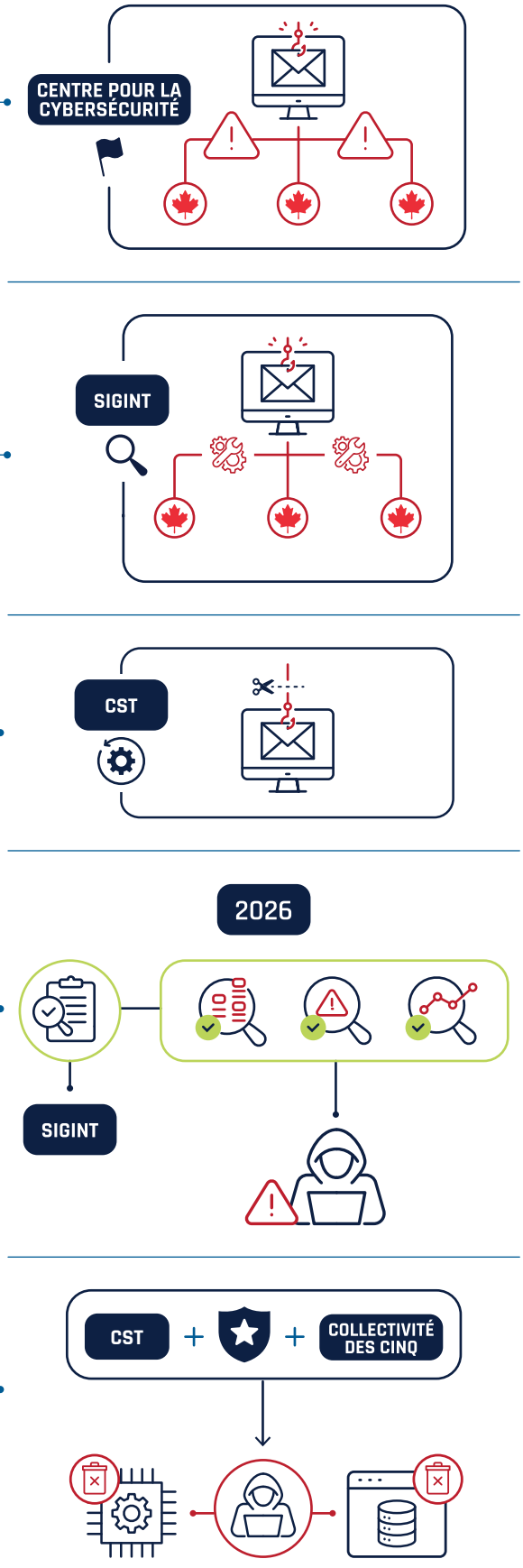
Fort des nouveaux investissements dans les cybercapacités, le CST a renforcé sa capacité à mener des cyberopérations défensives et actives à grande échelle afin de contrer les menaces étrangères.

Mission intégrée : synergie des volets du mandat

Le CST tire sa force de la collaboration entre ses équipes chargées du renseignement étranger, des cyberopérations et de la cyberdéfense. Cette approche intégrée permet de passer à l'action rapidement et efficacement. Le CST collabore également étroitement avec le Service canadien du renseignement de sécurité (SCRS) pour réunir les pouvoirs, l'expertise et l'information complémentaires des deux organismes, de sorte à détecter les menaces rapidement, à accroître la connaissance de la situation et à appuyer les interventions coordonnées dans la défense des intérêts du Canada en matière de sécurité. La motivation du CST, gardien de la sécurité nationale, est la confiance que les Canadiennes et Canadiens lui accordent et la responsabilité qui lui incombe de la respecter au fil de l'évolution de l'environnement de la sécurité et du renseignement.

Les exemples suivants montrent comment le renseignement étranger, les cyberopérations étrangères et la cyberdéfense s'entrecroisent pour perturber les menaces qui ciblent le Canada.

- En 2025, le Centre pour la cybersécurité a détecté une campagne d'hameçonnage qui ciblait les institutions fédérales canadiennes et les systèmes désignés comme étant d'importance.
- Les équipes responsables du SIGINT étranger ont analysé la campagne et déterminé les outils employés.
- Ce renseignement a permis de déclencher une cyberopération défensive qui a perturbé l'infrastructure de l'auteur de menace et a détérioré sa capacité à continuer de cibler les Canadiennes et Canadiens.
- Cette année, l'équipe de lutte contre le cybercrime fondée sur le SIGINT du CST, a produit des rapports de haute fiabilité qui décrivaient les tactiques, techniques et procédures sophistiquées utilisées par un groupe de cybercriminalité bien connu qui adhère au modèle de rançongiciel-service. Ce groupe était responsable de 25 incidents dans les secteurs des transports, de la santé, des produits pharmaceutiques et du commerce.
- Avec ses partenaires de la collectivité des cinq et des organismes d'application de la loi, le CST a mené à bien une cyberopération active qui a rendu inopérante l'infrastructure du groupe et qui a permis de supprimer un grand volume de données volées, annoncées pour la vente sur le Web clandestin.



Espionnage, ingérence étrangère et cybermenaces étatiques

Les auteurs de menace parrainés par des États sont de plus en plus agressifs et utilisent des méthodes plus poussées que les traditionnelles pour que leurs activités soient encore plus perturbatrices. L'environnement géopolitique actuel fait en sorte que les États-nations intensifient les activités de menace hybrides qui intègrent les cyberopérations, l'influence en ligne, les campagnes de désinformation et le ciblage des infrastructures essentielles afin d'atteindre leurs objectifs de perturbation.

Le CST fournit du renseignement étranger afin d'aider le Canada à comprendre les activités d'États hostiles qui minent la sécurité, la souveraineté et la prospérité du Canada, et à y répondre. Ce renseignement sous-tend les efforts de lutte contre l'ingérence étrangère, de protection des infrastructures essentielles et de défense des intérêts économiques et démocratiques du Canada, tout en éclairant les principales priorités, comme la sécurité dans l'Arctique et l'appui du Canada envers la souveraineté de l'Ukraine. Il soutient directement les activités du Centre pour la cybersécurité, comme les bulletins et conseils sur les menaces et le soutien opérationnel aux responsables de la cyberdéfense, et il est renforcé par l'étroite collaboration du CST avec le SCRS et d'autres partenaires. Ce faisant, il y a de meilleures connaissances communes et interventions coordonnées au sein de la collectivité de la sécurité et du renseignement du Canada.

Cette année, grâce au renseignement qu'il a recueilli et aux rapports qu'il a fournis en temps utile, le CST a :

- soutenu les efforts du Canada et des alliés en vue de répertorier et de faire appliquer les sanctions contre la Russie, notamment en déterminant les entités que le gouvernement russe utilise pour contourner les sanctions internationales;
- éclairé les efforts du Canada et des alliés afin de confronter et de contrer la désinformation persistante de la Russie, notamment une campagne de la Russie visant à promouvoir ses messages quant à la guerre en Ukraine, à brouiller les cartes et à diviser;
- cerné les cybermenaces de la Russie et de groupes affiliés qui ciblaient le Canada;
- appuyé les efforts du Canada et de ses alliés en vue de détecter et de contrer le cyberespionnage parrainé par la République populaire de Chine (RPC).

Souveraineté dans l'Arctique et partenariats de sécurité

L'Arctique est une priorité bien établie pour le Canada, en particulier dans le contexte géopolitique incertain qui s'ajoute aux changements climatiques. Au fur et à mesure que l'intérêt des États étrangers, comme la Russie et la RPC, dans la région croît, c'est aussi le cas des risques envers la sécurité, la souveraineté et la prospérité à long terme du Canada. Ces défis se complexifient et dépassent maintenant les menaces militaires et de cybersécurité traditionnelles pour inclure des activités économiques et d'influence qui visent à façonner l'accès, les infrastructures et la prise de décision dans la région.

En tant qu'un des principaux organismes en sécurité et en renseignement et que première ligne de défense du Canada, le CST joue un rôle essentiel dans la réponse à ces risques. En étroite collaboration avec ses partenaires nationaux et internationaux, il se charge du renseignement étranger, de la cyberdéfense et du soutien opérationnel qui sous-tendent les efforts en matière de sécurité du Canada et de l'Amérique du Nord. Ce travail représente la nature intégrée et interconnectée de la défense moderne dans l'Arctique, notamment par la collaboration étroite avec les partenaires, comme les Forces armées canadiennes (FAC) et la Garde côtière canadienne.

Fort de l'augmentation des investissements en défense, le CST a renforcé ses capacités de renseignement dans l'Arctique pour résoudre les lacunes prioritaires en matière de renseignement et donner de l'information sur les intentions, les capacités et les activités stratégiques des États dans la région, en appui aux priorités de souveraineté et de sécurité du Canada. Cette information éclaire également les efforts en matière de cyberdéfense du Centre pour la cybersécurité en lui permettant d'intervenir rapidement et de façon coordonnée face aux menaces émergentes. Grâce aux partenariats avec le gouvernement et les alliés, il assure la cyberdéfense, protège la sécurité économique et appuie les efforts de lutte contre l'ingérence étrangère.

Ce faisant, le CST améliore la capacité du Canada à anticiper les risques dans une région importante sur le plan stratégique et soutient la prise de décisions éclairées en matière de sécurité nationale.

Cette année, le CST a communiqué des rapports de renseignement classifiés sur la sécurité dans l'Arctique à de multiples ministères du gouvernement canadien ainsi qu'aux alliés internationaux du Canada. Rédigés à l'aide du renseignement et du soutien du SCRS, ces rapports portaient 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. Le CST s'est également employé à recueillir du renseignement sur les auteurs de cybermenace étrangers qui cherchent à exploiter et à compromettre des systèmes liés à l'Arctique.

Les partenariats dans l'Arctique

À mesure qu'une attention croissante se porte sur la souveraineté dans l'Arctique, le CST réalise d'importants progrès pour approfondir ses partenariats afin de mener à bien son mandat cette année. Il a notamment :

- continué de coprésider, aux côtés du Bureau du Conseil privé (BCP), 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;
- favorisé l'engagement par l'intermédiaire d'une équipe d'engagement auprès des Autochtones, qui travaille directement avec les partenaires autochtones dans l'Arctique pour faire progresser la cyberrésilience;
- participé aux tables rondes d'AMC pour donner de l'information sur les cybermenaces aux communautés et aux organisations autochtones du Yukon, des Territoires du Nord-Ouest, du Labrador et du Nunavut;
- pris part à un panel sur la cybersécurité en collaboration avec Nunavut Tunngavik Incorporated au Arctic Security Working Group;
- donné des présentations classifiées sur les cybermenaces aux partenaires des territoires;
- continué d'organiser et de diriger des forums internationaux sur le renseignement électromagnétique et les régions polaires.

Ces partenariats sont ancrés par un engagement multilatéral commun de collaboration, de respect et d'inclusion. Le CST travaille étroitement avec les gouvernements territoriaux et autochtones pour renforcer la sensibilisation collective aux menaces et appuyer les interventions en cas de cyberincidents touchant les systèmes critiques des communautés nordiques. Il est important de noter que l'engagement du CST auprès des communautés autochtones va bien au-delà de la sécurité dans l'Arctique. Plus loin dans ce rapport sont décrits les efforts élargis en matière de partenariats, y compris l'établissement de relations de nation à nation et le soutien adapté en cybersécurité.

Au cours de ses activités, le CST se fie à son partenariat robuste avec les FAC pour détecter et surveiller les menaces que représentent les adversaires étrangers dans l'Arctique. Il soutient les opérations de l'Armée canadienne, de la Marine royale canadienne, de l'Aviation royale canadienne,

du Commandement des Forces d'opérations spéciales et de la Garde côtière canadienne en contribuant à la connaissance de la situation et à l'efficacité opérationnelle dans le Nord.

Étant donné l'environnement opérationnel congestionné dans l'Arctique, le Canada joue un rôle de plus en plus important au sein du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD). Tout en respectant ce cadre, le CST fournit des indications et avertissements de possibles menaces aériennes ou maritimes.

En plus du travail stratégique et analytique, le Centre pour la cybersécurité crée des liens directement avec les communautés et les parties prenantes du Nord canadien, dont les organisations du secteur des infrastructures essentielles. Des activités d'engagement, comme des conférences et des présentations, permettent de favoriser la sensibilisation à la cybersécurité, de communiquer des avis et des conseils et d'offrir des services qui améliorent la résilience des infrastructures essentielles et des systèmes du gouvernement. En appui à cet effort, le Centre pour la cybersécurité a également déployé des capteurs avancés sur les systèmes des gouvernements territoriaux pour détecter et atténuer les activités de cybermenace malveillantes.

La sécurité frontalière et les drogues synthétiques illicites

Le trafic de fentanyl et d'autres drogues illégales a un effet direct et dévastateur sur les Canadiennes et Canadiens. Au CST, l'objectif est clair pour lutter contre le crime transnational : aider à sauver des vies et à réduire les dommages.

Le CST a répondu directement à la Directive du premier ministre sur la criminalité transnationale et la sécurité de la frontière en soutenant les efforts du Canada dans la collecte de renseignement et la perturbation des réseaux criminels. Il a fourni du renseignement électromagnétique étranger sur la logistique et les mécanismes du commerce international de drogues en mettant l'accent sur le trafic de stupéfiants illégaux et les chaînes d'approvisionnement.

Avec ses partenaires au Canada et à l'étranger, il communique du renseignement et prend des mesures, s'il y a lieu, notamment des cyberopérations qui perturbent les activités qui menacent le Canada et ses alliés.

Le CST a amélioré sa capacité à produire du renseignement exploitable et opportun sur les réseaux criminels étrangers qui participent au trafic de fentanyl, d'autres drogues illégales et des précurseurs de ces drogues en Amérique du Nord. En mettant au jour le fonctionnement et les méthodes d'adaptation de ces réseaux, le CST réduit leur capacité à passer inaperçu et à continuer de causer du tort aux communautés.

Cellule de coordination des opérations et de renseignement

Le crime organisé transnational, notamment le trafic de fentanyl et de ses précurseurs, représente une menace croissante à la sécurité publique et à la santé des Canadiennes et Canadiens. Pour lutter contre ces réseaux, il faut coordonner le renseignement et les mesures opérationnelles au sein du gouvernement et avec les partenaires étrangers.

Au sein de la Cellule de coordination des opérations et de renseignement (CCOR), le CST collabore avec la Gendarmerie royale du Canada (GRC), le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), l'Agence des services frontaliers du Canada (ASFC), le SCRS et Sécurité publique Canada (SP). Cette coordination permet de conjuguer le renseignement, l'analyse financière et les capacités d'application de la loi, en vue de mieux comprendre et perturber les réseaux criminels complexes.

Cette année, le CST a renforcé cette approche coordonnée en soutenant des initiatives comme le Forum régional du renseignement sécuritaire avec des partenaires du gouvernement du Canada, qui améliore la communication du renseignement et des informations opérationnelles entre les partenaires.

Le 10 juillet 2025, le CST a également organisé une journée de sensibilisation concernant le fentanyl dans un contexte classifié où il a été possible de collaborer et d'échanger de l'information. L'événement a permis de cimenter l'engagement du Canada dans la lutte contre le trafic de drogues illégales et la protection de la sécurité publique et a réuni les principaux partenaires fédéraux, notamment le tsar du fentanyl du Canada, les parties prenantes du CCOR et l'Agence de la santé publique du Canada. Le CST a également animé un forum multidisciplinaire mettant en vedette des expertes et experts internationaux du domaine médical et de l'application de la loi.

Ces efforts ont aidé le Canada à définir, à perturber et à réduire les répercussions des activités criminelles transnationales, y compris celles liées au fentanyl, afin de mieux protéger les communautés et renforcer la sécurité nationale.

Étude de cas Comment le renseignement et les cyberopérations du CST se sont combinés pour perturber l'approvisionnement en fentanyl et ses précurseurs au Canada

- En 2025, le CST a découvert que de grands cybercriminels, basés à l'étranger, commissionnaient l'achat et la vente de produits chimiques précurseurs utilisés dans la fabrication d'opioïdes synthétiques, comme le fentanyl.
- L'organisme a recueilli du renseignement étranger sur ces intermédiaires afin de mieux comprendre la menace visant le Canada et développer des options pour perturber leurs activités.
- Il a mené à bien des cyberopérations actives autorisées contre ces intermédiaires, qui ont permis de perturber et de réduire leurs capacités.
- Le CST a tiré parti de ses pouvoirs pour bel et bien atténuer les menaces transnationales complexes et soutenir les organismes d'application de la loi en vue de faire progresser les objectifs en matière de sécurité nationale et de protéger des vies et la sécurité publique.

Lutte contre l'extrémisme violent

L'extrémisme violent continue d'évoluer et nécessite donc des interventions coordonnées et proactives.

Le CST s'efforce de détecter et de contrer les menaces que représente l'extrémisme violent basé à l'étranger envers les Canadiennes et Canadiens. Le renseignement qu'il recueille aide le gouvernement et les partenaires de la sécurité et du renseignement à agir rapidement en relevant les menaces des idéologies et groupes extrémistes violents, notamment les groupes motivés par la religion (comme les affiliés d'Al-Qaïda et de Daech) et l'extrémisme violent à caractère idéologique (comme les idéologies xénophobes, antiautoritaires et fondées sur l'identité de genre ou les récriminations personnelles). Toutes les formes d'extrémisme violent à l'échelle mondiale connaissent une tendance à la hausse, qui se transpose autant dans le monde virtuel que réel dans le but de menacer la sécurité publique et de faire des victimes innocentes. Ces mouvements transnationaux utilisent des forums en ligne pour communiquer leur idéologie et propager leurs manifestes afin de recruter des personnes et de terroriser les autres. Bien que les motivations puissent varier, les menaces demeurent bien réelles et les auteurs de menace cherchent à profiter d'occasions pour créer le chaos.

En Amérique du Nord et en Europe, les efforts du CST ont aidé à mettre au jour et à perturber de multiples menaces extrémistes. Le CST poursuit sa collaboration avec d'autres services de renseignement et organismes d'application de la loi alliés, tout en tirant parti de ses pouvoirs en matière de cyberopérations étrangères pour perturber les complots et protéger la sécurité publique. Sa priorité demeure la détection des menaces à la vie et l'intervention connexe, de même que les cyberopérations visant à démanteler les réseaux terroristes qui cherchent à faire du mal. Le CST a également offert son soutien dans l'intervention du Canada à des situations de prise d'otages à des fins terroristes, à des menaces envers des événements publics et à des missions canadiennes.

En voici des exemples récents :

- collaborer étroitement avec des partenaires nationaux pour fournir du renseignement opportun sur des extrémistes à l'étranger qui cherchaient à mener des attaques au Canada;
- offrir du soutien dans le cadre des interventions dans le cas d'enlèvements ou de possibles prises d'otages touchant des Canadiennes et Canadiens à l'étranger;
- identifier les auteurs de menace responsables de menaces à la bombe contre des entités canadiennes;
- collaborer avec les partenaires étrangers à de nombreuses reprises en appui aux efforts d'atténuation et de perturbation des menaces extrémistes dans leur pays;
- surveiller les menaces visant les grandes manifestations sportives internationales;
- collaborer avec de nombreux partenaires étrangers afin d'appuyer la protection des athlètes canadiennes et canadiens, les délégations canadiennes et le publicen général lors des Jeux olympiques d'hiver de Milano Cortina 2026.

Cyberopérations visant à perturber les organisations d'extrémisme violent

Le CST a également mis sur pied et mené à bien des cyberopérations ayant des répercussions concrètes afin de perturber les activités des organisations étrangères d'extrémisme violent. En prenant pour cible leur présence en ligne et leur infrastructure technique, le CST a diminué la capacité de ces organisations à effectuer des activités, à recruter et à diffuser du contenu nuisible.

Étude de cas Croisement du renseignement et des cyberopérations du CST pour contrer l'extrémisme violent

- Le CST a recueilli du renseignement sur un groupe extrémiste étranger qui propageait une idéologie violente et cherchait à recruter dans les pays occidentaux, y compris au Canada.
- Les équipes SIGINT du CST ont produit du renseignement permettant d'analyser le réseau, la portée et les vulnérabilités du groupe afin de perturber ses activités.
- En fonction des pouvoirs pertinents, le CST a mené une cyberopération active qui a miné la crédibilité du groupe et réduit ses capacités à radicaliser et à recruter de nouvelles et nouveaux membres.

Cybercriminalité

La cybercriminalité représente une menace permanente pour le Canada. Comme le mentionne la Vue d'ensemble des menaces par rançongiciel de 2025 à 2027[2], les rançongiciels demeurent la forme la plus perturbatrice de cybercrime touchant les organisations canadiennes, y compris les infrastructures essentielles. Le CST joue un rôle important pour aider le gouvernement du Canada à comprendre ces menaces, à y répondre en collaboration avec ses alliés et ses partenaires, à surveiller les activités de cybercriminalité étrangères et à évaluer leur incidence potentielle sur les Canadiennes et Canadiens.

Le CST produit du renseignement étranger sur les tactiques, techniques et procédures utilisées par des cybercriminels étrangers et des États hostiles. Ce renseignement aide le Centre pour la cybersécurité à informer les responsables de la cyberdéfense, renforcer les mesures de protection et appuyer les mesures prises pour contrer les activités malveillantes ciblant les systèmes et les infrastructures essentielles du Canada. En combinant le renseignement et son expertise en cybersécurité, le CST aide à traduire la connaissance des menaces en mesures de défense et en interventions pratiques.

Cette année, le CST a entrepris des activités simultanées contre dix des plus grands groupes de rançongiciel qui nuisent au Canada et à ses alliés. Il a mené des activités autorisées visant la perturbation technique pour mettre hors d'état de nuire leurs infrastructures et a collaboré avec ses partenaires étrangers d'application de la loi pour perturber les réseaux étrangers de cybercriminalité et réduire le nombre de victimes de cybercrimes.

Soutien aux opérations militaires

Le renseignement du CST aide à protéger le personnel des FAC. En offrant des avertissements opportuns et une meilleure connaissance de la situation, le CST appuie les opérations au Canada et à l'étranger. Au cours de la dernière année, il a produit du renseignement étranger exploitable en appui à des opérations clés, dont UNIFIER, REASSURANCE et HORIZON.

Ce renseignement a soutenu :

- le repérage des menaces de contre-ingérence à l'endroit du personnel des FAC;
- les avertissements rapides aux forces déployées;
- l'évaluation de l'influence des entreprises d'État étrangères sur les opérations et les exercices du Canada;
- l'analyse des capacités de guerre électronique des adversaires afin de mieux éclairer l'intervention des FAC.

Le CST suit également le développement et l'utilisation des capacités des adversaires étrangers, notamment les systèmes de commande et de contrôle, et les outils informatiques, de communications, de renseignement, de surveillance, de reconnaissance et de ciblage. Cette information aide à protéger les forces canadiennes et alliées à mener à bien leurs opérations. Les FAC ont utilisé le renseignement produit cette année pour améliorer la sécurité opérationnelle, orienter les opérations et informer les alliés sur les intentions et les capacités des adversaires, de sorte à améliorer la connaissance et la protection collectives.

Opération REASSURANCE

Le Canada continue de jouer un rôle principal dans la défense du territoire de l'OTAN sur la terre, en mer et dans les airs en réponse à l'agression continue de la Russie contre l'Ukraine et ses activités hybrides contre les alliés.

En août 2025, le Canada a renouvelé pour trois ans son rôle de leadership dans le cadre de l'opération REASSURANCE à partir de 2026-2027. Cet engagement renforce la contribution du Canada envers la sécurité et la stabilité auprès de ses partenaires transatlantiques en Lettonie et dans les régions de la Méditerranée, de la mer Noire et de l'Atlantique Nord.

Le CST soutient cette mission par le biais de son Programme des agentes et agents de cybersécurité en déploiement (PACD). Au cours de la dernière année, les analystes du Centre pour la cybersécurité déployées et déployés en Lettonie et en Lituanie y ont :

- mené des activités proactives de chasse aux menaces;
- fourni des avis et des conseils sur le terrain;
- appuyé des opérations de cyberdéfense.

Ces efforts ont permis de renforcer la résilience des alliés et de veiller à ce que les forces canadiennes puissent œuvrer en toute sécurité et efficacement. Ces activités aident le Canada à comprendre et à contrer les menaces étrangères, et le CST met également en œuvre cette approche intégrée au pays par l'entremise du Centre pour la cybersécurité, afin de prévenir et d'évaluer les cyberincidents touchant les systèmes auxquels les Canadiennes et Canadiens se fient chaque jour, et d'y répondre.

Intervenir en cas de cyberincidents et prévenir les cyberincidents

L'environnement de cybermenace au Canada ne cesse de grandir et de se complexifier. Les auteurs de menace étatiques et les cybercriminels évoluent rapidement et utilisent de nouveaux outils et de nouvelles techniques pour cibler les systèmes d'importance des institutions démocratiques et les Canadiennes et Canadiens.

En 2025-2026, le Centre pour la cybersécurité a enregistré plus de **3 200 cyberincidents** touchant les institutions fédérales et les secteurs des infrastructures essentielles.

En étroite collaboration avec ses partenaires, il a offert l'évaluation technique, le tri des incidents, des conseils sur le confinement et du soutien en matière d'atténuation. En tirant parti de l'information obtenue par le renseignement, le Centre pour la cybersécurité a été en mesure de détecter et d'évaluer des cyberincidents et d'intervenir dans ces cas-là efficacement et rapidement.

Ce travail a aidé à réduire les perturbations subies par les services essentiels et les répercussions des cyberincidents sur les infrastructures essentielles, ainsi qu'à protéger les systèmes sur lesquels se fient les Canadiennes et Canadiens au quotidien.

Centre opérationnel de production et de coordination du CST : le noyau opérationnel en tout temps du CST

Le CST maintient une posture opérationnelle continuelle en appui à la sécurité nationale du Canada. Au cœur de ces efforts se trouve le Centre opérationnel de production et de coordination du CST (COPCC), qui fournit une connaissance de la situation et assure la coordination opérationnelle en tout temps pour le CST et les partenaires du gouvernement du Canada.

Le COPCC surveille le déroulement des événements mondiaux et coordonne les interventions de ceux qui pourraient toucher le Canada et les Canadiennes et Canadiens, notamment les cyberincidents, les menaces à la sécurité nationale et les événements majeurs au pays ou à l'étranger. Ces activités continuelles permettent de garantir la prise de mesures opportune et coordonnée partout dans la collectivité fédérale de la sécurité.

Son efficacité se fonde sur l'étroite collaboration avec les partenaires fédéraux et les centres des opérations de sécurité (COS) de la collectivité des cinq, de sorte à assurer une connaissance commune de la situation, la planification conjointe et les interventions coordonnées.

La première ligne de défense numérique

En dehors des heures normales de travail, y compris la nuit, le COPCC agit comme première ligne d'intervention du CST sur le front numérique. Il diffuse des alertes et des notifications et coordonne les activités d'intervention pour répondre aux cyberincidents sans tarder. Cette année, le COPCC a alerté le Centre pour la cybersécurité de **121 incidents de cybersécurité en dehors des heures de travail**, ce qui a permis de renforcer la résilience des infrastructures numériques du Canada.

Soutien lors d'événements mondiaux et de crises émergentes

En cette période d'instabilité mondiale accrue, le COPCC a coordonné l'intervention du CST dans le cadre d'événements internationaux et a informé les parties prenantes du CST de **220 incidents terroristes ou mondiaux importants** cette année.

Le COPCC a également collaboré étroitement avec les partenaires du gouvernement du Canada pour communiquer de l'information et coordonner les interventions aux situations émergentes, notamment les événements qui se sont déroulés au Mexique, à Cuba, au Venezuela, en Iran et plus généralement au Moyen-Orient.

Appuyer l'organisation sécurisée d'événements planifiés

Cette année, le COPCC a coordonné les efforts de renseignement étranger et en cybersécurité du CST dans le cadre d'événements majeurs planifiés, dont :

- les 45e élections générales;
- le Sommet des leaders du G7 à Kananaskis, en Alberta;
- les Jeux olympiques et paralympiques d'hiver de Milano Cortina 2026.

Le COPCC a également soutenu les préparatifs liés à l'organisation et à la participation du Canada dans la Coupe du Monde de la Fédération Internationale de Football Association (FIFA) 2026™.

S'appuyant sur le rôle de coordination du COPCC, le Centre pour la cybersécurité a offert un soutien opérationnel plus direct aux partenaires de l'événement en aidant à interpréter la connaissance de la situation pour adopter des mesures de cyberdéfense pratiques avant et pendant les événements majeurs.

Soutien en matière de cybersécurité pour les événements majeurs

Les événements majeurs représentent des défis de cybersécurité uniques qui nécessitent une planification et une intervention coordonnées.

Le CST a joué un rôle important dans la coordination du soutien en matière de cybersécurité pour les événements majeurs cette année, notamment les Jeux olympiques d'hiver de Milano Cortina 2026, le Sommet du G7 et la préparation à la Coupe du Monde de la FIFA 2026™. Ce travail était appuyé par la mission intégrée, qui combinait le renseignement étranger, les avis en matière de cybersécurité et la coordination opérationnelle, en vue d'aider les partenaires des événements à se préparer et à répondre aux menaces en évolution.

En tant que membre et leader du groupe de travail fédéral sur la cybersécurité, le CST a :

- collaboré avec les partenaires du gouvernement du Canada afin de renforcer la posture de cybersécurité au sein des organisations et des infrastructures essentielles;
- fourni des avis stratégiques, des conseils techniques et des évaluations de menace;
- soutenu l'intégration d'organisations participantes du secteur des infrastructures essentielles aux services du Centre pour la cybersécurité;
- donné des présentations adaptées sur la cybersécurité aux parties prenantes.

Il a également pris part à des exercices de simulation et à des exercices fonctionnels conçus pour mettre à l'essai la préparation et améliorer la coordination entre les partenaires. Durant les événements, le CST a maintenu une présence sur place aux centres de commandement des événements pour assurer une participation opérationnelle directe et un soutien en temps réel.

Protéger les Jeux olympiques de 2026

Le CST a appuyé l'effort coordonné de renseignement visant à assurer la sécurité des Jeux olympiques d'hiver de Milano Cortina 2026. En collaboration avec les partenaires de l'événement, il a établi et maintenu des processus robustes de communication de l'information afin de surveiller les menaces et d'assurer le déroulement sécuritaire de l'événement. Il a également établi les priorités de ses efforts de collecte de renseignement, afin de détecter toute menace possible visant les Jeux ou les Canadiennes et Canadiens y participant ou y assistant.

Ce travail a contribué au bon déroulement des Jeux, à la protection des athlètes, des représentantes et représentants officiels et desspectatrices et spectateurs, en plus de renforcer le rôle du Canada en tant que partenaire de confiance en sécurité à l'échelle internationale.

Sommet du G7

En juin 2025, le Canada a accueilli le 51e Sommet du G7 à Kananaskis, en Alberta. Le Centre pour la cybersécurité a appuyé l'événement en déployant des spécialistes, en offrant des services de cyberdéfense et en conseillant les partenaires fédéraux, provinciaux et municipaux.

Le CST a maintenu un état de préparation élevé afin de détecter les cyberincidents qui auraient pu avoir des répercussions sur le sommet, les atténuer et y répondre.

Coupe du Monde de la FIFA 2026™

Le CST soutient les préparatifs en vue de la Coupe du Monde de la FIFA 2026™ en Amérique du Nord.

Aux côtés de ses homologues du Mexique et des États-Unis, le Centre pour la cybersécurité du CST fait partie d'un groupe de travail créé par CSIRTAmericas, qui a pour objectif de renforcer la coordination opérationnelle, stratégique et technique et l'échange d'information. Ces efforts conjoints visent à prévenir et à détecter les cyberincidents et à intervenir en cas de cyberincident.

Durant l'étape de planification, le Centre pour la cybersécurité a offert des séances d'information qui décrivaient la posture de cybersécurité du Canada, du Mexique et des États-Unis.

Les activités préparatoires comprenaient notamment les suivantes :

- communiquer le renseignement sur les menaces, améliorer la surveillance et donner des séances d'information de sensibilisation;
- participer à des groupes de travail et à des exercices de simulation;
- appuyer les efforts de coordination du gouvernement.

Au cours du tournoi, le Centre pour la cybersécurité maintiendra une posture opérationnelle accrue et aura du personnel déployé au centre de commandement technologique de la FIFA® à Miami et aux centres des opérations de sécurité locaux.

Afin de maintenir la connaissance de la situation et la préparation opérationnelle, le COPCC a également supervisé la participation du CST dans plusieurs exercices de sécurité nationale avec des partenaires du Canada et d'autres pays au cours de l'année.

Toujours sur ses gardes

Si une situation de crise représentant une menace pour le Canada ou pour des Canadiennes et Canadiens à l'étranger survenait, le COPCC est déjà prêt à surveiller les événements, à coordonner les interventions et à veiller à ce que les décisionnaires aient l'information nécessaire au moment crucial.

Avis et alertes

Le Centre pour la cybersécurité a constaté cette année une augmentation du nombre de vulnérabilités et leur gravité, qui a eu pour effet d'entraîner une augmentation du nombre d'alertes (25) et d'avis (995). Se fondant sur le renseignement étranger, les analyses techniques et les rapports opérationnels, ces produits ont aidé les partenaires à mieux comprendre les risques émergents et à agir rapidement. Il s'agit d'une augmentation de 25 % des alertes et de 28 % des avis comparativement à l'année financière 2023-2024.

Parmi les plus notables se trouvaient les suivantes :

- l'alerte sur la vulnérabilité critique touchant les dispositifs de réseau étendu à définition logicielle (SD-WAN) de Cisco, accompagnée du bulletin conjoint sur les cybermenaces malveillantes contre les réseaux SD-WAN[3], publié par les partenaires de la collectivité des cinq;
- l'alerte sur l'abus de systèmes de contrôle industriels accessibles depuis Internet par des hacktivistes[4] dans les infrastructures essentielles canadiennes;
- l'alerte sur la vulnérabilité du jour zéro touchant SharePoint.

Vulnérabilités du jour zéro touchant SharePoint

En juillet 2025, Microsoft a révélé qu'un ensemble de vulnérabilités du jour zéro touchait les serveurs sur site de SharePoint. Étant donné la vaste exposition aux menaces au Canada et la possibilité d'une compromission répandue, le Centre pour la cybersécurité a coordonné l'intervention du gouvernement du Canada en collaboration avec ses partenaires fédéraux.

Dans le cadre de cet effort, le Centre pour la cybersécurité a publié des alertes, a fourni un soutien de surveillance des capteurs, a effectué des analyses criminalistiques et a publié des évaluations techniques détaillées. Grâce à ses enquêtes, le Centre pour la cybersécurité a constaté une exploitation sophistiquée, notamment par l'utilisation précoce de nouvelles techniques et de charges de virus en mémoire sur mesure pour obtenir un accès permanent, permettre un déplacement latéral dans les réseaux et exfiltrer les données sensibles, des activités qui avaient parfois commencé des semaines avant la divulgation publique.

La publication du Centre pour la cybersécurité, Détection des menaces pour vulnérabilités touchant SharePoint, consignait la façon dont les vulnérabilités ont été exploitées en pratique, soulignait les limites des indicateurs de compromission traditionnels, mettait l'accent sur l'importance des correctifs combinés à la rotation des clés et des justificatifs d'identité et communiquait des conseils de détection et d'atténuation pour aider les organisations à détecter des activités semblables et y répondre.

En parallèle, le Centre pour la cybersécurité a collaboré étroitement avec la collectivité élargie de la cybersécurité pour échanger de l'information opportune et aviser rapidement les exploitants canadiens d'infrastructures essentielles des systèmes vulnérables au moyen du Système national de notification de cybermenace (SNNC).

Système national de notification de cybermenace

Le SNNC est un service canadien d'avertissement rapide des cybermenaces offert par le Centre pour la cybersécurité. Il surveille les activités de cybermenace et envoie des notifications opportunes aux abonnés lorsque des cyberincidents, des vulnérabilités ou d'autres risques sont détectés.

Cette année, c'est plus de **97 000 notifications** qui ont été envoyées à des organisations de partout au pays afin de les avertir rapidement de possibles menaces. En moyenne, les notifications étaient envoyées à **450 organisations** chaque semaine. En date de la période visée par le présent rapport, **1 363 organisations** étaient inscrites au service, dont **97 sont nouvellement inscrites**.

Ces alertes aident les organisations à agir rapidement, de sorte à réduire les risques que des cyberincidents surviennent et à renforcer la résilience globale du Canada.

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

Les notifications de signes avant-coureurs d'une attaque par rançongiciel du Centre pour la cybersécurité aident les organisations à mettre fin aux cyberincidents avant qu'ils n'entraînent de vols de données ou de perturbations de systèmes.

Cette année, le Centre pour la cybersécurité a envoyé **67 notifications** aux organisations canadiennes qui étaient de possibles cibles. Les partenariats en matière de renseignement évoluent continuellement, donc la portée des notifications aux organisations peut varier selon le contexte changeant des cybermenaces. Ils comprenaient des partenaires à tous les niveaux gouvernementaux et dans des secteurs clés, comme le secteur manufacturier et les secteurs de la santé, de l'énergie, des finances et de l'éducation. Puisqu'elles permettaient aux organisations d'agir rapidement, ces notifications ont permis de réduire les possibles répercussions financières et opérationnelles.

Les notifications de signes avant-coureurs d'une attaque par rançongiciel du Centre pour la cybersécurité peuvent offrir de réels avantages financiers en permettant aux organisations d'agir avant que les incidents ne s'aggravent. En déterminant et en avisant les victimes rapidement dans le cycle de vie d'une attaque, les notifications donnent l'occasion aux organisations de contenir les menaces avant que ne survienne le chiffrement ou le vol de données, de sorte à éviter les périodes d'indisponibilité coûteuses, les efforts à mettre dans la reprise et les paiements possibles de rançons. Au cours de la période visée par un rapport antérieur, cette approche a contribué à des économies allant jusqu'à 18 millions de dollars entre les organisations avisées, la preuve de la valeur importante d'une intervention rapide.

Protéger la démocratie et les systèmes les plus essentiels du Canada

Au fur et à mesure que les cybermenaces ciblent davantage les systèmes démocratiques et les services essentiels, le CST continue de collaborer avec les principales parties prenantes afin de protéger les institutions démocratiques canadiennes.

Au moyen de la sensibilisation proactive, de la collaboration auprès d'équipes spécialisées en renseignement et des outils de détection avancée des menaces, le CST renforce les systèmes critiques des provinces et des territoires. Ce travail assure la sécurité et l'intégrité des élections, la résilience des infrastructures essentielles et la protection du quotidien des Canadiennes et Canadiens, en ligne et hors ligne.

Soutenir les institutions fédérales

Le CST et le Centre pour la cybersécurité collaborent étroitement avec les institutions fédérales pour les aider à prévenir les cyberincidents, de même qu'à intervenir et à reprendre leurs activités en cas de cyberincident.

Au cours de la dernière année, ils ont :

- offert une assistance directe lors de cyberincidents;
- produit des avis et des conseils adaptés en vue de réduire les risques à la cybersécurité;
- donné des séances d'information personnalisées aux ministères touchés par des activités malveillantes.

Combinés, ces efforts ont renforcé la résilience collective du gouvernement fédéral et des sociétés d'État.

Séances d'information sur les services du Centre pour la cybersécurité

Le Centre pour la cybersécurité continue d'offrir des séances d'information sur ses services aux institutions fédérales. Ces séances interactives aident les équipes responsables de la cybersécurité au sein du gouvernement du Canada à comprendre les outils et les services du Centre pour la cybersécurité et à y accéder.

En 2025-2026, **1 330 participantes et participants** provenant de **153 ministères** ont participé à ces séances et ont donc amélioré les connaissances et l'adoption des services au sein du gouvernement.

Série de rencontres éclair

Cette année, le Centre pour la cybersécurité a lancé une série de rencontres éclair, un forum en ligne pour les professionnelles et professionnels des TI et de la cybersécurité, où se communiquent des informations et sont abordés les défis émergents.

La série a réuni environ **2 300 participantes et participants** provenant de **91 ministères et organismes fédéraux**. Elle répondait à la demande d'un espace de collaboration fédéral où discuter des enjeux techniques, opérationnels et stratégiques.

Engagement auprès des sociétés d'État et des ministères fédéraux

Le Centre pour la cybersécurité approfondit continuellement ses engagements auprès des sociétés d'État et des ministères fédéraux afin de renforcer la cybersécurité partout au gouvernement.

Il a notamment :

- fait la promotion d'une application uniforme de la directive de cybersécurité du Secrétariat du Conseil du Trésor (SCT);
- soutenu l'intégration de services clés, dont le programme de capteurs, qui demeure l'un des outils les plus efficaces du Centre pour la cybersécurité afin de détecter et de bloquer les cyberactivités malveillantes dans les systèmes d'importance.

Ces engagements ont donné un aperçu inestimable des lacunes, des besoins et des défis opérationnels au sein des ministères. Ils aident à parfaire les services du Centre pour la cybersécurité et à offrir un soutien ciblé lorsqu'il est le plus nécessaire.

Sécurité des communications : protéger l'information sensible

En tant qu'autorité nationale en matière de sécurité des communications (COMSEC pour *Communications Security*), le CST propose un ensemble complet de capacités de protection de l'information la plus sensible du gouvernement du Canada.

Conformément au volet de son mandat touchant l'assurance de l'information, il continue d'améliorer son programme COMSEC, sur les plans techniques et stratégiques, afin de suivre le rythme des menaces sophistiquées et les demandes d'un environnement interconnecté.

Ce travail sous-tend les communications sécurisées partout au gouvernement et chez ses partenaires. Il comprend les éléments suivants :

- la gestion des clés cryptographiques;
- l'élaboration de politiques et la conformité;
- la gestion des actifs des systèmes de chiffrement;
- la conception et la livraison de solutions de télécommunications novatrices, basées sur la recherche et le développement robustes.

Au cours de l'année, le CST a approfondi ses partenariats avec les États-Unis et le Royaume-Uni, tout en établissant de nouvelles collaborations en matière de communications sécurisées et de solutions mobiles. Ces efforts appuient le fonctionnement du gouvernement fédéral, au pays et avec les partenaires étrangers, en plus d'améliorer les outils à la disposition des décisionnaires en vue de protéger les systèmes et l'information du gouvernement. Grâce à la prévoyance, le CST adopte une posture de préparation et de résilience, et elle se manifeste par le travail précieux que le CST accomplit aux côtés de ses alliés.

Protéger les institutions démocratiques

Tandis que les cybermenaces contre les élections et les processus démocratiques ne cessent de gagner en ampleur et en sophistication, la priorité pour le CST demeure de protéger les institutions démocratiques du Canada.

Pendant l'année, le Centre pour la cybersécurité a collaboré étroitement avec les partenaires fédéraux et les institutions démocratiques pour protéger l'intégrité des élections canadiennes. Le Centre pour la cybersécurité a présenté des séances d'information afin de sensibiliser aux menaces en évolution et d'offrir un soutien adapté en vue de renforcer la résilience des systèmes opérationnels. Le renseignement étranger généré par les activités SIGINT du CST a sous-tendu ce travail. Ces informations ont permis d'éclairer les efforts visant à détecter et à contrer les menaces parrainées par la RPC, de même qu'à appuyer la protection des processus démocratiques du Canada aux niveaux fédéral et provinciaux, afin d'assurer la sécurité des élections et la confiance.

Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections

Le CST est un membre principal du Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (GT MSRE), aux côtés du SCRS, d'AMC et de la GRC.

Mis sur pied en 2019, le GT MSRE coordonne les efforts à l'échelle du gouvernement en vue de surveiller les menaces envers les élections fédérales et d'y répondre.

Pas l'intermédiaire du GT MSRE, le CST a communiqué du renseignement étranger concernant les menaces visant les processus démocratiques du Canada pendant l'année, notamment les 45e élections générales de 2025 et l'élection partielle dans Battle River-Crowfoot. Mené en étroite coordination avec les autres partenaires du GT MSRE, ce travail a aidé à renforcer la capacité du gouvernement du Canada à détecter et à évaluer les menaces visant les institutions démocratiques, de même qu'à y répondre.

Avec ses partenaires, le CST a également soutenu l'attribution publique de deux occurrences d'opérations d'information d'États étrangers sur les médias sociaux, dont le but était d'influencer l'opinion du public. Cette collaboration met en lumière l'efficacité du gouvernement du Canada dans la protection de ses processus démocratiques et l'amélioration de la transparence et de la sensibilisation du public quant aux menaces qui visent les Canadiennes et Canadiens en ligne.

Le CST continue de surveiller les menaces qui ciblent les processus démocratiques et les infrastructures essentielles du Canada tout au long de l'année afin de veiller à ce que les Canadiennes et Canadiens puissent avoir confiance dans les institutions qui gouvernent en leur nom.

Soutenir les provinces et les territoires

Les auteurs de cybermenace, y compris les auteurs étatiques, prennent de plus en plus pour cible les différents ordres de gouvernement. Les gouvernements provinciaux, territoriaux et autochtones et les administrations municipales sont fort probablement perçus comme des cibles précieuses de cyberespionnage, étant donné qu'ils conservent des informations sensibles et qu'ils sont des partenaires clés dans l'environnement de cybersécurité du Canada.

Le CST approfondit sa collaboration avec toutes ces administrations afin d'améliorer la sensibilisation et l'intervention collectives.

En 2024-2025, à la suite d'une série d'incidents de cybersécurité ciblant des établissements du nord du Canada et avec l'autorisation du ministre de la Défense, le Centre pour la cybersécurité est allé en amont de la menace et a déployé des capteurs sur les biens de TI des gouvernements du Yukon, des Territoires du Nord-Ouest et du Nunavut. Ces capteurs sophistiqués détectent les cyberactivités malveillantes dans les dispositifs qui se trouvent sur le périmètre du réseau et dans le nuage. Ils comptent parmi les instruments cruciaux que détient le Centre pour la cybersécurité pour défendre les systèmes d'importance du gouvernement du Canada.

Grâce à sa stratégie d'expansion des capteurs dans les provinces et les territoires, le Centre pour la cybersécurité étend ses services de capteurs à l'extérieur du gouvernement et des territoires fédéraux, dans le but de protéger les systèmes d'importance critique du Canada. Les capteurs sont maintenant déployés dans plusieurs provinces et dans les trois territoires, soit environ 5 % du parc de capteurs. En 2025, ces déploiements ont entraîné environ 150 rapports de prévention et de détection qui ont été communiqués avec les partenaires provinciaux et territoriaux pour soutenir la détection rapide des menaces et l'intervention accélérée.

Cette année, les provinces et les territoires ayant accès aux services de capteurs de l'organisme ont également reçu l'accès à ObservationDeck. Il s'agit d'une application Web interactive qui regroupe des données découlant des services de sécurité offerts par le Centre pour la cybersécurité de sorte à donner un aperçu clair de la posture de cybersécurité. Les rapports d'ObservationDeck sont étoffés d'analyses commerciales, internes et de source ouverte qui font le sommaire des biens de TI du ministère visé et de leurs vulnérabilités.

Entente fédérale-provinciale-territoriale liée à la cybersécurité

À l'automne 2025, les gouvernements fédéral, provinciaux et territoriaux ont franchi une importante étape en vue de défendre les Canadiennes et Canadiens contre les cybermenaces. La conclusion de l'**Entente de collaboration canadienne en matière de cybersécurité** renforce la coordination pancanadienne en permettant l'échange efficace d'information relative à la cybersécurité, de l'expertise et des outils entre les administrations. Par l'intermédiaire du Centre pour la cybersécurité, le CST soutient la mise en œuvre de l'entente en établissant les canaux d'échange d'information, en faisant progresser les outils et les processus conjoints et en travaillant avec les partenaires pour améliorer la préparation collective aux cybermenaces. Ces efforts combinés renforcent la capacité du Canada à intervenir en cas de cyberincident et à protéger les Canadiennes et Canadiens dans un environnement de menace qui se complexifie.

Table ronde fédérale, provinciale et territoriale des responsables de la cybersécurité

En avril 2025, le Centre pour la cybersécurité a organisé la troisième itération annuelle de la Table ronde fédérale, provinciale et territoriale des responsables de la cybersécurité. Des représentantes et représentants de partout au Canada se sont rencontrés pour échanger des points de vue, améliorer la coordination entre les administrations et discuter des priorités, comme l'intervention en cas d'incident, la sécurité de la chaîne d'approvisionnement et les cadres réglementaires des infrastructures essentielles.

Cette collaboration garantit une approche nationale coordonnée face aux cybermenaces.

Soutenir les infrastructures essentielles

Les infrastructures essentielles du Canada sont à la base de la sécurité, du bien-être et de la sécurité économique des Canadiennes et Canadiens. Elles sont également une cible croissante de cybermenaces, qu'il s'agisse d'activités criminelles motivées par le gain financier ou d'attaques parrainées par un État. Ces menaces peuvent perturber les services essentiels auxquels les Canadiennes et Canadiens se fient chaque jour.

> *« Les cyberactivités malveillantes qui ciblent les infrastructures essentielles du Canada […] sont en hausse et il s'agit d'une menace réelle et urgente. […] Toute perturbation des infrastructures essentielles constitue non seulement une menace pour la santé et la sécurité publiques, mais aussi une menace pour la confiance du public, l'environnement et l'économie. »*
>
> *Déclaration commune sur les cyberactivités malveillantes qui ciblent les infrastructures essentielles canadiennes*[5]

Par conséquent, le CST a pour objectif de protéger les infrastructures essentielles, d'améliorer la cyberrésilience et de réduire les risques. Par l'intermédiaire du Centre pour la cybersécurité, il s'associe aux organisations de secteurs clés, dont les télécommunications, l'énergie, les finances, les transports, la gestion de l'eau et la santé. Le renseignement qu'il recueille aide à cerner les menaces émergentes envers ces secteurs et permet au Centre pour la cybersécurité d'offrir des conseils, des alertes et du soutien opérationnel adaptés.

Au cours de la dernière année, le CST a :

- présenté des séances d'information par secteur;
- participé à des exercices de simulation et à des exercices fonctionnels;
- donné des conseils techniques sur les risques, notamment quant aux vulnérabilités, à la sécurité des réseaux mobiles et à l'intégrité de la chaîne d'approvisionnement;
- réuni des forums nationaux et des communautés de pratique ayant pour objectif d'aider les organisations à traduire les conseils en actions.

Faits saillants de 2025-2026 :

- 522 engagements avec des organisations clés des secteurs et des échelons de gouvernement
- Séances d'information bimensuelles sur les cybermenaces à l'intention de 1 000 professionnelles et professionnels de la sécurité des TI dans les secteurs des infrastructures essentielles du Canada
- 8 séances « Passons à l'action », qui comptaient en moyenne 810 participantes et participants

Secteur des télécommunications

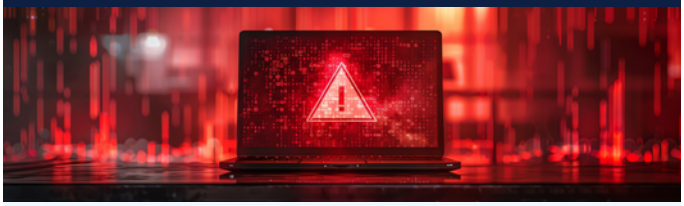
Les réseaux de télécommunications sont l'épine dorsale de l'Internet du Canada et sont une principale cible d'espionnage étranger. Les auteurs de cybermenace parrainés par un État continuent d'exploiter ces systèmes pour accéder à l'information sensible.

Par l'intermédiaire du Programme de cyberrésilience des télécommunications du Centre pour la cybersécurité, le CST collabore avec les exploitants de réseaux mobiles canadiens pour renforcer la sécurité et la résilience des réseaux 3G, 4G et 5G du Canada.

En 2025-2026, les principaux efforts comprenaient les suivants :

- faire avancer les activités de chasse aux cybermenaces avec les partenaires de protection cybernétique des télécommunications canadiennes en vue de détecter et d'éliminer la présence des auteurs de menace qui sont prépositionnés pour perturber les réseaux canadiens;
- cerner les risques dans les technologies mobiles patrimoniales et promouvoir les mesures d'atténuation visant à réduire l'exposition aux menaces de tous les dispositifs mobiles du gouvernement du Canada;
- donner des conseils quant aux pratiques exemplaires relatives aux modules d'identification d'abonné intégré (eSIM pour *embedded subscriber identity module*), aux cartes UICC (pour *universal integrated circuit card*) intégrées et à l'intégrité de la chaîne d'approvisionnement dans la mobilité et les réseaux privés 5G;
- mener des tests ciblés et donner des conseils en matière d'atténuation dans le cadre de nouveaux efforts dirigés par l'industrie visant à contrer les menaces globales de signalisation et à renforcer les données des abonnées et abonnés.

Salt Typhoon



À l'hiver 2025, Salt Typhoon est apparu comme une grave menace émergente aux réseaux partout dans le monde. Une fois les cyberincidents découverts, le Centre pour la cybersécurité a collaboré avec le SCRS et ses partenaires étrangers pour mieux comprendre la menace et y répondre. De cette collaboration a découlé la publication d'un bulletin de cybersécurité conjoint[6] avec la National Security Agency (NSA) et d'un bulletin de cybermenace conjoint[7] avec le Federal Bureau of Investigation (FBI), qui décrivaient la menace et recommandaient des mesures d'atténuation à prendre.

Le Centre pour la cybersécurité continue de surveiller étroitement cette menace. Il collabore étroitement avec les fournisseurs de services de télécommunications et les exploitants d'infrastructures essentielles du Canada et publie des conseils quant aux cybermenaces[8] à leur intention pour qu'ils demeurent informés et prêts.

Transport maritime

Cette année, il y avait un accent sur le renforcement de la cyberrésilience dans le secteur canadien du transport maritime. Le transport maritime est un secteur profondément connecté aux chaînes d'approvisionnement du Canada, et toute perturbation, qu'elle touche les opérations portuaires, les systèmes de navigation des navires ou le traitement des cargaisons, peut avoir d'importantes répercussions économiques et de sécurité.

En appui à ce secteur, le Centre pour la cybersécurité a publié une évaluation de la cybermenace qui pèse sur le transport maritime[9], y compris les ports et les industries connexes. Cette évaluation décrivait les rançongiciels et les activités cybercriminelles motivées par le gain financier comme représentant les risques les plus importants. Elle présentait également des conseils pratiques pour aider les exploitants à renforcer leurs mesures de défense et à réduire leur exposition aux vulnérabilités.

Secteur de la gestion de l'eau

Les systèmes d'approvisionnement en eau et des eaux usées du Canada sont essentiels à la santé et à la sécurité publiques. Ces systèmes s'activent souvent hors de vue, mais ils dépendent de plus en plus des technologies numériques, qui les exposent aux cybermenaces.

Dans ce contexte de cybermenaces en évolution, les infrastructures de gestion des eaux sont maintenant confrontées à des risques auxquels elles n'étaient pas préparées à l'origine. Étant donné que les perturbations peuvent avoir un effet domino sur d'autres secteurs des infrastructures essentielles, le CST appuie la protection des systèmes critiques et fournit du soutien afin d'améliorer leurs mesures de cyberdéfense.

Afin d'assurer la sensibilisation et de promouvoir de meilleures mesures de protection, le Centre pour la cybersécurité a publié une évaluation des cybermenaces visant les systèmes de gestion des eaux du Canada[10], qui présente des conseils clairs et des mesures d'atténuation pour aider les exploitants de systèmes de gestion des eaux à empêcher les auteurs de cybermenace de compromettre leurs systèmes, de perturber leurs services ou de voler leurs données sensibles.

Accès non autorisé à une installation de traitement de l'eau du Québec

Le 7 octobre 2025, CSIRTAmericas a relayé la revendication du groupe NoName quant à l'accès non autorisé à une installation municipale de traitement de l'eau du Québec, qui lui a donné notamment la capacité de contrôler secrètement les pompes, le dosage de chlore, les réglages de pression et les systèmes de surveillance et d'alerte. Ce renseignement opportun a permis au Centre pour la cybersécurité d'évaluer rapidement la menace et de collaborer avec les partenaires pour coordonner les efforts d'atténuation et réduire les risques à la sécurité publique.

Pour appuyer les infrastructures essentielles, il faut aussi aider les partenaires à comprendre l'environnement de menace. Pour compléter le soutien direct et l'engagement opérationnel, le CST traduit le renseignement et les observations de première ligne en rapports de menace exploitables par les organisations.

Évaluer les cybermenaces et produire des rapports

Fournir de l'information pratique et opportune sur les menaces est une part importante du soutien qu'offre le CST aux partenaires.

Tout au long de l'année, le Centre pour la cybersécurité a présenté des évaluations, des rapports techniques et des bulletins de menace non classifiés pour aider les organisations à comprendre les risques émergents et à prendre des mesures. Bon nombre de ces produits combinaient le renseignement étranger, l'analyse technique et l'information opérationnelle pour donner une vue d'ensemble de l'approche intégrée du CST en matière de sensibilisation aux menaces et de mesures de cyberdéfense. Notamment, il y a eu la publication intitulée Vue d'ensemble des menaces par rançongiciel de 2025 à 2027[11], de même que six évaluations et bulletins non classifiés sur les menaces :

- Bulletin sur les cybermenaces : Les activités de cybermenace de la République populaire de Chine : Les auteurs de cybermenace de la RPC ciblent les entreprises de télécommunications dans le cadre d'une campagne mondiale de cyberespionnage[12]
- Bulletins sur les cybermenaces : Cybermenace de l'Iran visant le Canada émanant du conflit entre Israël et l'Iran[13]
- Les cybermenaces visant les systèmes de gestion des eaux du Canada : évaluation et atténuation[14]
- La cybermenace qui pèse sur le transport maritime[15]
- Bulletin sur les cybermenaces : Intervention en cas de cybermenaces iraniennes émanant des frappes des États-Unis et d'Israël, février 2026[16]
- Cyberbulletin : Cyberactivités parrainées par la République populaire de Chine et menées contre les gouvernements provinciaux, territoriaux et autochtones et les administrations municipales du Canada[17]

Vue d'ensemble des menaces par rançongiciel de 2025 à 2027

La publication Vue d'ensemble des menaces par rançongiciel de 2025 à 2027[18] a présenté un aperçu clair des menaces par rançongiciel et leur évolution au Canada. Elle aide les organisations canadiennes à comprendre comment la menace évolue et présente des avis et conseils pratiques du Centre pour la cybersécurité, qui visent à renforcer la cyberrésilience et à assurer la préparation en cas de cyberincident.

Le rapport aborde l'historique des rançongiciels, de même que les tendances émergentes et prévues, et réfute et les mythes courants et les idées fausses. La publication relève quatre observations :

- **Les rançongiciels sont une menace croissante :** Les auteurs de menace utilisent des outils et des techniques avancés pour augmenter l'ampleur et l'incidence des attaques.
- **Les auteurs de menace s'adaptent :** Ils tirent parti de nouvelles technologies, comme l'IA et la cryptomonnaie, tout en élaborant de nouvelles tactiques d'extorsion pour accroître leurs gains financiers.
- **Les pratiques exemplaires de base en cybersécurité fonctionnent :** Les mesures de protection les plus efficaces demeurent les mises à jour logicielles régulières, l'authentification multifacteur (AMF) et la vigilance contre les activités suspectes.
- **La collaboration est essentielle :** Les gouvernements, l'industrie, les organismes d'application de la loi et les personnes ont tous un rôle à jouer pour réduire les risques.

La publication a suscité un fort intérêt des médias et a fait l'objet d'une grande couverture à la suite de sa publication en janvier 2026 et elle a aidé à accroître la sensibilisation aux menaces par rançongiciel partout au Canada.

Comprendre les menaces n'est toutefois qu'une partie de la réponse. Le CST traduit également ses connaissances en conseils pratiques, en outils et en analyses techniques pour aider les responsables de la défense à renforcer la résilience et à réduire les risques à la cybersécurité au Canada. Le CST tire parti de ses pleins pouvoirs pour protéger les Canadiennes et les Canadiens contre les cybermenaces.

Renforcer la cyberrésilience et la cyberdéfense du Canada

Les cybermenaces continuent de gagner en ampleur et en sophistication. Les auteurs de menace s'adaptent constamment et trouvent de nouvelles façons de cibler les organisations et les personnes. Tout comme les cybermenaces, les documents d'orientation mis à la disposition de la population canadienne continuent d'évoluer.

Le Centre pour la cybersécurité fournit aux Canadiennes et Canadiens des documents d'orientation pratiques et accessibles pour les aider à garder une longueur d'avance sur ces menaces. Que ce soit pour appuyer le gouvernement, les infrastructures essentielles ou les personnes, ces documents d'orientation permettent de renforcer les mesures de défense et d'accroître l'état de préparation à l'échelle du pays.

Documents d'orientation sur la cybersécurité

Cette année, le Centre pour la cybersécurité a publié un large éventail de documents d'orientation pour appuyer les organisations et les personnes, des spécialistes techniques aux hautes dirigeantes et hauts dirigeants du gouvernement et du secteur privé.

Parmi les sujets abordés, mentionnons l'intelligence artificielle, la sécurité infonuagique, l'utilisation de drones et la préparation aux situations d'urgence. Cet effort a également favorisé l'adoption de pratiques de sécurisation dès la conception au gouvernement, notamment au moyen de documents d'orientation en architecture de sécurité d'entreprise à l'intention des ministères.

Le Centre pour la cybersécurité a également amélioré ses processus d'élaboration et de diffusion des documents d'orientation, pour permettre une prestation plus rapide et mieux coordonnée.

En tout, il a publié :

- **41** documents d'orientation sur la cybersécurité;
- **28** publications élaborées conjointement avec les partenaires étrangers et de la collectivité des cinq.

Les 10 mesures de sécurité en matière d'intelligence artificielle : Introduction

En mars 2026, le Centre pour la cybersécurité a publié un document d'orientation ponctuel visant à encourager les Canadiennes et Canadiens à adopter des mesures de sécurité conçues pour contrer les menaces liées à l'IA[19]. Que ce soit à l'échelle individuelle ou collective, ces mesures sont essentielles pour préserver la confidentialité des renseignements et éviter que des fonds durement gagnés ne soient volés dans le cadre d'activités malveillantes facilitées par l'IA. À mesure que les modèles évoluent, cela exige une surveillance continue et une supervision humaine pour les décisions critiques pour faire en sorte que les systèmes d'IA respectent les limites acceptables en ce qui a trait au risque. Il est conseillé aux organisations de mettre en œuvre ces 10 mesures de sécurité des TI[20] visant à protéger les réseaux Internet et l'information contre les cybermenaces à la sécurité.

Outils permettant aux responsables de la cyberdéfense de garder une longueur d'avance sur les menaces

Le Centre pour la cybersécurité continue d'élargir sa gamme d'outils de source ouverte afin de soutenir les responsables de la cyberdéfense et de promouvoir les pratiques de sécurisation dès la conception.

En octobre 2025, le Centre pour la cybersécurité a lancé l'outil **Clue**, un cadre d'enrichissement qui aide les analystes à découvrir les incidents de cybersécurité, à en faire l'examen, à les trier et à les signaler plus rapidement. Clue s'intègre à d'autres outils de source ouverte du Centre pour la cybersécurité. Il est accessible sur GitHub.

Parallèlement, le système d'analyse de maliciels **Assemblyline** a traité des volumes exceptionnellement élevés cette année, ce qui a permis au gouvernement du Canada et à ses partenaires de procéder à des analyses plus rapides.

En accélérant la rapidité avec laquelle les menaces sont repérées et comprises, ces outils aident les responsables de la cyberdéfense à intervenir plus rapidement, ce qui réduit le risque de perturbation des systèmes et services critiques sur lesquels comptent les Canadiennes et Canadiens au quotidien. Alors que les cybermenaces s'intensifient, les travaux d'innovation menés au moyen d'outils comme Clue et Assemblyline aident le Canada à garder une longueur d'avance sur les menaces et à renforcer sa première ligne de défense numérique.

Rapports d'analyse technique

Le Centre pour la cybersécurité a également publié plusieurs rapports d'analyse technique de grande portée pour aider les organisations canadiennes à mieux comprendre les menaces émergentes.

S'appuyant sur des enquêtes menées en contexte réel et sur des observations à grande échelle, ces rapports offrent un aperçu des méthodes qu'utilisent les auteurs de menace étatiques et criminels pour mener des attaques modernes, ainsi que des moyens de se défendre contre ces attaques.

Cette année, le Centre pour la cybersécurité a publié trois rapports d'analyse technique. Les rapports portaient sur :

- les attaques de type adversaire au milieu grâce à une authentification multifacteur résistante à l'hameçonnage[21] ciblant Entra ID (anciennement Azure AD);
- les techniques utilisées par des auteurs de menace pour exploiter les vulnérabilités dans des serveurs locaux de SharePoint[22];
- la technique EtherHiding[23], une attaque impliquant du code malveillant caché dans des outils de développement.

En communiquant des constatations détaillées, des indicateurs et des recommandations en matière de défense, le Centre pour la cybersécurité a aidé les responsables de la cyberdéfense à renforcer leurs capacités de détection de même que la cyberrésilience globale de leur organisation.

Améliorations stratégiques en matière de défense et de sécurité

Face à l'évolution des défis mondiaux en matière de sécurité, le Canada doit être prêt à défendre son territoire et ses valeurs, à assurer sa souveraineté et à respecter ses engagements envers ses alliés.

La nature des conflits a évolué au-delà des champs de bataille physiques pour inclure le cyberespace et les domaines numériques. Les percées dans les domaines de l'IA, de l'informatique quantique et des systèmes autonomes redéfinissent la façon dont les pays protègent leurs intérêts et progressent vers leurs objectifs de sécurité.

Au cours de la dernière année, le CST a jeté les bases des priorités essentielles en matière de sécurité nationale, de défense et de résilience. Ces améliorations reflètent un engagement commun du CST, des Forces armées canadiennes et de la collectivité de la sécurité et du renseignement à défendre le Canada et à protéger la population canadienne. L'objectif commun : renforcer la sécurité nationale du pays dans un contexte de menace de plus en plus complexe. Pour ce faire, il faut notamment :

- mettre au point **une infrastructure numérique et des outils sécurisés modernes** pour les Forces armées canadiennes et la collectivité de la sécurité et du renseignement;
- augmenter la capacité de cyberdéfense pour **soutenir les opérations militaires en cours**;
- travailler avec le gouvernement, le milieu universitaire et l'industrie à l'élaboration de **solutions d'IA canadiennes**.

Le CST poursuit ses efforts en matière d'innovation et de résilience, renforçant la capacité du Canada à évoluer de façon sécurisée, décisive et assurée dans un environnement de sécurité de plus en plus complexe.

Contribuer à un Canada numérique souverain et sécurisé

Alors que le CST poursuit ses efforts en matière d'innovation et de résilience, le budget de 2025 a mis en évidence le rôle essentiel que joue l'organisme dans le renforcement de la capacité du Canada à évoluer de façon sécurisée, décisive et assurée dans un environnement de sécurité de plus en plus complexe. Cet important investissement dans le CST soutiendra une transformation pluriannuelle qui renforcera la sécurité nationale, la compétitivité économique et la souveraineté numérique, tout en améliorant l'interopérabilité des systèmes au Canada et à l'étranger.

Stimuler la transformation numérique et la résilience

En collaboration avec des partenaires de la collectivité de la défense, de la sécurité et du renseignement, le CST améliorera la façon dont l'information est analysée et communiquée en toute sécurité, surtout en période de crise et de conflit. Les investissements générationnels renforceront la capacité du Canada à :

- protéger l'information, les communications et les opérations de nature délicate;
- déployer des capacités modernes et très efficaces;
- intégrer les technologies émergentes comme l'intelligence artificielle pour appuyer la prise de décisions plus éclairées;
- collaborer en toute sécurité avec des partenaires de confiance.

Le déploiement de ces capacités exige une infrastructure informatique résiliente et performante ainsi qu'une main-d'œuvre hautement qualifiée. À cette fin, le CST a commencé à prévoir ses besoins en matière de centres de données et de biens immobiliers, en priorisant les investissements dans les collectivités et les industries canadiennes. Ces investissements fondamentaux contribueront à l'accroissement de la présence nationale du CST, ce qui lui permettra de se développer à mesure que ses besoins évoluent.

Expansion de la présence du Réseau canadien Très secret

Le CST continue d'élargir et de moderniser ses infrastructures de communications sécurisées afin de soutenir les opérations gouvernementales et de répondre aux besoins croissants en matière d'accès au renseignement. Ces efforts comprennent le déploiement d'un Réseau canadien très secret (RCTS) résilient et unifié, offrant à un plus grand nombre de ministères et organismes un accès sécurisé au renseignement.

Cette année, le RCTS a pris de l'expansion pour inclure huit membres fédéraux et a continué de soutenir les opérations à l'étranger au moyen de postes de travail sécurisés portables. Ensemble, ces capacités offrent une connectivité souple et sécurisée aux utilisatrices et utilisateurs au Canada et à l'étranger.

Solutions infonuagiques

Le CST poursuit l'élaboration de solutions infonuagiques à l'appui de la stratégie d'informatique en nuage classifiée du gouvernement du Canada, en collaboration avec le ministère de la Défense nationale et Services partagés Canada. Les organismes à sécurité élevée comme le CST et le ministère de la Défense nationale travaillent quotidiennement avec des renseignements classifiés qui nécessitent une protection accrue et une infrastructure numérique sécurisée. Le CST et ses partenaires fédéraux reconnaissent le rôle essentiel de l'informatique en nuage dans un ensemble plus vaste de capacités techniques pour assurer la sécurité nationale et rendre durable l'infrastructure des communications du Canada. Grâce à sa portée dans les domaines de la cybersécurité, de l'informatique quantique, de l'intelligence artificielle et de la cryptographie, le contrôle du Canada sur les données sensibles est davantage renforcé.

La cryptographie au Canadaet la transition vers la cryptographie post-quantique

En tant qu'autorité nationale du Canada en matière de renseignement électromagnétique étranger, de cybersécurité et d'assurance de l'information, le CST joue un rôle clé dans la prévision des nouvelles menaces cryptographiques, notamment celles liées aux avancées dans le domaine des technologies quantiques.

Le CST dirige les efforts déployés à l'échelle du gouvernement pour se préparer à une transition sécuritaire vers la cryptographie post-quantique (CPQ), renforcer son programme COMSEC et travailler avec des partenaires et l'industrie canadienne pour élaborer des solutions sûres et souples qui peuvent s'adapter aux nouvelles menaces et répondre aux futurs besoins Cette année, en étroite collaboration avec ses partenaires de confiance, le CST a également travaillé à sensibiliser davantage le secteur privé aux besoins du gouvernement du Canada en matière de sécurité cryptographique, ce qui a permis une plus grande participation et soutenu la croissance d'une industrie nationale.

Cette année, le CST a publié la Feuille de route pour la migration vers la cryptographie post-quantique au sein du gouvernement du Canada[24]. Elle fournit aux ministères une approche par étapes bien définie pour appuyer la planification et la mise en œuvre. Pour soutenir l'adoption, le Centre pour la cybersécurité a également offert un programme d'apprentissage visant à sensibiliser les fonctionnaires et à les aider à se préparer. Parallèlement, il a fait évoluer l'approvisionnement post-quantique en travaillant en étroite collaboration avec Services publics et Approvisionnement Canada et Services partagés Canada pour intégrer les exigences en matière de CPQ au processus de passation de marchés.

Le CST a également renforcé la coordination et l'engagement international :

- en présidant un groupe de travail interministériel sur la migration vers la CPQ;
- en dirigeant le Groupe de travail sur la cybersécurité du G7 sur la préparation post-quantique;
- en contribuant à l'élaboration de normes.

Les concepts de défense du Canada et de renforcement du Canada ne s'excluent pas mutuellement. Dans le contexte de la Stratégie industrielle de défense, le renforcement de la sécurité cryptographique aujourd'hui contribuera à préserver la souveraineté du Canada pour les générations futures.

Soutenir la Stratégie industrielle de défense du Canada

Le Canada a amorcé une nouvelle période d'investissement en défense nationale, et le CST soutient directement la Stratégie industrielle de défense (SID)[25]. La stratégie mobilise des ressources à l'échelle du Canada afin de renforcer sa capacité technologique, de développer l'expertise nationale et de consolider la souveraineté du pays.

Alors que les opérations de défense s'appuient de plus en plus sur les systèmes numériques, le CST soutient la capacité du Canada à s'adapter en misant sur la recherche et l'innovation, en soutenant des chaînes d'approvisionnement robustes et en collaborant avec l'industrie pour offrir des capacités modernes.

> *« La nature changeante de la guerre est en train de remodeler la sécurité mondiale. Les conflits s'étendent désormais au-delà des champs de bataille traditionnels dans le cyberespace, l'espace et le domaine numérique, alimentés par des technologies telles que l'IA, les systèmes quantiques et autonomes, la robotique et les capacités cybernétiques et spatiales avancées. Les pays s'efforcent d'exploiter les innovations commerciales non seulement pour sauvegarder leur souveraineté, mais aussi pour tirer parti des avantages économiques qu'elles procurent. »*
>
> *Stratégie industrielle de défense du Canada*[26]

Bureau de recherche, d'ingénierie et de leadership avancés en matière d'innovation et de science

Le Bureau de recherche, d'ingénierie et de leadership avancés en matière d'innovation et de science (BOREALIS) est l'une des principales initiatives de la SID.

En réunissant les partenaires du gouvernement, du milieu universitaire et de l'industrie, BOREALIS constitue un carrefour central pour promouvoir l'innovation en matière de défense et de sécurité nationale. Il vise à accélérer la mise au point de capacités avancées dans le domaine des technologies de défense et de sécurité, comme l'IA et l'informatique quantique.

En tant que membre du Bureau de programme conjoint de BOREALIS, le CST contribue à faire progresser cette initiative et à en définir l'orientation.

Cette année, le CST a contribué à définir les priorités de BOREALIS, a appuyé l'élaboration de politiques et a travaillé avec l'industrie et le milieu universitaire afin de promouvoir un nouveau cadre de collaboration avec le gouvernement, le milieu universitaire et l'industrie dans le domaine des technologies de défense.

Intelligence artificielle

Au cours de la dernière année, le CST a poursuivi le déploiement de sa Stratégie en matière d'intelligence artificielle[27], en développant sa capacité à utiliser des outils d'IA tout en intégrant de solides mécanismes de gouvernance, de gestion des risques et de protection éthique.

Pour le CST, l'IA n'est pas une chose nouvelle. Depuis plusieurs années, l'organisme développe, adapte et exploite des outils d'IA, d'automatisation, d'apprentissage automatique et de science des données pour favoriser un travail plus efficace, produire des analyses plus rapidement et renforcer les capacités opérationnelles.

Les investissements dans les technologies de pointe permettent au CST de déployer l'IA à plus grande échelle dans l'ensemble de ses activités. Il s'agit notamment d'accroître l'efficacité au sein de l'organisme en automatisant les tâches courantes, en produisant des analyses plus rapidement et en offrant au personnel le soutien nécessaire pour se concentrer sur des activités à valeur ajoutée. Parallèlement, ces technologies renforcent les capacités d'analyse des menaces, de cyberdéfense et de cybersécurité dans un environnement de menace en constante évolution et toujours plus complexe.

Le CST collabore activement avec les partenaires du gouvernement, du milieu universitaire et de l'industrie pour échanger des idées, harmoniser les pratiques exemplaires et progresser vers les priorités communes en matière d'IA responsable. Ces partenariats permettent de doter l'effectif d'outils de pointe et de savoir-faire, tout en favorisant des solutions sécurisées et adaptées qui améliorent l'efficacité opérationnelle et contribuent à la défense du Canada face aux cybermenaces facilitées par l'IA.

Face à l'évolution rapide des capacités d'IA, notamment les modèles de pointe de plus en plus performants, le CST continue de suivre ces avancées de près et de s'adapter en conséquence. Il surveille activement l'utilisation abusive de l'IA par des auteurs de menace et prend des mesures pour prévenir une telle utilisation, puisque ces outils peuvent contribuer à l'émergence de cybermenaces plus sophistiquées, évolutives et persistantes tout en réduisant l'intervalle entre la découverte de la vulnérabilité et l'exploitation de celle-ci.

Grâce à son leadership et à son expertise technique en matière d'IA de pointe, le CST veille à ce que ces technologies soient adoptées en toute sécurité et de façon responsable partout au Canada. Cela comprend une collaboration étroite avec des partenaires, notamment des secteurs des infrastructures essentielles, afin de renforcer la résilience et de se préparer

à faire face à des menaces plus avancées. Il continue de partager du renseignement avec ses partenaires et poursuit ses efforts de recherche pour aider le Canada à garder une longueur d'avance sur les menaces évolutives facilitées par l'IA.

Grâce à une expertise établie, une innovation responsable et des partenariats stratégiques, le CST est bien placé pour exploiter l'IA de façon à assurer la sécurité nationale, la prospérité économique et les valeurs démocratiques du Canada.

Exploiter l'IA pour renforcer l'analyse de renseignement étranger

Le CST intègre des solutions d'IA pour renforcer l'analyse du renseignement électromagnétique en améliorant la façon dont les analystes traitent des données massives et complexes. En appliquant ces technologies aux mesures de protection et aux cadres de gestion des risques bien établis, le Canada peut améliorer l'efficacité opérationnelle tout en maintenant la confiance, la responsabilité et la surveillance humaine nécessaires à une utilisation responsable.

De nouvelles approches sont mises à l'essai pour :

- automatiser les tâches répétitives exigeant un grand volume de données;
- permettre aux analystes de consacrer plus de temps à la prise de décisions et aux analyses à valeur ajoutée;
- optimiser la recherche, la compréhension et l'utilisation de l'information.

À titre d'exemple, le CST élabore un outil intégrant l'IA qui peut :

- traduire des données de plus de 200 langues vers l'anglais et le français au moyen de grands modèles de langage;
- extraire des informations pertinentes de grands jeux de données;
- traiter des échanges dialogués par clavardage, permettant la formulation de questions en langage naturel;
- faire des recherches plus précises au moyen de l'analyse sémantique, en permettant l'interrogation des données selon l'intention du texte plutôt que de simples correspondances lexicales;
- organiser et analyser les données en utilisant des modèles thématiques, permettant de visualiser les données par thème ou sujet.

MOBILISER LA RECHERCHE ET LES PARTENARIATS POUR ASSURER L'AVENIR

Pour assurer l'avenir du Canada et garder une longueur d'avance sur les menaces en constante évolution, il ne suffit pas d'exploiter des technologies – il faut instaurer une collaboration.

En s'appuyant sur la recherche et les partenariats, le CST met au point les outils et les capacités nécessaires pour relever les défis actuels en matière de cybersécurité et se préparer à ceux à venir. Puisqu'aucune organisation ne peut à elle seule relever ces défis, l'organisme collabore avec tous les ordres de gouvernement, les exploitants d'infrastructures essentielles, le milieu universitaire et les alliés internationaux. L'objectif commun est de relever des défis complexes en matière de cybersécurité, en renforçant la souveraineté numérique du Canada et en établissant un environnement de cybersécurité plus résilient.

Renforcer les capacités essentielles à la mission par la recherche

Le CST transforme les idées novatrices en solutions opérationnelles. En collaboration avec des partenaires du gouvernement, du milieu universitaire et de l'industrie, la Direction générale de la recherche s'emploie à trouver des solutions aux défis complexes et persistants dans le cadre de la mission du CST.

Recherche sur l'intelligence artificielle et l'apprentissage automatique

Cette année, les équipes de recherche du CST en matière d'intelligence artificielle et d'apprentissage automatique ont concentré leurs efforts sur le développement et l'application responsable de ces technologies dans des environnements sécurisés. Elles ont élaboré et testé des modèles sur mesure pour répondre aux besoins prioritaires de l'organisme, comme l'analyse de grandes quantités de données multimédia. Elles ont également créé des jeux de données d'évaluation afin de permettre au CST et à ses partenaires d'évaluer adéquatement le comportement des modèles d'apprentissage automatique avant leur intégration dans les opérations.

Hors de l'environnement de laboratoire, les équipes de recherche ont mis à contribution leur expertise et leur soutien à l'échelle du CST et aux partenaires :

- en organisant des séances avec les partenaires de la collectivité des cinq et d'autres ministères du gouvernement du Canada;
- en participant aux ateliers phares du CST sur l'innovation et la collaboration, comme la Grande exploration, Kickstart et GeekWeek;
- en planifiant des séances mensuelles consacrées à l'apprentissage automatique;
- en offrant une formation pratique, notamment des modules sur la science des données.

Ce travail permet l'application responsable et efficace de l'IA, en soutien aux opérations.

Recherche sur les vulnérabilités

Le Centre de recherche sur les vulnérabilités[28] du CST mène des efforts de recherche appliquée pour cerner et atténuer les vulnérabilités en matière de cybersécurité à l'appui de son mandat.

Au cours de la dernière année, les travaux réalisés avec le laboratoire de sécurité informatique du Collège militaire royal du Canada ont mené au développement de nouvelles techniques de détection et à la divulgation responsable de trois vulnérabilités à des partenaires de l'industrie, notamment Microsoft et Netgear.

Ces efforts permettent de réduire les risques dans l'ensemble de l'environnement de cybersécurité.

Institut Tutte pour les mathématiques et le calcul

Au cours de la dernière année, l'Institut Tutte pour les mathématiques et le calcul (ITMC) a continué de développer des théories fondamentales, des techniques novatrices et des outils efficaces dans deux principaux domaines d'étude : les principes mathématiques de la cryptographie et les rudiments de l'intelligence artificielle et de l'apprentissage automatique. L'engagement et la collaboration avec des communautés de recherche dynamiques, dans des contextes classifiés et non classifiés, ont permis à l'ITMC de produire d'importants résultats de recherche.

Contribution aux progrès scientifiques

L'ITMC travaille à rendre accessibles ses activités et ses outils au public et à la communauté universitaire sur une base régulière.

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

- publier 10 articles de revues et 1 livre;
- produire 16 versions de logiciels contenant du nouveau code ou modifiant du code;
- organiser 3 conférences;
- réviser les travaux de 1 congrès;
- participer à 6 discussions et à 3 présentations lors de conférences externes;
- occuper des places au Conseil d'administration de la Société mathématique du Canada et des comités.

Par ailleurs, un grand nombre de personnes effectuent plus de 6,5 millions de téléchargements chaque mois à partir des bibliothèques de logiciels de l'ITMC, ce qui accroît l'influence du Canada dans les domaines de cybersécurité et de recherche mathématique.

Collaboration avec les universités de la région de la capitale nationale

À Ottawa et à Gatineau, l'ITMC travaille avec les universités au perfectionnement de personnel hautement qualifié, en soutenant des événements universitaires et en collaborant aux travaux de recherche.

Communautés de recherche du CST et du CRSNG

Le CST, en partenariat avec le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), offre un soutien aux communautés de recherche qui mènent des recherches non classifiées sur les technologies de pointe d'importance stratégique pour le CST et le gouvernement du Canada.

Cette année, le CST a eu le plaisir d'annoncer la création de la communauté de recherche du CST et du CRSNG sur l'analyse exploratoire des données non structurées dans le cadre du projet intitulé *ZenithVector: Advanced Vectorization, Embedding, and Cybersecurity Analytics Toolkit for Scalable Intelligence*[29]. Sous la direction de l'Université McGill, ce projet réunit des chercheuses et chercheurs provenant de 10 universités canadiennes pour étudier l'analyse de données à grande échelle.

L'objectif est d'élaborer une solution multimodale complète pour l'analyse exploratoire des grandes collections de données non structurées (p. ex. texte, code et images). Le projet intègre des techniques avancées pour élaborer les éléments de base nécessaires à la compréhension, l'exploration et la visualisation des collections de données non structurées d'une manière qui soit logique pour le cerveau humain.

C'est la deuxième de quatre communautés créées dans le cadre des subventions CRSNG-CST à l'appui des communautés de recherche[30].

Nouveau centre de collaboration en matière de recherche à Toronto

Le CST cherche régulièrement des occasions de renforcer la collaboration avec les chercheuses et chercheurs canadiens. Dans le cadre d'un nouveau partenariat avec le Conseil national de recherches du Canada (CNRC), l'organisme travaille à accroître sa présence et à établir un nouveau centre de collaboration au centre-ville de Toronto. Situé dans le noyau universitaire de la ville, le centre facilitera les échanges en personne, le partage de connaissances et l'établissement de partenariats de recherche. La proximité du Centre de collaboration en sciences mathématiques CNRC-Fields contribuera à renforcer les liens entre la recherche publique et la communauté universitaire canadienne en mathématiques.

Protéger le Canada grâce à une approche pansociétale

La cybersécurité est une responsabilité partagée.

La complexité des menaces actuelles fait en sorte qu'aucune organisation du secteur public ou privé ne peut gérer ces menaces seule. Le CST s'appuie sur diverses perspectives du gouvernement et de l'extérieur afin de consolider ses connaissances et ses capacités collectives, et ainsi mener à bien sa mission.

Collectif canadien de cyberdéfense

Cette année, dans le cadre de la Stratégie nationale de cybersécurité, le gouvernement du Canada a mis sur pied le Collectif canadien de cyberdéfense (CCCD). Il a pour objectif de renforcer et de faire progresser la cyberrésilience du Canada par l'intermédiaire d'interventions directes des secteurs public et privé concernant les défis nationaux, les priorités stratégiques et les opérations en matière de cybersécurité.

Le CCCD veille à ce que les exploitants d'infrastructures essentielles, les entreprises, les gouvernements provinciaux et territoriaux, les administrations municipales, les gouvernements autochtones et la population canadienne bénéficient du partage de renseignement, d'innovations et de pratiques exemplaires. Cette initiative renforce la capacité du Canada à détecter, à prévenir et à contrer les cyberactivités malveillantes, créant ainsi un contexte numérique sûr pour les Canadiennes et Canadiens.

Le CCCD comprend deux forums distincts, soit le Forum opérationnel et le Forum stratégique.

Le Forum opérationnel est présidé par le Centre pour la cybersécurité et assume les responsabilités suivantes :

- tirer parti des partenariats pour coordonner des interventions à l'échelle nationale afin de contrer les cybermenaces;
- contribuer au développement du renseignement sur les cybermenaces;
- consolider l'échange d'information;
- mettre en œuvre des stratégies techniques pour atténuer les défis relatifs à la cybersécurité;
- développer conjointement des solutions de cyberdéfense, en établissant entre autres une stratégie de collaboration par niveau afin de coopérer avec des collectivités de cyberdéfense.

Le Forum opérationnel est formé d'un groupe restreint de partenaires de cyberdéfense nationaux et internationaux qui sont dignes de confiance et qui proviennent des secteurs privé et public. Des réunions bilatérales et multilatérales préliminaires ont été amorcées et opérationnalisées en 2025, ouvrant la voie à la collaboration sur les plans opérationnel et analytique. Le groupe s'est employé à mettre sur pied les premiers partenariats, processus et technologies nécessaires pour soutenir un travail coordonné avec les partenaires de l'industrie.

Le Forum stratégique, coprésidé par Sécurité publique Canada et le Centre pour la cybersécurité, est le comité consultatif du Canada pour tout ce qui touche à la cybersécurité. Parmi ses membres, on trouve des partenaires des secteurs public et privé qui prennent part à des discussions générales, orientent les priorités nationales et font front commun pour formuler des solutions de cybersécurité dont peut tirer parti le Canada.

Présence régionale à Montréal

Cette présence locale rend les services plus accessibles, renforce les relations avec des partenaires clés à tous les ordres de gouvernement et ailleurs, et favorise un échange d'information bidirectionnel.

En 2025, l'équipe de Montréal a mené plus de 100 activités de sensibilisation et de mobilisation dans les secteurs de la cybersécurité et du renseignement. Les activités comprenaient les suivantes :

- des conférences;
- des discussions en groupe;
- des séances d'information sur les services;
- une collaboration avec les équipes de recrutement lors de salons de l'emploi;
- des présentations offertes conjointement avec d'autres services de sécurité et de renseignement de la région de Montréal;
- des séances d'information classifiées sur les cybermenaces à des partenaires ayant une habilitation de sécurité correspondante.

Les premiers commentaires recueillis auprès des partenaires locaux sont positifs.

Déjeuners consultatifs de la chef

Le CST continue d'approfondir ses partenariats avec l'industrie.

Dans le cadre d'initiatives comme les déjeuners consultatifs de la chef, le CST tisse des liens avec des leaders de divers secteurs pour discuter des difficultés et des possibilités communes.

Cette année, les séances visaient à faciliter le dialogue sur les grandes priorités du CST, notamment :

- attirer, former et maintenir en poste les talents des secteurs des TI, de la défense, et de la sécurité et du renseignement au Canada;
- la dynamique et les occasions de renforcer la collaboration et les partenariats entre le CST, le gouvernement du Canada, l'industrie et le milieu universitaire.

Les déjeuners consultatifs appuient les efforts déployés par le CST pour accroître la collaboration avec les partenaires de l'industrie. Ce dialogue oriente le travail de l'organisme et lui permet de s'adapter aux besoins changeants du Canada.

Mise à l'essai et évaluation de solutions de l'industrie

Pour accélérer l'innovation, le CST améliore ses mécanismes d'essai et d'adoption de nouvelles technologies.

Le CST reconnaît que l'industrie joue un rôle important dans l'innovation et qu'elle peut appuyer son mandat de sécurité nationale; toutefois, la réalisation de projets pilotes dans un environnement sécurisé comporte des défis.

Cette année, le CST a collaboré avec un facilitateur externe pour accélérer sa capacité à mettre à l'essai et à évaluer des solutions non classifiées de l'industrie. La première autorisation de tâche a permis aux équipes opérationnelles d'évaluer plusieurs solutions de l'industrie à la fois, ce qui a accéléré la transition de projet pilote à une capacité évolutive et contribué à éclairer les décisions d'approvisionnement futures. Des tâches supplémentaires sont toujours en cours d'élaboration.

Partenariats avec les communautés autochtones

Le Centre pour la cybersécurité travaille en collaboration avec les communautés autochtones pour renforcer la cyberrésilience et appuyer les priorités communes en matière de sécurité.

L'équipe d'engagement auprès des Autochtones établit des relations de nation à nation fondées sur le respect, la reconnaissance des droits et la collaboration. L'organisme respecte le principe « rien pour elles sans elles », veillant ainsi à ce que les initiatives et les projets soient élaborés conjointement et qu'ils tiennent compte des priorités et des besoins particuliers des communautés.

Cette année, l'équipe a :

- contribué au groupe de travail sur la sécurité dans l'Arctique, réunissant les gouvernements fédéral, territoriaux et autochtones;
- participé à la conférence de l'Alliance nationale autochtone des technologies de l'information;
- fourni des conseils, des services et des avis en matière de cybersécurité aux organisations autochtones;
- renforcé les relations avec les organisations autochtones afin d'assurer la coordination et l'intervention en cas d'incident de cybersécurité;
- diffusé auprès des gouvernements autochtones un bulletin sur les cybermenaces concernant les cyberactivités parrainées par la RPC visant tous les ordres de gouvernement;
- collaboré avec des partenaires pour intégrer les communications liées aux incidents de cybersécurité et les breffages sur les menaces dans les canaux fédéraux-autochtones de confiance;
- soutenu l'engagement des membres de la direction, notamment des discussions dirigées par des Inuit, ayant mené à une plus grande collaboration et à des activités de sensibilisation proactive aux incidents.

De janvier à mars 2026, le Centre pour la cybersécurité, en collaboration avec les partenaires fédéraux d'Affaires mondiales Canada, du ministère de la Défense nationale, du Service canadien du renseignement de sécurité et d'Innovation, Sciences et Développement économique Canada, a livré des séances d'information adaptées aux communautés autochtones sur le contexte des menaces dans le Nord. Ces efforts ont renforcé les relations entre les communautés autochtones et le Centre pour la cybersécurité, ce qui lui a permis de fournir des conseils et des services adaptés afin de pouvoir accroître leur cyberrésilience.

En février 2026, les membres de la haute direction du Centre pour la cybersécurité ont joué un rôle de premier plan lors du Sommet sur la sécurité dans l'Arctique, où ils ont prononcé un discours principal et participé à une discussion en groupe. L'événement, tenu à Whitehorse, a réuni des communautés autochtones, des partenaires de l'Arctique et des décisionnaires afin de renforcer les relations en ce qui concerne les cybermenaces, la cyberrésilience et les pratiques exemplaires dans les collectivités nordiques et éloignées.

Les contributions à ShadowServer

Cette année, le Centre pour la cybersécurité a travaillé avec ShadowServer, un organisme sans but lucratif, pour échanger des alertes de sécurité. Guidé par un objectif commun visant à recueillir et à analyser des données sur les menaces mondiales, ShadowServer a communiqué des renseignements essentiels qui ont alimenté le Système national de notification de cybermenace du Centre pour la cybersécurité. À son tour, le Centre pour la cybersécurité a fourni de l'expertise et des conseils à la communauté de ShadowServer afin d'améliorer la détection et le signalement des vulnérabilités critiques et des dispositifs compromis.

Partenariats internationaux

Les cybermenaces sont de portée mondiale : elles transcendent les frontières et évoluent à grande vitesse. La collaboration internationale est essentielle à l'approche pansociétale du Canada en matière de cybersécurité.

En œuvrant aux côtés de ses alliés, notamment la collectivité des cinq, le CST progresse vers les priorités communes et appuie les efforts visant à promouvoir la cyberrésilience, la stabilité et les comportements responsables dans le cyberespace.

Groupe de travail à composition non limitée des Nations Unies sur les technologies de l'information et des communications

Le CST appuie les efforts d'Affaires mondiales Canada visant à renforcer le rôle du Canada au sein du Groupe de travail à composition non limitée (GTCNL) des Nations Unies sur les technologies de l'information et des communications (TIC).

Le CST a ainsi contribué à l'élaboration de règles, de normes et de principes pour promouvoir un comportement responsable des États dans le cyberespace. Au terme du mandat de quatre ans du GTCNL en juillet 2025, les États membres ont convenu d'établir un mécanisme permanent pour poursuivre et approfondir les discussions sur les TIC dans le contexte de la sécurité internationale. Le CST continuera d'appuyer la participation du Canada.

Groupe de travail sur la cybersécurité du G7

Lors de la présidence canadienne du G7 en 2025, le CST et Sécurité publique Canada ont coprésidé le Groupe de travail sur la cybersécurité du G7, favorisant ainsi la coopération internationale entre les autorités nationales de cybersécurité des pays du G7. Sous la direction du Canada, le CST a élaboré conjointement des conseils techniques sur l'IA, la cryptographie post-quantique et d'autres sujets clés. Le groupe a également favorisé une compréhension partagée des approches opérationnelles et stratégiques qui soutiennent une culture de cybersécurité, et a publié une déclaration commune sur la sécurité des produits d'Internet des objets.

Consolider les relations avec l'OTAN

Le Centre pour la cybersécurité renforce sa collaboration avec les partenaires de l'OTAN en matière de cyberdéfense.

Une visite importante au début de 2026 au National Cyber Security Centre de l'OTAN et à l'Agence d'information et de communication de l'OTAN a permis de faire avancer les discussions sur les capacités communes, le partage d'outils et les possibilités pour le Canada d'appuyer les nouvelles initiatives de l'OTAN. Ces échanges témoignent d'une volonté commune de renforcer la collaboration. L'option de déployer une ou un membre canadien du personnel intégré pour appuyer ce travail est à l'étude

Renforcement des relations entre les équipes d'intervention en cas d'incident lié à la cybersécurité

Au cours de la dernière année, le Centre pour la cybersécurité a renforcé ses relations avec les équipes d'intervention en cas d'incident lié à la cybersécurité de plusieurs pays de l'OTAN dans le cadre d'engagements bilatéraux et d'échanges techniques. Il a également collaboré étroitement avec des partenaires américains pour appuyer les efforts de préparation en matière de cybersécurité en vue de la Coupe du Monde de la FIFA 2026™.

Ces efforts ont contribué à consolider les partenariats de confiance et à faciliter l'échange de connaissances opérationnelles, de pratiques exemplaires et de renseignements sur les menaces.

Le Pacific Cyber Security Operational Network

Le Centre pour la cybersécurité est prêt à soutenir des partenaires aux vues similaires ainsi que des spécialistes techniques du monde entier, notamment dans les pays d'Australasie et les îles du Pacifique, par l'entremise du Pacific Cyber Security Operational Network.

Cette année, le Centre pour la cybersécurité a :

- offert de la formation et des séances d'information sur Assemblyline et l'utilisation de l'IA pour améliorer l'analyse du renseignement sur les menaces et la communication auprès de divers auditoires;
- renforcé la posture de sécurité des membres grâce à des échanges rapides et bidirectionnels de renseignement sur les menaces;
- contribué à l'établissement de leurs processus et infrastructures d'échange d'information;
- soutenu leur participation à l'atelier GeekWeek.

Renforcer la résilience nationale par la formation et la sensibilisation

Le CST renforce la résilience nationale en favorisant la littératie numérique, la sensibilisation et l'état de préparation. Grâce à des initiatives d'éducation et de sensibilisation, il dote la population canadienne et les organisations de la confiance et des connaissances nécessaires pour évoluer en toute sécurité dans l'environnement numérique.

Cours et ressources du Carrefour de l'apprentissage

À mesure que l'environnement des cybermenaces évolue, il est essentiel de former l'effectif actuel et de perfectionner ses compétences.

Le Carrefour de l'apprentissage du Centre pour la cybersécurité propose des formations en cybersécurité validées à l'intention des personnes qui travaillent dans la fonction publique fédérale, dans d'autres ordres de gouvernement, dans les organisations du secteur des infrastructures essentielles, dans les petites et moyennes organisations et dans le milieu de l'éducation.

Cette année, **6 585 personnes** ont suivi des formations offertes par le Carrefour de l'apprentissage du Centre pour la cybersécurité. Les cours sont régulièrement mis à jour et portent sur des sujets comme la cryptographie post-quantique, l'IA générative et la gestion des cyberincidents.

Les besoins en professionnelles et professionnels de la cybersécurité continuent de croître à l'échelle du pays. Pour répondre à ces besoins, plusieurs établissements d'enseignement ont créé des programmes de cybersécurité spécialisés. Afin d'assurer la relève au Canada, le Carrefour de l'apprentissage tient à jour une base de données consultable de programmes offerts par des établissements postsecondaires canadiens[31].

Ayant été consultée plus de 30 000 fois, cette ressource aide les stagiaires ainsi que les professionnelles et professionnels à découvrir des cheminements de carrière et contribue à la croissance du bassin de talents en cybersécurité au Canada.

Centre d'entraînement à la cyberdéfense – programme Telfer

Un leadership fort est essentiel pour gérer les risques liés à la cybersécurité.

Cette année, le Centre pour la cybersécurité a conclu un partenariat avec l'École de gestion Telfer de l'Université d'Ottawa pour accroître les possibilités de perfectionnement professionnel par l'entremise du Laboratoire uOttawa-IBM Cyber Range. S'appuyant sur le programme de simulation de leadership en situation de crise de Telfer, cet espace immersif permet aux leaders de s'exercer à intervenir en cas d'incidents de cybersécurité réels.

Dans le cadre de ce partenariat, le Centre pour la cybersécurité a élargi l'offre du Laboratoire en proposant de nouvelles simulations en situation de crise, des catalogues de simulations et des programmes de perfectionnement professionnel fondés sur des menaces réelles. En conjuguant l'expertise en matière de renseignement sur les menaces, de cyberdéfense et de protection des infrastructures essentielles, le programme prépare les cadres de direction et les spécialistes de première ligne à prévenir les incidents de cybersécurité, à y répondre et à s'en remettre.

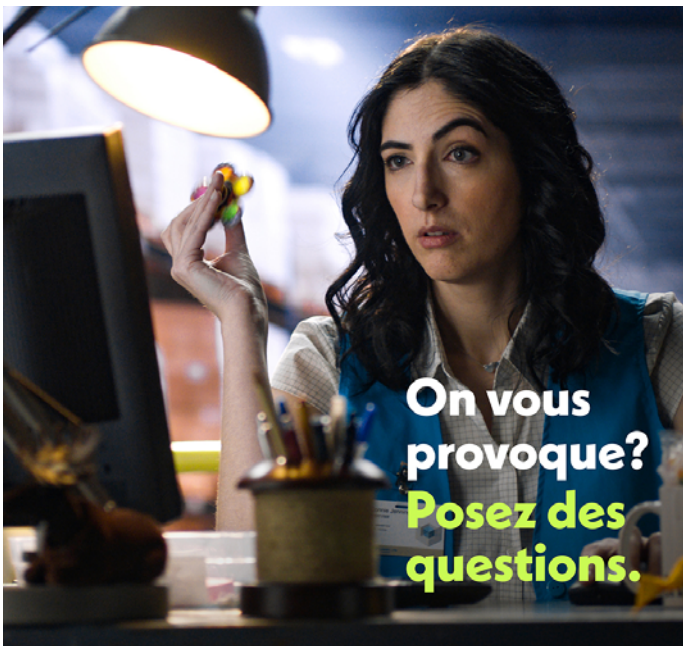
Ensemble, le programme Telfer et le Centre pour la cybersécurité visent à doter les leaders des compétences stratégiques nécessaires pour protéger la population canadienne et les systèmes sur lesquels ils comptent.

Campagne de désinformation en ligne

Un plus grand nombre de préoccupations liées à la désinformation en ligne et à ses effets sur la société ont été soulevées au cours des dernières années. Les auteurs de menace étatiques étrangers utilisent les plateformes numériques, les médias sociaux et les technologies émergentes comme l'intelligence artificielle pour diffuser de l'information fallacieuse ou trompeuse, miner la confiance et accentuer les divisions sociales. La désinformation en ligne peut également constituer une menace grave pour les processus démocratiques, notamment en tentant de miner la confiance dans les élections, de discréditer des personnes et des sources d'information, et de polariser le débat public.

Au début de 2024, le CST a lancé une campagne nationale de sensibilisation[32] pour inciter la population canadienne à analyser de façon plus critique l'information en ligne. La campagne, qui s'est poursuivie pendant les élections fédérales de 2025, présentait le message « Si ça vous fait hausser les sourcils, ça devrait soulever des questions » et encourageait les Canadiennes et Canadiens à prendre le temps de vérifier l'information et à réfléchir avant de partager du contenu.

La campagne a été diffusée sur les plateformes où la désinformation se propage généralement, notamment les médias sociaux et d'autres canaux numériques. Les publicités ont été diffusées plus de 44 millions de fois et ont généré plus de 250 000 consultations de la page Web sur la désinformation en ligne[33].



Sensibilisation communautaire

La collectivité est au cœur du travail que fait le CST pour assurer la sécurité des Canadiennes et Canadiens, et ses programmes sont adaptés à différents publics.

Par l'entremise de son programme d'approche communautaire, le CST favorise l'accès à des carrières en science, technologie, ingénierie et mathématiques (STIM) et en cybersécurité, en particulier pour les groupes qui sont confrontés à des obstacles à la participation ou qui sont sous-représentés dans le domaine. Cela comprend les partenariats avec des organismes sans but lucratif, des établissements d'enseignement et des groupes communautaires.

En 2025-2026, le soutien du CST dans le cadre du concours CyberSci a mené à l'obtention des distinctions suivantes :

- L'équipe canadienne s'est classée au deuxième rang dans la catégorie des pays invités lors du European Cybersecurity Challenge. Il s'agissait de la quatrième année consécutive où le CST a parrainé et encadré l'équipe.
- L'équipe du Canada s'est classée cinquième au classement général lors de l'International Cybersecurity Challenge. Il s'agissait de la première année où le CST a parrainé et encadré l'équipe.

Le CST a également soutenu les organisations et les initiatives suivantes :

- Hackergal
- Colourfully Digital
- Conseil des écoles catholiques du Centre-Est
- Raspberry Pi

En plus des programmes pour les jeunes, le Centre pour la cybersécurité fournit des conseils pratiques, des renseignements sur les menaces et des outils pour aider les organisations et les collectivités à mieux comprendre les risques émergents et à renforcer leur état de préparation en matière de cybersécurité.

Campagne Pensez cybersécurité

Par l'entremise de sa campagne nationale de sensibilisation publique Pensez cybersécurité, le CST offre des conseils en matière de cybersécurité pour aider la population canadienne à se protéger en ligne.

Cette année, le CST a continué d'élargir la portée de la campagne au-delà des deux langues officielles en proposant certaines ressources en ojibwé, en cri, en inuktitut et en micmac, afin que les communautés autochtones puissent accéder plus facilement à l'information concernant la cybersécurité.

Tout au long de l'année, le CST a diffusé du contenu régulièrement, fait la promotion de ses ressources les plus populaires et soutenu la mobilisation à l'échelle nationale par l'entremise de ses canaux numériques.

Parmi les ressources nouvelles et mises à jour publiées cette année, mentionnons les suivantes :

- Comment repérer les signaux d'alarme sur les plateformes de rencontre en ligne[34]
- Les types d'hameçonnage que vous risquez de rencontrer en voyage[35]
- Des habitudes à éviter sur les médias sociaux pour vous protéger et renforcer votre cybersécurité[36]
- Comment parler à vos proches de cybersécurité[37]
- Nouvelles vidéos sur les sauvegardes[38] et les gestionnaires de mots de passe[39]
- Nouveau jeu-questionnaire appelé Êtes-vous vulnérable au piratage?[40]

Pensez cybersécurité continue de démontrer la façon dont le CST joint la population canadienne, en protégeant les infrastructures nationales et la vie numérique quotidienne de millions de personnes.

Mois de sensibilisation à la cybersécurité

Chaque année, des pays partout dans le monde prennent part au Mois de la sensibilisation à la cybersécurité (Mois de la cybersécurité) pour promouvoir la protection des activités en ligne et des données personnelles.

Ici au Canada, la campagne Pensez cybersécurité[41] est dirigée par le CST et s'appuie sur des avis et conseils pratiques du Centre pour la cybersécurité.

Le thème de cette année, « **Pensez cybersécurité – Pensez à votre avenir** », encourageait les Canadiennes et Canadiens à prendre des mesures simples dès aujourd'hui pour se protéger à l'avenir.

Au cours d'une période de cinq semaines en octobre, les Canadiennes et Canadiens se sont mobilisés pour se renseigner davantage sur la cybersécurité, notamment en faisant part de leurs réussites, en utilisant les mots-clics de la campagne dans leurs publications sur les médias sociaux dans les deux langues officielles, et en discutant tout simplement de l'importance du Mois de la cybersécurité avec leurs collègues et leurs proches. La campagne, au ton à la fois informatif, inclusif et pratique, a suscité des discussions à l'échelle du pays grâce à des vidéos sympathiques, une chanson pop country complète[42] et du contenu multiplateforme.

Des partenaires nationaux des secteurs public et privé ont contribué à produire et à transmettre le contenu. Plus de 310 organisations ont utilisé les ressources du Mois de la cybersécurité pour joindre leur public.

Au cours du Mois de la cybersécurité, le contenu de la campagne a :

- été vu plus de 356 000 fois, en hausse par rapport à l'année précédente (293 000 fois);
- été partagé par 253 comptes de médias sociaux uniques;
- généré 210 081 impressions publicitaires et a joint 2,6 millions d'utilisatrices et utilisateurs;
- entraîné 82 709 visites de site Web, en hausse par rapport à l'année précédente (73 081 visites).

Sensibilisation communautaire

Les ambassadrices et ambassadeurs de la campagne Pensez cybersécurité ont engagé un dialogue avec des Canadiennes et Canadiens dans le cadre d'activités de sensibilisation en personne, notamment à la foire d'automne de Markham et au Carrefour Laval. Les visiteuses et visiteurs ont participé à un jeu-questionnaire interactif sur les habitudes en matière de cybersécurité ainsi qu'à un défi d'authentification multifacteur démontrant des méthodes de vérification biométrique.

Les participantes et participants ont reçu des prix et des ressources à emporter afin de renforcer les comportements de cybersécurité tout au long de l'année.

Environ 136 000 personnes ont consulté les éléments de sensibilisation, dont 32 483 impressions publicitaires confirmées. Les visiteuses et visiteurs sont restés en moyenne plus de 8 minutes aux kiosques, alors que la moyenne de l'industrie se situe entre 3 et 5 minutes. Cela illustre l'engagement de la population canadienne à protéger ses activités en ligne, tout en suivant les avis et conseils du CST et du Centre pour la cybersécurité.

Ateliers sur la cybersécurité

Dans le cadre du Mois de la sensibilisation à la cybersécurité, le CST, en collaboration avec HabilosMédias, a soutenu la diffusion et la promotion de trois ateliers virtuels gratuits sur la cybersécurité[43] adaptés aux personnes âgées. Les séances ont porté sur les compétences pratiques en matière de sécurité numérique, notamment la création de mots de passe robustes, la reconnaissance et l'évitement des arnaques en ligne, la sécurisation des appareils personnels et le repérage de mésinformation.

Chronique Deception Decoded sur CTV

Alors que l'intérêt pour la cybersécurité s'accroît dans tous les groupes démographiques, le CST a continué de collaborer avec les médias nationaux pour sensibiliser les Canadiennes et Canadiens aux cybermenaces et leur fournir des conseils pratiques sur les moyens de protéger leur présence en ligne.

Le 25 février 2026, Rajiv Gupta, dirigeant principal du Centre pour la cybersécurité, a participé à la première diffusion en direct du CST dans la chronique de CTV News, Deception Decoded. La chronique, « Canada's critical infrastructure is being targeted in cyber attacks[44] » (en anglais seulement), a mis en lumière la menace croissante visant les infrastructures essentielles et a souligné l'importance d'appliquer des pratiques exemplaires en cybersécurité, comme l'utilisation de mots de passe robustes et de l'authentification multifacteur, afin qu'il soit plus difficile pour les auteurs de menace d'accéder aux précieuses informations stockées en ligne.

Le CST continuera de participer à cette chronique aux côtés de ses partenaires assurant la sécurité nationale afin de sensibiliser davantage la population aux cybermenaces en constante évolution.

INSTAURER LA CONFIANCE PAR LA REDDITION DE COMPTES ET LA TRANSPARENCE

La capacité du CST à réaliser son mandat dépend de la confiance que lui accordent ses partenaires et la population canadienne. Il instaure et maintient cette confiance en étant aussi ouvert et transparent que possible quant à ses activités et à ses mécanismes de reddition de comptes. Bien qu'une part importante de ses activités doive demeurer classifiée afin de protéger la sécurité nationale, il s'engage à communiquer des renseignements pertinents sur ses activités.

Le Rapport annuel constitue l'un des moyens par lesquels le CST donne suite à cet engagement, parallèlement à la gestion des demandes d'accès à l'information, aux comparutions devant les comités parlementaires et à la tenue d'audits. Il s'assure que toutes ses actions sont menées dans le respect de la loi, de manière responsable et en adéquation avec les attentes de la population canadienne. Une surveillance indépendante, une gouvernance solide, un suivi continu et des pratiques rigoureuses de conformité, y compris la mesure de la conformité interne, permettent d'assurer la reddition de comptes et de renforcer la confiance du public.

Faire évoluer le cadre stratégique opérationnel

Le CST dispose d'un ensemble robuste de politiques qui répond aux besoins opérationnels et appuie les équipes dans la réalisation de leurs activités en conformité avec les exigences juridiques et politiques du gouvernement du Canada. Le cadre stratégique opérationnel du CST oriente toutes les activités opérationnelles. Il établit des règles et des responsabilités claires pour veiller à ce que le CST mène ses activités conformément à la loi et selon les exigences du gouvernement du Canada dans la réalisation de son mandat.

En 2025-2026, le CST a mis à jour des parties importantes du cadre afin de tenir compte du monde complexe actuel et des technologies qui évoluent rapidement. Ces mises à jour aident l'organisme à respecter les priorités du Canada en matière de renseignement et à protéger les systèmes critiques contre les cybermenaces.

Les politiques et le cadre sont examinés et mis à jour régulièrement pour suivre l'évolution des changements. Cela comprend notamment :

- des modifications aux autorisations ministérielles;
- de nouvelles technologies et activités opérationnelles;
- des commentaires provenant d'organes d'examen et de surveillance indépendants;
- la gestion des lacunes, des incohérences ou des éléments nécessitant des clarifications.

Arrêtés ministériels

Les arrêtés ministériels sont accordés par la ou le ministre de la Défense nationale. Ils établissent à qui le CST peut offrir du soutien et quels systèmes sont désignés comme étant d'importance pour le gouvernement fédéral.

En date du 31 mars 2026, six arrêtés ministériels sont en vigueur au CST. Ces arrêtés désignent :

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

Autorisations ministérielles

En vertu de la *Loi sur le CST*, certaines activités requièrent une autorisation ministérielle de la ou du ministre de la Défense nationale. Il y a différentes autorisations selon les volets du mandat du CST. Les autorisations sont valides pendant un an, et les éléments qui suivent doivent être approuvés par la ou le commissaire au renseignement[45] avant qu'une activité soit menée.

Cette année, le CST a présenté **neuf** demandes d'autorisations auprès du commissaire au renseignement, lesquelles ont toutes été approuvées. Les activités comprenaient les suivantes :

- **1** autorisation de cybersécurité pour protéger les institutions fédérales
- **5** autorisations de cybersécurité pour protéger des institutions non fédérales
- **3** autorisations de renseignement étranger

Par ailleurs, le nombre d'autorisations de cyberopérations[46] étrangères est resté inchangé par rapport à l'année précédente. Ces autorisations sont également valides pendant un an et sont accordées pour des objectifs précis, lesquels peuvent soutenir plusieurs opérations.

- **3** cyberopérations actives
- **1** cyberopérations défensives

Divulgation d'informations nominatives sur des Canadiennes et Canadiens

Le CST ne mène pas d'activités qui visent des Canadiennes et Canadiens, au pays ou à l'étranger, ni des personnes se trouvant au Canada. Toutefois, lors de la conduite d'activités de renseignement étranger, il est possible qu'il obtienne incidemment de l'information qui se rapporte à une Canadienne ou à un Canadien. Dans pareille situation, l'information nominative sur une Canadienne ou un Canadien est supprimée ou masquée avant que le renseignement soit communiqué.

Dans des cas bien précis, des ministères et organismes désignés par la ou le ministre de la Défense nationale peuvent demander l'accès à cette information. Chaque demande est examinée soigneusement conformément aux dispositions de la *Loi sur le CST* avant toute communication d'information.

Divulgations d'informations nominatives sur des Canadiennes et Canadiens en 2025	
Reçues (Canada)	1 032
Reçues (à l'étranger)	75
Signalées	930
Refusées/annulées	177

Conformité interne

L'équipe responsable de la conformité au CST surveille les activités de l'organisme afin de s'assurer qu'elles sont menées conformément aux politiques internes et aux exigences juridiques. Les évaluations et conclusions sont accessibles aux organes d'examen externe.

En 2025-2026, l'équipe responsable de la conformité au CST a dénombré les incidents suivants :

- **14** incidents de conformité opérationnelle ne concernant pas l'information qui se rapporte à une Canadienne ou à un Canadien
- **186** incidents de conformité opérationnelle concernant l'information qui se rapporte à une Canadienne ou à un Canadien

Tous les incidents font l'objet d'un examen et d'une évaluation. L'équipe responsable de la conformité détermine les mesures correctives à prendre et les tendances observées afin de renforcer les pratiques et d'orienter les activités de formation et de sensibilisation.

Cette année, le CST a également mis en place une équipe d'apprentissage lié à la conformité afin de favoriser l'application uniforme des pratiques à l'échelle de l'organisme.

Examens externes

Étant donné son rôle au sein de la collectivité de la sécurité nationale et du renseignement du Canada, le CST fait l'objet d'examens externes de la part de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR).

Ces organes d'examen externe veillent, au nom des Canadiennes et Canadiens, à ce que les activités du CST respectent la loi. Leur travail est essentiel pour assurer la transparence, la reddition de comptes et la confiance du public. Le CST est ouvert aux examens indépendants et aux perspectives externes qui contribuent à améliorer ses processus.

Cette année, le CST a contribué à **26 examens externes**, dont un grand nombre étaient plus vastes et plus complexes par rapport aux années précédentes. À titre d'exemple, le CST a participé au projet pilote d'examen d'assurance technique de l'OSSNR, dans le cadre duquel de nouvelles méthodes ont été appliquées pour examiner les informations et les systèmes techniques du CST sur une courte période bien définie.

Le CST a continué de fournir des réponses de qualité, en temps opportun, à toutes les demandes provenant d'organes d'examen; il a encore une fois respecté tous les délais convenus. Il a également continué de publier ses réponses de la direction aux examens externes[47] et de rendre compte des progrès réalisés dans la mise en œuvre des recommandations convenues. Cette année, il a publié les réponses aux recommandations de deux rapports d'examen de l'OSSNR.

Statistiques liées aux examens externes pour 2025-2026	
Collaborations aux examens et aux rapports	26
Séances d'information offertes aux organes d'examen	24
Réponses aux questions	454

Plaintes externes

Cette année, le CST a reçu sept plaintes externes à l'intention de la chef. Aucune plainte concernant les activités du CST n'a été envoyée à l'OSSNR. Le CST s'engage toujours à s'améliorer et assure un processus structuré pour faire le suivi des plaintes et rendre compte de la mise en œuvre des recommandations connexes.

Audit et évaluation

Les équipes chargées des audits et des évaluations fournissent des services et des conseils impartiaux fondés sur des données probantes à la haute direction. Leur travail appuie la prise de décisions éclairées et aide le CST à atteindre ses objectifs stratégiques. Les deux équipes reçoivent un soutien en matière d'assurance de la qualité de la part du Bureau des pratiques professionnelles et de reddition de comptes du CST.

Cette année, les équipes ont réalisé :

- **3** audits d'assurance;
- **1** audit consultatif;
- **3** évaluations du rendement;
- **1** analyse comparative.

Elles ont également :

- aidé des groupes de travail en matière d'audit interne;
- offert un soutien à l'audit à titre d'invitées à un partenaire fédéral externe;
- contribué à l'élaboration d'un cadre de mesure du rendement pour un programme interne.

Cette année, le Bureau du vérificateur général du Canada a mené un audit afin d'évaluer la cybersécurité des réseaux fédéraux, ainsi que le rôle du CST. L'audit a conclu que le gouvernement dispose des outils nécessaires pour protéger et défendre ses systèmes et que son plan global de cybersécurité est solide.

Programme d'audit de la cybersécurité

Depuis 2018, le CST propose une gamme d'outils gratuits[48] pour aider les responsables des audits à évaluer les pratiques de cybersécurité de leurs organisations. À ce jour, le CST a reçu plus de 250 demandes d'accès à ces outils de la part du gouvernement du Canada et du secteur privé.

Accès à l'information et protection des renseignements personnels (AIPRP)

Le CST s'engage à assurer la transparence et la communication d'information, tout en protégeant ses renseignements les plus sensibles.

Cette année, l'équipe de l'Accès à l'information a traité :

- **85** demandes d'AIPRP;
- **130** consultations sur l'AIPRP;
- **78** demandes d'information en vertu de la *Loi sur la protection des renseignements personnels*.

Afin de respecter ses obligations législatives en vertu de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*, le CST continue de collaborer avec ses partenaires de la collectivité de la sécurité nationale et du renseignement pour améliorer les processus de consultation et répondre plus rapidement aux demandes de documents historiques. Ces efforts se poursuivent, et le CST s'emploie à accroître la transparence tout en protégeant l'information sensible qui lui est confiée afin d'assurer la sécurité nationale, la défense, les relations internationales et les intérêts du Canada.

Accroître la transparence par la mobilisation du public

Instaurer la confiance exige aussi une collaboration constante et visible avec la population canadienne. Dans un environnement de sécurité complexe, une communication proactive permet de démystifier les activités du CST, de renforcer la confiance à l'égard de son mandat et de transformer des renseignements techniques en conseils pratiques que l'on peut appliquer. Elle contribue aussi à mettre en lumière le rôle du CST – un organisme dont les activités sont souvent peu visibles, mais essentielles à la sécurité du Canada.

Au cours de la dernière année, le CST a renforcé sa présence auprès du public en faisant davantage appel aux médias, en participant à des forums nationaux et internationaux et en rehaussant la visibilité de sa direction.

Le CST a répondu à **169 demandes des médias**, a mené **20 entrevues** et a participé à **6 conférences de presse nationales**, fournissant des renseignements concrets et opportuns sur les nouvelles menaces et les questions de cybersécurité.

Parallèlement, le CST a intensifié ses échanges directs avec les partenaires, les parties prenantes et le public dans le cadre de discours et participant à des discussions en groupe, des événements clés et des débats publics.

Ces échanges ont permis au CST de soutenir les priorités du Canada en matière de cybersécurité, de renseignement et de technologies émergentes, tout en contribuant à guider les orientations futures, à consolider les partenariats et à soutenir l'action collective. Ces forums ont également favorisé un dialogue bidirectionnel, permettant au CST de faire part de ses points de vue, de promouvoir des mesures de cyberdéfense pratiques et de mieux comprendre l'évolution des risques dans différents secteurs.

Cela contribue à humaniser le travail du CST, à renforcer la reddition de comptes et à mettre en valeur son apport aux priorités générales du gouvernement et à la coopération internationale.

Ces efforts de sensibilisation contribuent également à inspirer la prochaine génération. En mobilisant les étudiantes et étudiants, les chercheuses et chercheurs et les professionnelles et professionnels en début de carrière, le CST suscite l'intérêt pour des carrières d'analyste du renseignement étranger et de responsable de la cyberdéfense, renforce le bassin de talents du Canada et contribue à une main-d'œuvre de l'avenir plus résiliente.

Ensemble, ces efforts rehaussent la transparence, accroissent la sensibilisation aux cybermenaces et renforcent la confiance à l'égard du CST à titre de porte-parole fiable et faisant autorité. Ils complètent les mécanismes officiels de reddition de comptes et contribuent à un Canada plus informé, plus résilient et plus sécuritaire.

Valeurs et éthique

Le CST continue de renforcer sa culture d'éthique et de reddition de comptes.

Cette année, le CST a mis en place un processus annuel de déclaration des conflits d'intérêts pour l'ensemble du personnel afin de promouvoir la transparence et de maintenir des normes éthiques élevées.

L'équipe de l'Éthique a offert plus d'une douzaine de séances de formation sur l'éthique en personne, fondées sur des scénarios, dont une séance interactive avec les cadres du CST. Elle a également élaboré des conseils pratiques de type « hypothétique » sur des sujets comme les conflits d'intérêts, l'utilisation personnelle des médias sociaux, l'impartialité et le recours à l'IA.

Dans le cadre de la Semaine de l'éthique en janvier 2026, le CST a accueilli un conférencier d'un organisme partenaire de la collectivité des cinq. La séance a souligné l'importance de l'éthique en milieu de travail et les bénéfices qu'apportent des pratiques éthiques rigoureuses aux personnes et aux organisations. Elle a également permis de se pencher sur les

MENER À BIEN LA MISSION EN TANT QU'UN CST INTÉGRÉ

Le personnel du CST est au cœur de tout ce qu'il fait. Sa plus grande force, c'est son effectif diversifié et inclusif. Unis par un objectif commun et un engagement envers la mission, les employées et employés du CST mettent à contribution leur souplesse, leurs compétences spécialisées et leur expertise pour relever les défis les plus complexes du pays. L'innovation et la perspective axée sur la résolution de problème contribuent à ces efforts.

Alors que le Canada renforce sa posture de défense, notamment dans le cadre de son engagement envers l'OTAN, il est essentiel de bâtir et de maintenir une main-d'œuvre saine, qualifiée et résiliente. L'équité, la diversité, l'inclusion et l'accessibilité (EDIA) guident la manière dont le CST recrute, forme et fait avancer les talents, communique ses réalisations et collabore avec ses partenaires. En investissant dans son personnel, le CST s'assure de disposer des capacités nécessaires pour réaliser son mandat, maintenant et à long terme.

Reconnaissance comme l'un des meilleurs employeurs

Le CST continue d'être reconnu comme un employeur de choix.

Encore une fois cette année, le CST a été nommé l'un des **meilleurs employeurs de la région de la capitale nationale** et, pour la première fois, l'un des **meilleurs employeurs pour la diversité au Canada**.

Développer et soutenir l'effectif

Afin de répondre aux besoins croissants dans un contexte de menace de plus en plus complexe, le CST continue d'accroître son effectif.

Cette année, l'effectif du CST a atteint **4 178 employées et employés**, une **augmentation de 8,1 %** comparativement à l'année dernière. Cette croissance témoigne d'efforts soutenus pour attirer et maintenir en poste les meilleurs talents. Elle reflète également une demande accrue découlant des investissements en matière de défense et de sécurité, permettant au CST d'accroître sa capacité opérationnelle et de réaliser son mandat, qui continue d'évoluer.

Par ailleurs, l'effectif du CST reflète de plus en plus la diversité du pays qu'il sert. En date de mars 2026, les employées et employés sont représentés dans les quatre groupes visés par l'équité en matière d'emploi, ainsi que dans les communautés 2ELGBTQIA+ et les identités intersectionnelles.

La représentation des Autochtones et des personnes en situation de handicap est particulièrement élevée, leur présence étant supérieure à leur disponibilité au sein de la population active canadienne.

Représentation au sein de l'effectif du CST (auto-identification) en 2025-2026	
↳ Femmes	33,9 %
↳ Personnes en situation de handicap	14,1 %
↳ Personnes racisées	17,9 %
↳ Autochtones	2,6 %
↳ Personnes 2ELGBTQIA+	6,4 %

À mesure que le CST prend de l'expansion, il améliore également l'expérience du personnel. Il continue de faire du mieux-être une priorité, en créant des conditions propices à l'épanouissement du personnel. Ces efforts contribuent à bâtir l'avenir du CST et à donner aux employées et employés les moyens de produire des résultats innovants pour le Canada, tout en favorisant une culture de travail inclusive et dynamique reconnue année après année.

Prospection de candidates et candidats

Le CST continue d'accroître sa visibilité pour attirer différents talents.

Il recourt à des plateformes de recrutement ciblé, comme Obsidi et Indigenous Link, et mène des activités de rayonnement ciblant les groupes en quête d'équité. L'objectif est de faire en sorte que **trois recrues sur quatre** proviennent de ces groupes.

Cette année, le CST a :

- participé à **139 activités de recrutement** menées dans 8 provinces;
- offert **26 séances d'information** virtuelles;
- embauché des étudiantes et étudiants diplômés de partout au Canada, principalement en génie informatique, en informatique, en mathématiques et en affaires.

À l'automne 2025, le CST a poursuivi ses efforts de recrutement en déployant une campagne publicitaire qui encourageait les personnes intéressées à présenter leur candidature pour différents postes au sein de l'organisme. La campagne a été diffusée sur de multiples canaux numériques pour joindre des personnes travaillant dans les domaines des STIM, en ciblant les femmes et les minorités visibles. Elle a généré :

- plus de **11 millions d'impressions publicitaires**;
- plus de **205 000 clics**;
- plus de **195 000 consultations** de la page sur les possibilités d'emploi.

Campagne de recrutement d'analystes du renseignement en langues étrangères

Le CST a également mené des campagnes ciblées visant à recruter des talents clés et à attirer les profils parmi les plus prometteurs au Canada.

À l'hiver 2026, une campagne publicitaire ciblée visant à recruter des analystes du renseignement en langue chinoise a été lancée sur des canaux traditionnels et des canaux adaptés à la culture. La campagne a généré plus de **43 000 consultations** du site Web du CST, et l'organisme continue de rechercher des personnes possédant des compétences linguistiques pour appuyer l'ensemble de sa mission.

Mises à jour du programme de sécurité

La protection de l'information sensible constitue un élément central de la mission du CST.

Compte tenu de la nature hautement sensible du renseignement très secret lié aux opérations du pays, l'organisme adopte des mesures strictes pour en assurer la protection. Tout au long de l'année, le CST examine ses processus et ses politiques de sécurité et apporte des mises à jour au besoin, tout en veillant à leur concordance avec ses valeurs et ses priorités.

Cette année, le CST a bonifié son programme d'assurance de la sécurité pour accroître l'efficacité des processus de filtrage de sécurité et d'octroi des habilitations. La mise en place de nouveaux outils et de nouvelles mesures permet de mieux gérer les risques pour les employées et employés en poste et pour ceux qui quittent l'organisme. Ainsi, il est possible de maintenir un effectif robuste et capable de s'adapter à l'évolution constante du contexte de menace.

De plus, le CST a :

- lancé un programme de formation et de sensibilisation de base relative à la sécurité à l'intention des nouvelles employées et nouveaux employés;
- publié de nouveaux conseils sur son site Web externe afin d'aider les candidates et candidats à comprendre les exigences de sécurité lorsqu'ils présentent une demande d'emploi au CST.

Lancement de l'Espace mieux-être

Cette année, le CST a mis en place un Espace mieux-être centralisé, qui offre aux membres du personnel un meilleur accès aux ressources et un soutien adapté à leurs besoins. La création d'un poste de navigatrice ou navigateur de mieux-être et d'un forum de consultation renforce davantage l'approche du CST en matière de mieux-être du personnel.

Amélioration des services de soutien en santé mentale offerts aux employées et employés noirs

Le CST s'engage à offrir un plus grand nombre de ressources en santé mentale. Dans le cadre de ses efforts, il continue d'adapter ses services en la matière afin de mieux répondre aux besoins des employées et employés. Cela comprend l'offre d'options davantage adaptées aux réalités culturelles, notamment la possibilité pour les employées et employés noirs de consulter des professionnelles et professionnels de la santé mentale qui représentent leurs communautés.

Bassin de talents en début de carrière

Les étudiantes et étudiants et les professionnelles et professionnels en début de carrière jouent un rôle important au CST.

Chaque année, le CST embauche plus de **235 étudiantes et étudiants**, dont près des **deux tiers** intègrent par la suite des postes permanents. Cette année, 91 étudiantes et étudiants ont intégré des postes à temps plein, et les personnes de moins de 30 ans représentaient 16 % de l'effectif.

Cela témoigne de l'engagement du CST à repérer et favoriser le développement des talents en début de carrière, afin de soutenir une croissance durable et de maintenir un effectif robuste et prêt pour l'avenir.

Mission de bouger

Sous la direction de Caroline Xavier, chef du CST, l'initiative Mission de bouger incite les employées et employés à demeurer actifs durant les jours bien chargés et à privilégier leur bien-être.

Au cours de plusieurs semaines, les employées et employés ont relevé le défi en participant à des activités favorisant à la fois la santé physique et mentale, témoignant d'une solide culture organisationnelle axée sur les rapports, la résilience et l'équilibre.

Promouvoir l'inclusion, l'appartenance et l'accessibilité

Un milieu de travail inclusif est essentiel pour permettre au CST de réaliser son mandat et de répondre à ses futurs besoins opérationnels.

Le CST s'engage à créer un milieu de travail où chaque employée et employé peut apporter sa pleine contribution et s'épanouir. S'appuyant sur son cadre Un CST intégré[49], il continue d'intégrer les principes d'EDIA dans l'ensemble de ses activités, non pas comme un objectif à atteindre, mais comme une composante essentielle de son mode de fonctionnement.

Lancement du Plan sur l'accessibilité du CST de 2026 à 2028

Cette année, le CST a publié une version mise à jour du Plan sur l'accessibilité de 2026 à 2028[50], l'objectif étant de réduire davantage les obstacles en milieu de travail. L'innovation et l'adoption faisant partie intégrante de son mandat, le CST examine régulièrement les dispositions en matière d'accessibilité pour le personnel. Cette année, le CST a rencontré la dirigeante principale de l'accessibilité du gouvernement du Canada pour discuter de l'accessibilité et de l'autonomisation dans le contexte de ses activités. Ces échanges importants permettent au CST de poursuivre l'étude et la mise en œuvre de solutions technologiques pour appuyer l'accessibilité, tout en démontrant que les environnements à sécurité élevée peuvent être inclusifs et adaptables.

Le saviez-vous?

Au CST, **14,1 %** des employées et employés s'identifient comme des **personnes en situation de handicap**.

Un environnement sans obstacles au sein d'un organisme à sécurité élevée

Le CST s'engage à rendre son milieu de travail accessible à tout le personnel, y compris les personnes en situation de handicap et les employées et employés neurodivergents. Pour y parvenir, il adopte des approches novatrices en matière d'accessibilité, même dans des environnements à sécurité élevée.

Un outil de sous-titrage alimenté par l'IA pour favoriser l'accessibilité et les mesures d'adaptation en milieu de travail

En vue d'améliorer l'accessibilité, le CST étudie la possibilité de mettre à l'essai un outil de sous-titrage mobile hors ligne alimenté par l'IA. Cette solution profitera aux employées et employés malentendants ou neurodivergents en améliorant la compréhension, en réduisant la charge cognitive et en maintenant l'attention. En adoptant une approche proactive, le CST démontre que les environnements à sécurité élevée et les milieux de travail inclusifs ne s'excluent pas mutuellement.

Dispositifs médicaux mobiles sécurisés

Cette année, le CST a élargi son offre de mesures d'adaptation en milieu de travail aux employées et employés ayant des besoins médicaux, notamment dans le cadre d'un projet pilote intégrant des technologies médicales en milieu de travail pour aider les personnes qui utilisent des outils numériques de surveillance de la santé. Ces outils permettent aux employées et employés de gérer leur santé en toute sécurité et de façon discrète pendant les heures de travail.

Par ailleurs, le CST a continué d'examiner régulièrement les dispositifs médicaux portés, en évaluant les technologies actuelles de même que les nouvelles technologies. Cela permet d'assurer que l'approche en matière d'accessibilité évolue au même rythme que les technologies médicales, tout en réduisant les obstacles de manière proactive avant qu'ils n'aient une incidence sur le personnel.

Ces efforts démontrent que l'accessibilité ne constitue pas une contrainte, mais qu'elle accroît le rendement, l'inclusion et l'innovation. Ils témoignent également de l'engagement du CST à créer un milieu de travail accessible où les employées et employés peuvent apporter leur pleine contribution et s'épanouir. Cela lui permet d'attirer et de maintenir en poste les talents dont il a besoin pour réaliser son mandat.

Cérémonie de citoyenneté

En janvier 2026, le CST, en collaboration avec Immigration, Réfugiés et Citoyenneté Canada, a eu le privilège d'accueillir avec fierté sa troisième cérémonie de citoyenneté à l'édifice de Vanier, au cours de laquelle on a accueilli 60 nouvelles Canadiennes et nouveaux Canadiens provenant de 26 pays. Cet événement témoigne de son engagement continu envers l'inclusion et la communauté.

Un CST intégré : la collection – deuxième édition

À la suite du succès de la première édition du jeu « Un CST intégré : la collection », le CST a lancé la deuxième édition en janvier 2026. Cette édition subséquente s'appuie sur le cadre Un CST intégré[51] et se veut une extension des principes directeurs du CST, à savoir l'épanouissement culturel, l'apprentissage continu, la consultation et la transparence, l'élimination des obstacles et de la discrimination, et l'engagement profond envers l'inclusion.

La deuxième édition mise sur le succès de la première édition, à laquelle on a décerné le Prix phare d'excellence en communication pour son modèle de mobilisation du personnel parmi les initiatives gouvernementales semblables.

Analyse comparative entre les sexes Plus

L'analyse comparative entre les sexes Plus (ACS Plus) continue de renforcer la prise de décisions du CST en tenant compte des diverses perspectives et des expériences vécues.

L'ACS Plus soutient directement **Un CST intégré** en repérant et en éliminant les préjugés et les obstacles systémiques, contribuant ainsi à faire évoluer la culture organisationnelle et à produire des résultats plus équitables pour tout le personnel.

Le CST continue d'intégrer l'ACS Plus des façons suivantes :

- incorporer l'ACS Plus dans ses processus, ainsi que dans les mémoires au Cabinet, les présentations au Conseil du Trésor et les propositions budgétaires, afin de favoriser une prise de décisions fondée sur les données, de mettre en œuvre des initiatives inclusives et adaptées, et de soutenir la réalisation de son mandat;
- adopter une approche axée sur la personne dans l'élaboration des politiques, des processus, des services et des initiatives, afin de s'assurer qu'ils sont inclusifs, accessibles et adaptés à la diversité de la communauté du CST;
- intégrer l'ACS Plus dans ses documents de base, notamment la Charte d'éthique, le Code de conduite et la Politique sur l'obligation de prendre des mesures d'adaptation;
- outiller et habiliter les employées et employés à appliquer une perspective intersectionnelle dans leur travail, notamment en prenant les mesures suivantes :
  - » approfondir les connaissances de base au moyen de formations obligatoires sur l'ACS Plus, les préjugés culturels et les préjugés inconscients;
  - » affecter des ressources en matière de conseils, d'orientation et de rétroaction pour soutenir l'élaboration d'initiatives adaptées;
  - » offrir des ressources et des outils d'apprentissage en milieu de travail pour permettre aux employées et employés ainsi qu'aux équipes de renforcer leurs capacités d'analyse et leur confiance.

Le CST collabore également au sein du gouvernement du Canada des façons suivantes :

- participer régulièrement à des activités interministérielles;
- coprésider, avec Sécurité publique Canada, le Groupe de travail Cyberidentité/inclusion, diversité, équité et accessibilité, afin de partager les leçons apprises, les pratiques exemplaires et les ressources, et de cerner des possibilités de collaboration.

En tant qu'ancien lauréat du Prix phare d'excellence en communication, le CST est reconnu comme un chef de file au sein du gouvernement du Canada en matière d'ACS Plus et d'EDIA, notamment pour son approche réfléchie favorisant les échanges entre les membres du personnel et une connaissance durable des principes d'EDIA.

Femmes en défense et sécurité – Déjeuner annuel de remise de prix de 2026

En mars 2026, huit employées du CST ont reçu le Prix Leader remarquable lors du Déjeuner annuel de remise de prix de Femmes en défense et sécurité[52] (en anglais seulement). Elles ont été reconnues aux côtés de lauréates provenant de la communauté élargie de la sécurité et de la défense.

Caroline Xavier, chef du CST, a prononcé un discours principal émouvant sur le thème d'une communauté engagée et de l'influence du changement au service du bien commun.

Groupes d'affinité

Les groupes d'affinité sont des réseaux dirigés par les employées et employés au sein desquels les membres cultivent un sentiment d'appartenance communautaire, font part de leurs perspectives et abordent les obstacles qu'ils peuvent rencontrer en milieu de travail. Ils jouent un rôle important dans le renforcement de l'organisation en offrant des perspectives qui contribuent à orienter les politiques, les programmes et les initiatives visant à faire avancer les priorités en milieu de travail et à améliorer l'expérience globale du personnel.

De plus, les groupes d'affinité sont invités aux tables de décision et font état chaque année de leurs défis, de leurs besoins et de leurs progrès auprès des cadres du CST.

Il y a 14 groupes d'affinité au CST :

- Réseau de la Fierté
- Cybersécurité et renseignement au féminin
- Réseau de soutien pour les femmes au sein de l'Accès
- EmbRACE, qui regroupe :
  - le Cercle des employées et employés noirs
  - le sous-groupe Moyen-Orient et Afrique du Nord
  - Patrimoine asiatique
  - Groupe d'affinité sud-asiatique
- Groupe de la neurodiversité
- Groupe d'affinité des personnes handicapées
- Groupe d'affinité juif
- Groupe d'affinité musulman
- Réseau franco
- Cercle des transmetteurs en code (pour les employées et employés qui s'identifient comme membres des communautés autochtones)
- Minorités audibles

Affinity • Affinité

AMG • GMA

AWSN • RSFA

CTC • CPC

Disability Handicap

EmbRACE

Franco

JAG • GAJ

MAG • GAM

Neurodiversity Neurodiversité

Pride • Fierté

WICI • CRAF

Sommet autochtone de la collectivité des cinq

Du 24 au 26 juin 2025, le CST a accueilli le Sommet autochtone de la collectivité des cinq, en étroite collaboration avec le SCRS, qui en assurait la présidence, ainsi qu'avec le Cercle des transmetteurs en code. Le CST et le SCRS ont coordonné le sommet à l'édifice de Vanier afin de réunir les partenaires et de discuter des partenariats avec les communautés autochtones, notamment en matière de sécurité. Le sommet a également comporté un enseignement traditionnel autochtone, offrant une perspective culturelle significative qui a permis d'ancrer les échanges dans les savoirs autochtones.

Réseau des jeunes professionnelles et professionnels du CST

Le Réseau des jeunes professionnelles et professionnels (RJP), mis sur pied en 2012, est un réseau dynamique pour les nouvelles, les nouveaux et les jeunes employés. Les membres participent invariablement à la création d'un milieu de travail cohésif et favorisent des changements positifs afin de mettre en place un effectif durable au CST. Les personnes visées comprennent généralement les étudiantes et étudiants en enseignement coopératif ainsi que les employées et employés comptant moins de 10 ans de service dans la fonction publique, sans limite d'âge prescrite. Qu'une personne soit en début de carrière, une recrue au CST ou simplement jeune d'esprit, toutes et tous sont invités à se joindre au réseau.

Cette année, le RJP a organisé 14 activités à l'échelle de l'organisme, dont des formations, des séances de réseautage professionnel, des rencontres sociales et des événements interministériels. Des cadres de direction et des employées et employés en début de carrière ont pris part à ces activités, pour favoriser des échanges avec la communauté élargie du gouvernement fédéral portant sur des thèmes comme le perfectionnement professionnel, la représentation intersectorielle, la durabilité et le bien-être général.

Reconnaître la culture organisationnelle du CST pour les jeunes professionnelles et professionnels

En octobre 2025, le Comité directeur du RJP a remporté le prix Cabot Trail décerné lors de l'événement d'appréciation des champions annuel du Réseau des jeunes professionnels de la région de la capitale nationale. On a souligné le travail actif et l'engagement du Comité directeur du RJP du CST, de même que ses efforts constants pour repousser les limites au sein du gouvernement du Canada.

Soutenir l'effectif dans l'adoption de la transformation numérique

Conformément à son engagement envers l'innovation continue, le CST donne à son effectif les moyens d'adopter les technologies nouvelles et émergentes, afin de demeurer au premier plan d'une transformation numérique responsable. Dans le cadre de son évolution vers un organisme qui utilise l'IA, il mobilise son effectif pour exploiter les nouvelles technologies dans la conduite de ses activités, en conformité avec la Stratégie en matière d'IA du CST[53].

Adopter l'intelligence artificielle de façon responsable

Cette année, le CST a réalisé des progrès importants dans l'intégration de l'intelligence artificielle à ses activités, en élargissant l'adoption de technologies alimentées par l'IA à l'échelle de l'organisme. Guidé par les principes énoncés dans sa Stratégie en matière d'IA et soutenu par des cadres solides de gouvernance et de gestion des risques, le CST veille à ce que le personnel ait accès à des outils de pointe dans un environnement sécurisé et encadré.

Dans le cadre de cet effort, le CST a continué d'évaluer les outils d'IA offerts sur le marché (y compris ceux ayant des capacités d'IA générative), et de les intégrer dans les flux de travail quotidiens. Les considérations liées à la sécurité ont été prises en compte à chaque étape afin de préserver l'intégrité de l'environnement informationnel, des contrôles étant intégrés dès le départ. Des activités continues de formation et de mobilisation des utilisatrices et utilisateurs ont permis d'assurer une adoption sécuritaire et efficace, le personnel étant guidé par un principe fondamental consistant à toujours valider les processus et les résultats générés par IA.

Les premiers résultats sont encourageants – les utilisatrices et utilisateurs ont fait état d'améliorations mesurables en matière de productivité et d'efficacité des flux de travail. Ces constats éclairent les décisions futures concernant l'adoption de l'IA à l'échelle de l'organisme, afin de permettre au CST de continuer à outiller le personnel tout en protégeant l'information sensible et en maintenant la confiance du public.

Élaborer un cadre de gouvernance pour l'IA responsable

Cette année, le CST a officiellement lancé une boîte à outils d'IA responsable afin d'aider le personnel à prendre des décisions sûres et sécuritaires en matière d'adoption de l'IA au travail. Inspirée des pratiques exemplaires partagées par des partenaires internationaux, la boîte à outils comprend un processus de gestion des risques liés à l'IA ainsi qu'un registre des cas d'utilisation de l'IA. Grâce à la documentation, à l'évaluation et à l'atténuation systématiques des risques à l'échelle de l'organisme, le CST fait preuve de diligence raisonnable tout en intégrant l'IA de manière constructive.

Le CST a également mis en place un programme de formation de base sur l'IA à l'intention du personnel, ce qui contribue à uniformiser les compétences en matière d'IA au sein de l'organisme. En s'appuyant sur des technologies sécurisées, le personnel du CST est bien placé pour faire avancer le travail de l'organisme à ce chapitre.

Notes en fin de texte

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

2 https://www.cyber.gc.ca/fr/orientation/vue-densemble-menaces-rancongiciel-2025-2027

3 https://www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-conjoint-cybermenaces-malveillantes-contre-reseaux-sd-wan

4 https://www.cyber.gc.ca/fr/alertes-avis/al25-016-abus-systemes-controle-industriels-sci-accessibles-internet-hacktivistes

5 https://www.canada.ca/fr/securite-telecommunications/nouvelles/2025/11/declaration-commune-sur-les-cyberactivites-malveillantes-qui-ciblent-les-infrastructures-essentielles-canadiennes.html

6 https://www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-cybersecurite-conjoint-compromissions-reseaux-lechelle-mondiale-auteurs-menace-parraines-republique-populaire-chine

7 https://www.cyber.gc.ca/fr/orientation/cyberbulletin-auteurs-cybermenace-rpc-cliblent-entreprises-telecommunications-campagne-mondiale-cyberespionnage

8 https://www.cyber.gc.ca/fr/orientation/cyberbulletin-centre-cybersecurite-invite-canadiennes-canadiens-sinformer-se-proteger-contre-activites-cybermenace-rpc

9 https://www.cyber.gc.ca/fr/orientation/cybermenace-qui-pese-transport-maritime

10 https://www.cyber.gc.ca/fr/orientation/cybermenaces-visant-systemes-gestion-eaux-canada-evaluation-attenuation

11 https://www.cyber.gc.ca/fr/orientation/vue-densemble-menaces-rancongiciel-2025-2027

12 https://www.cyber.gc.ca/fr/orientation/cyberbulletin-auteurs-cybermenace-rpc-cliblent-entreprises-telecommunications-campagne-mondiale-cyberespionnage

13 https://www.cyber.gc.ca/fr/orientation/bulletin-cybermenaces-cybermenace-liran-visant-canada-emanant-conflit-entre-israel-liran

14 https://www.cyber.gc.ca/fr/orientation/cybermenaces-visant-systemes-gestion-eaux-canada-evaluation-attenuation

15 https://www.cyber.gc.ca/fr/orientation/cybermenace-qui-pese-transport-maritime

16 https://www.cyber.gc.ca/fr/orientation/bulletin-cybermenaces-intervention-cas-cybermenaces-iraniennes-emanant-frappes-etats-unis-disrael-fevrier-2026

17 https://www.cyber.gc.ca/fr/orientation/cyberbulletin-cyberactivites-parrainees-republique-populaire-chine-menees-contre-gouvernements-provinciaux-territoriaux-autochtones-administrations-municipales-canada

18 https://www.cyber.gc.ca/fr/orientation/vue-densemble-menaces-rancongiciel-2025-2027

19 https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-matiere-dintelligence-artificielle-introduction-itsap10049

20 https://www.cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-visant-proteger-les-reseaux-internet-et-0

21 https://www.cyber.gc.ca/fr/orientation/defense-contre-attaques-type-adversaire-milieu-grace-authentification-multifacteur-resistante-lhameconnage-itsm30031

22 https://www.cyber.gc.ca/fr/nouvelles-evenements/detection-menaces-vulnerabilites-touchant-sharepoint

23 https://www.cyber.gc.ca/fr/nouvelles-evenements/etherhiding-cheval-troie-chaine-doutils

24 https://www.cyber.gc.ca/fr/orientation/feuille-route-migration-vers-cryptographie-post-quantique-sein-gouvernement-canada-itsm40001

25 https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/strategie-industrielle/securite-souverainete-prosperite.html

26 https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/strategie-industrielle/securite-souverainete-prosperite.html

27 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/centre-securite-telecommunications-canada-strategie-matiere-dintelligence-artificielle

28 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/centre-recherche-vulnerabilites

29 https://www.canada.ca/fr/securite-telecommunications/nouvelles/2025/07/le-cst-et-le-crsng-financeront-la-recherche-sur-lanalyse-exploratoire-des-donnees-non-structurees.html

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

31 https://www.cyber.gc.ca/fr/education-communaute/collaboration-milieu-education-developpement-cybercompetences/programmes-postsecondaires-lies-cybersecurite

32 https://www.youtube.com/watch?v=3ZOy8UtBlYk

33 https://www.canada.ca/fr/campagne/desinformation-enligne.html

34 https://www.pensezcybersecurite.gc.ca/fr/ressources/comment-reperer-signaux-dalarme-plateformes-rencontre-ligne

35 https://www.pensezcybersecurite.gc.ca/fr/blogues/types-dhameconnage-que-vous-risquez-rencontrer-voyage

36 https://www.pensezcybersecurite.gc.ca/fr/blogues/habitudes-eviter-medias-sociaux-vous-proteger-renforcer-cybersecurite

37 https://www.pensezcybersecurite.gc.ca/fr/blogues/comment-parler-vos-proches-cybersecurite

38 https://www.pensezcybersecurite.gc.ca/fr/ressources/effectuez-sauvegardes

39 https://www.pensezcybersecurite.gc.ca/fr/ressources/gestionnaires-mots-passe

40 https://www.pensezcybersecurite.gc.ca/fr/ressources/etes-vous-vulnerable-piratage

41 https://www.pensezcybersecurite.gc.ca/fr

42 https://www.pensezcybersecurite.gc.ca/fr/ressources/video-lettre-futur-vous-chanson-mois-cybersecurite-2025

43 https://www.pensezcybersecurite.gc.ca/fr/blogues/serie-dateliers-gratuits-ligne-cybersecurite-personnes-ainees-pendant-mois-cybersecurite

44 https://www.ctvnews.ca/video/deception-decoded/2026/02/25/canadas-critical-infrastructure-is-being-targeted-in-cyber-attacks-deception-decoded

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

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

47 https://www.cse-cst.gc.ca/fr/reddition-comptes/transparence/reponses-rapports-examens

48 https://www.cyber.gc.ca/fr/outils-services/programme-audit-cybersecurite

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

50 https://www.cse-cst.gc.ca/fr/accessibilite/plan-laccessibilite-centre-securite-telecommunications-canada-2026-2028

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

52 https://www.wids.ca/events/details&e=97

53 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/centre-securite-telecommunications-canada-strategie-matiere-dintelligence-artificielle


Canada