ISSN 2564-047X
CAT D95-11F-PDF

Centre de la sécurité des télécommunications Canada

Rapport annuel 2024-2025

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

Canada

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

ISSN 2564-047X
CAT D95-11F-PDF

Table des matières

Avant propos du ministre 2

Message de la chef 3

À propos du CST 5

Mandat 7

L'année 2024 à 2025 en chiffres 9

Le CST repère les menaces étrangères, les atténue et y répond 13

L'interrelation des volets du mandat du CST : un exemple 15

La collecte, l'analyse et la diffusion de renseignement électromagnétique étranger 16

Conduite de cyberopérations étrangères 20

Publication des évaluations des menaces 22

Protection des institutions démocratiques et des infrastructures essentielles du Canada 24

Intervention en cas de cyberincidents et prévention des cyberincidents 29

Prestation de soutien et d'expertise lors d'événements mondiaux 30

Innovation et évolution du CST 33

Promotion de l'utilisation responsable de l'intelligence artificielle 34

Amélioration de l'infrastructure et des services classifiés 36

Promotion de l'innovation et des partenariats par l'intermédiaire de sourçage libre 38

Recherche et renforcement des partenariats de recherche 38

Le CST habilite et joint les Canadiennes et Canadiens 41

De nouvelles manières de sensibiliser les Canadiennes et Canadiens 42

Étendre les activités de sensibilisation 44

Le CST croît et apprend 47

Améliorer les activités d'embauche, de recrutement et de sensibilisation 48

L'inclusivité dans toutes les activités 49

Le CST est transparent et rend des comptes 53

Maintenir l'engagement envers la transparence et la reddition des comptes 54

Contribuer à l'Enquête publique sur l'ingérence étrangère 56

Notes en fin de texte 57

Avant propos du ministre

Les événements survenus au cours de la dernière année, tant au Canada qu'à l'étranger, ont consolidé le rôle essentiel du Centre de la sécurité des télécommunications Canada (CST) dans la protection de la sécurité nationale et économique. Dans un contexte de menace qui évolue rapidement, le CST joue un rôle déterminant en aidant le Canada à relever les défis complexes et émergents. L'expertise et le dévouement de l'équipe du CST sont de calibre mondial, et le travail qu'elle accomplit contribue fondamentalement à la sécurité nationale du Canada. Je tiens à remercier sincèrement le personnel du CST de son engagement indéfectible.

Alors que les auteurs de menace étrangers poursuivent leurs campagnes de désinformation visant à miner la confiance dans les institutions démocratiques, le Canada a besoin de renseignements opportuns fiables sur les activités, les capacités et les tactiques de ces auteurs. C'est précisément ce que fait le CST, en fournissant des renseignements clairs sur le contexte de menace mondial et en indiquant où et de quelle façon les adversaires cherchent à déstabiliser la société.

Les incidents de cybersécurité perturbent de plus en plus les organisations et les infrastructures essentielles du Canada. Par l'entremise du Centre pour la cybersécurité, le CST joue un rôle capital dans la défense des institutions fédérales, provinciales, territoriales, autochtones et municipales. Le Centre pour la cybersécurité conscientise les parties prenantes, favorise la sensibilisation et renforce les capacités grâce à des avis et conseils spécialisés et à un soutien technique. Ces efforts s'avèrent nécessaires pour accroître la résilience du Canada face à un éventail croissant de cybermenaces.

L'investissement du gouvernement dans le CST met en évidence le mandat crucial de l'organisme et son influence considérable sur le secteur de la sécurité nationale. Le CST s'emploie depuis longtemps à assurer ce qui revêt la principale priorité, soit de protéger le Canada et la population canadienne. À mesure que les cybermenaces évoluent et que la défense du pays se complexifie, le gouvernement s'engage à doter le CST des outils et des ressources nécessaires pour défendre la souveraineté canadienne et réaliser les priorités du Canada en matière de renseignement.

C'est grâce au travail inlassable des fonctionnaires dévouées et dévoués du CST que tout cela est possible. Les efforts déployés par ces fonctionnaires sont essentiels pour assurer la sécurité des Canadiennes et Canadiens aujourd'hui et à l'avenir.

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

Message de la chef

Ce fut une autre importante année pour le CST. Je suis ravie de vous présenter ce rapport, pour montrer aux Canadiennes et Canadiens diverses façons dont notre remarquable organisation travaille à assurer leur sécurité. Ce qui motive le CST, c'est l'excellence. Notre passion pour la collaboration au sein de l'organisme et avec nos divers partenaires afin de résoudre des problèmes complexes nous permet d'innover davantage.

Le rapport annuel de cette année souligne notre engagement à l'égard de la sécurité du Canada, qu'il s'agisse de nos efforts soutenus visant à produire du renseignement exploitable pour les décideuses et décideurs fédéraux ou de notre détermination à établir des partenariats solides et variés en vue d'élaborer des solutions créatives qui renforcent la cyberrésilience du Canada. Notre rôle et les répercussions de notre travail sur la sécurité, la prospérité et la protection du Canada sont très tangibles, mais pas toujours sous l'œil du public. Notre travail oriente les décisions qui protègent les citoyennes et citoyens canadiens, défendent nos valeurs et renforcent le rôle du Canada en tant que partenaire de confiance sur la scène mondiale.

Cette année, nous avons jeté des bases solides pour l'avenir. Pour ce faire, nous avons poursuivi notre étroite collaboration avec nos partenaires de la collectivité des cinq et avec nos divers partenaires des secteurs public et privé, tant au pays qu'à l'étranger. Ensemble, nous avons publié des bulletins conjoints sur les cybermenaces. Nous avons également travaillé de concert pour nous attaquer aux défis liés à l'intelligence artificielle (IA) et pour protéger la sécurité des institutions démocratiques du Canada. Le CST est plus que jamais prêt pour la suite des choses.

La diversité est la force de la mission du CST. Elle constitue une priorité pour le recrutement et l'élaboration de nos politiques. Notre croissance soutenue indique que nous sommes sur la bonne voie. Notre force découle de notre effectif diversifié, car nous avons instauré une culture permettant aux personnes d'être au sommet de leur forme au travail, où elles se sentent appuyées et vues. L'équité, la diversité, l'inclusion et l'accessibilité orientent tout ce que nous faisons. Ces éléments sont essentiels pour nous aider à réaliser notre mission.

La sécurité nationale et la cybersécurité exigent un effort concerté, et le CST est fier des relations qu'il a établies avec d'autres ministères, ordres de gouvernement, intervenants et alliés partout dans le monde. À un moment où le monde fait face à un contexte de menace de plus en plus complexe – cybermenaces, menaces ciblant la sécurité économique, extrémisme violent, ingérence étrangère, campagnes de désinformation et plus encore –, je trouve rassurant de savoir que notre équipe exceptionnelle du CST travaille jour et nuit pour aider le Canada à s'y attaquer de front.

Le CST ne travaille pas seul dans ce domaine. Il travaille de concert avec des organismes indépendants de surveillance et d'examen externe qui assurent la reddition de comptes pour notre travail au nom des Canadiennes et Canadiens et appuient nos efforts vis-à-vis de la transparence et de la confiance.

Ce fut une grande année pour le CST. Nous avons contré des cybermenaces provenant d'adversaires dotés de moyens de plus en plus sophistiqués. Nous avons également soutenu d'importants événements, publié notre stratégie en matière d'IA et participé à l'Enquête publique sur l'ingérence étrangère, pour ne citer que quelques exemples. Je sais que l'année prochaine sera tout aussi grande. Au cours de ses quelque 80 années d'existence en tant qu'organisme, le CST a été témoin de changements extraordinaires et il est parvenu à s'y adapter. Notre Vision 2030, en cours d'élaboration, est un effort panorganisationnel qui orientera nos priorités, nos activités et nos plans d'avenir. Quels que soient les défis de la prochaine année, nous nous préparons, et nous sommes prêtes et prêts. Nous formons un CST intégré.

Caroline Xavier (elle)
Chef, CST

À PROPOS DU CST

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

Le CST chapeaute le Centre canadien pour la cybersécurité (Centre pour la cybersécurité), l'organe opérationnel et technique du Canada pour la cybersécurité et l'assurance de l'information. En tant que partie intégrante du CST, il fournit des conseils et des services de pointe en vue d'aider à prévenir les cyberincidents et à faire en sorte que les services critiques demeurent fonctionnels et accessibles.

L'effectif du CST est composé de 3 841 employées et employés permanents à temps plein. Les autorisations totales du CST pour l'année 2024 à 2025 étaient plus de 1 milliard de dollars. Le présent rapport est un sommaire non classifié des activités qu'a menées le CST du 1er avril 2024 au 31 mars 2025. À moins d'indication contraire, « cette année » fait référence à l'année financière 2024 à 2025.

Collectivité des cinq

Le CST est un fier membre de la collectivité des cinq, la plus ancienne et la plus étroite alliance en matière de partage du renseignement au monde. La collectivité des cinq comprend les organismes de renseignement électromagnétique et de cybersécurité du Canada, de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.

Mandat

Le mandat du CST est défini dans la *Loi sur le Centre de la sécurité des télécommunications (Loi sur le CST)*[1] et comporte 5 volets :

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

Le présent rapport met en lumière les efforts déployés cette année pour accroître la sécurité des Canadiennes et Canadiens.

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.

L'ANNÉE 2024 À 2025 EN CHIFFRES

Le CST a connu une année productive! Voici quelques principaux chiffres qui donnent un aperçu des réalisations :

L'effectif en 2024 à 2025

Effectif total	3 841
Taux d'attrition	3 %* (1,3 % – départs volontaires)
Augmentation de l'effectif par rapport à l'année dernière	6 %
Représentation au sein de l'effectif (par auto-identification)	
↳ Femmes	33 %
↳ Personnes handicapées	15 %
↳ Personnes racisées	19 %
↳ Autochtones	3 %
↳ Personnes 2SLGBTQIA+	7 %
Prix des meilleurs employeurs	2 prix (meilleur employeur pour les jeunes et meilleur employeur de la région de la capitale nationale)

Alertes et notifications émises pour se protéger contre les activités malveillantes en 2024 à 2025

Demandes générales reçues par le Centre pour la cybersécurité	13 500
Interventions aux incidents de cybersécurité	Gouvernement du Canada : 1 155 Infrastructures essentielles : 1 406
Notifications de signes avant-coureurs d'une attaque par rançongiciel	336 notifications envoyées à 309 organisations canadiennes
Incidents liés à des rançongiciels qui auraient été évités grâce à ces notifications	Entre 74 et 148, ce qui aurait permis de réaliser des économies allant de 6 à 18 millions de dollars
Évaluations des risques liés à la chaîne d'approvisionnement	1 371
Vulnérabilités communiquées aux fournisseurs	10

Renseignement électromagnétique étranger en 2024 à 2025

Signalements	3 385
Ministères clients	32
Clientes et clients particuliers	3 016
Demandes d'assistance	51

Rapports, publications et conseils diffusés en 2024 à 2025

Publications de conseils en matière de cybersécurité	29
Publications conjointes	20
Évaluations de menaces non classifiées	7
Rapports de renseignement sur la sécurité dans l'Arctique	196

Interactions avec d'autres ministères et des industries des infrastructures essentielles en 2024 à 2025

Séances d'information individuelles offertes	30
Séances de groupe menées avec des équipes de TI et de cybersécurité ainsi qu'avec des cadres de direction	12
Collaborations avec des organisations du gouvernement du Canada pour accroître leur cyberrésilience	150
Présentations	Plus de 200
Séances d'information sur la préparation à la menace que l'informatique quantique fait peser sur la cryptographie	Plus de 30
Exercices de simulation	13
Séances d'information bimensuelles sur les menaces pour les professionnelles et professionnels de la sécurité des TI	38
Séances « Passons à l'action »	7

Interactions avec le public et les médias en 2024 à 2025

Demandes des médias	209
Entrevues	19
Conférences de presse nationales	3
Témoignages devant un comité parlementaire	15
Réponses aux questions inscrites au Feuilleton	142
Inscriptions aux cours offerts par le Carrefour de l'apprentissage	11 895

* Ce chiffre n'inclut pas les emplois d'une durée déterminée et les départs à la retraite.

Responsabilisation, transparence et conformité en 2024 à 2025

Autorisations ministérielles	12
Arrêtés ministériels en vigueur	5
Directives ministérielles	1
Examens externes	
↳ Collaborations aux examens et aux rapports	25
↳ Séances d'information offertes aux organes d'examen	29
↳ Réponses aux questions	412
Divulgation d'informations nominatives sur des Canadiennes et Canadiens	
↳ Reçues (gouvernement du Canada)	669
↳ Reçues (collectivité des cinq)	83
↳ Approuvées	559
↳ Refusées	95
↳ En attente	10
↳ Annulées	88
Incidents de conformité opérationnelle	
↳ Concernant de l'information qui se rapporte à une Canadienne ou à un Canadien	119
↳ Ne concernant pas de l'information qui se rapporte à une Canadienne ou à un Canadien	22
Plaintes externes	
↳ Transmises à la chef du CST	3
↳ Transmises à l'OSSNR	1
Téléversements du portail du gouvernement ouvert	
↳ Jeux de données	5
↳ Éléments d'actif informationnel	47
Demandes présentées en vertu de la *Loi sur l'accès à l'information*	61
Divulgations proactives	5 cahiers de comité
Documents déposés	3
Audits internes	2
Évaluations de programme internes	3
Documents produits à l'appui de l'Enquête publique sur l'ingérence étrangère	plus de 85 000

LE CST REPÈRE LES MENACES ÉTRANGÈRES, LES ATTÉNUE ET Y RÉPOND

Le Canada fait face à un contexte de menace dynamique et complexe. Le CST est déterminé à défendre le Canada contre les menaces étrangères hostiles tout en faisant valoir les intérêts stratégiques, économiques et commerciaux ainsi que les intérêts en matière de sécurité, de défense et de politique étrangère du pays. En étroite collaboration avec ses partenaires nationaux et internationaux, le CST exploite son mandat pour repérer les menaces, se défendre contre elles et prendre des mesures pour perturber les activités d'auteurs de menace étrangers malveillants. Les équipes spécialisées du CST travaillent jour et nuit pour :

- recueillir du renseignement électromagnétique étranger (SIGINT);
- informer le gouvernement du Canada aux plus hautes instances sur la sécurité économique, les affaires diplomatiques, l'extrémisme violent, l'ingérence étrangère, les cybermenaces, la souveraineté dans l'Arctique, le soutien aux opérations militaires et plus encore;
- rédiger et publier des rapports non classifiés et des conseils sur les cybermenaces;
- sensibiliser les parties prenantes de tous les ordres de gouvernement et des secteurs des infrastructures essentielles, au moyen de séances d'information, de cours, de réunions et d'autres activités de sensibilisation, sur la façon de se protéger contre les cybermenaces;
- appuyer les partenaires de sécurité et d'application de la loi en leur fournissant du renseignement pertinent;
- répondre aux cyberincidents, notamment en avisant les personnes et entités qui pourraient être victimes d'incidents liés à des rançongiciels;
- mener des cyberopérations défensives et actives pour répondre aux menaces et les contrer;
- collaborer avec la collectivité des cinq et d'autres partenaires internationaux pour comprendre intégralement le contexte de menace diversifié et établir des réseaux et des relations solides pour affronter ces menaces.

Le CST, tout comme le contexte de menace, évolue. Il s'adapte pour garder une longueur d'avance sur le savoir-faire des États-nations et des auteurs de menace criminels dotés de moyens sophistiqués. Dans un climat géopolitique tendu et incertain, le CST procure au Canada et à ses alliés un avantage stratégique. Il est constamment à l'avant-garde des avancées technologiques au sein de la collectivité de la sécurité et du renseignement pour exécuter son mandat et réaliser les priorités de sa mission.

La diversité au CST

Un effectif diversifié est essentiel à la réalisation de la mission du CST. Des employées et employés provenant de divers milieux offrent une mine de connaissances et de points de vue qui sont essentiels à la collecte de renseignement précis et complet. Par exemple, le fait d'avoir

des locutrices et locuteurs natifs qui comprennent très bien les nuances d'une langue étrangère et de la culture connexe garantit que l'information est interprétée correctement et en contexte. Cette compréhension de la culture permet d'éviter de mauvaises interprétations qui pourraient mener à des évaluations du renseignement erronées.

Une équipe diversifiée offre également des approches de résolution de problèmes variées et des idées novatrices, permettant ainsi au CST d'aborder plus efficacement des problèmes mondiaux complexes. La diversité au CST accroît la capacité de l'organisme à fournir au gouvernement du Canada les bons renseignements pour appuyer la prise de décision stratégique.

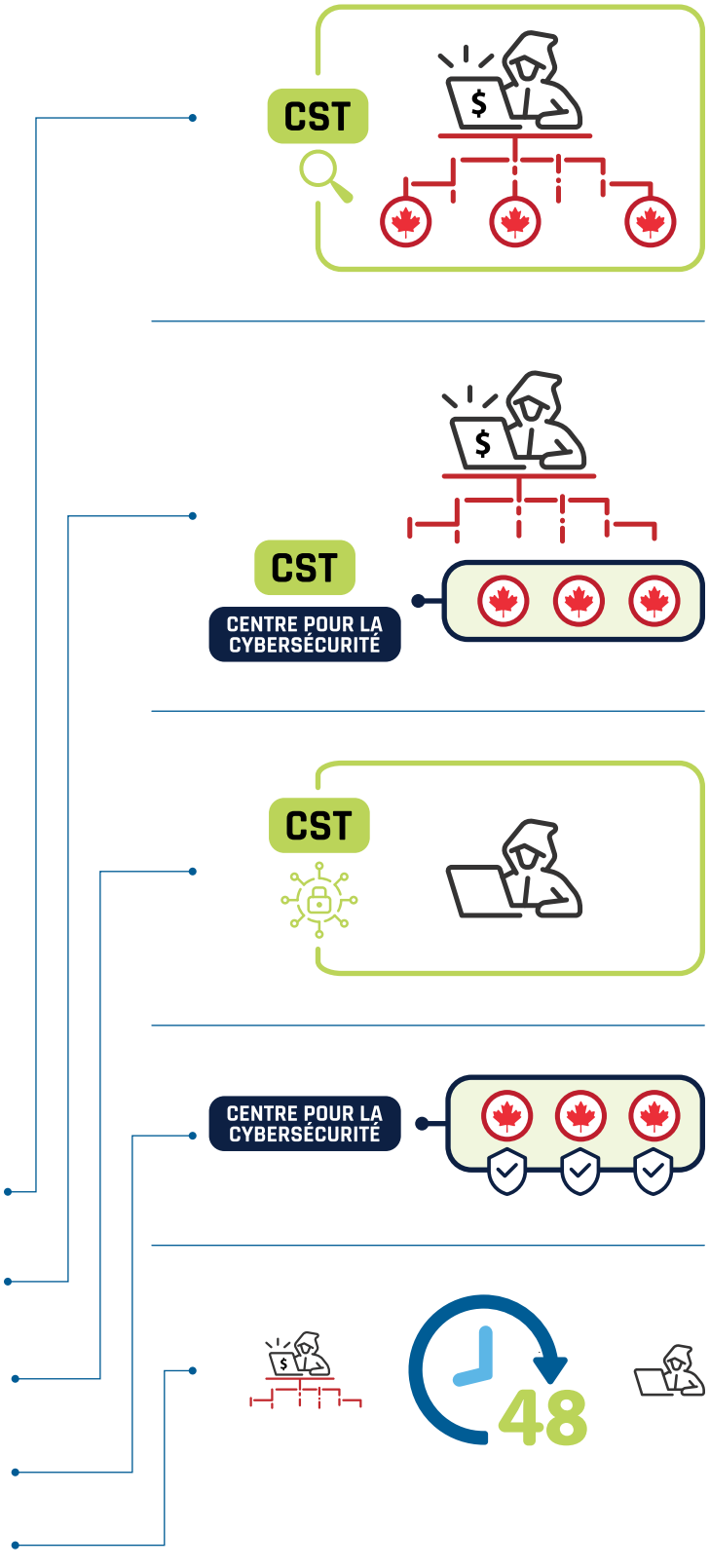
L'interrelation des volets du mandat du CST : un exemple

La *Loi sur le CST* autorise l'organisme à réaliser 2 différents types de cyberopérations : des cyberopérations actives et des cyberopérations défensives. Les deux types d'opérations comportent la prise de mesures dans le cyberespace en vue de contrecarrer les menaces étrangères visant le Canada.

Des **cyberopérations défensives** peuvent servir à protéger les systèmes d'importance et les institutions fédérales lors de cyberincidents majeurs, lorsque les mesures de cybersécurité ne suffisent pas. Des **cyberopérations actives** peuvent servir, de manière proactive, à contrecarrer les menaces étrangères visant les intérêts du Canada en matière d'affaires internationales, de défense ou de sécurité.

Voici un exemple de la façon dont les équipes du renseignement étranger, de la cybersécurité et des cyberopérations du CST ont uni leurs efforts cette année pour contrecarrer une menace visant les Canadiennes et Canadiens :

- À la fin de 2024, le CST a recueilli du renseignement électromagnétique étranger au sujet d'un groupe d'attaque par rançongiciel qui ciblait des victimes canadiennes dans un secteur industriel important pour les infrastructures essentielles du pays.
- L'équipe des cyberopérations étrangères du CST et le Centre pour la cybersécurité ont collaboré afin de repérer les victimes et de contrecarrer la menace.
- L'équipe des cyberopérations étrangères du CST a mené une opération visant à perturber techniquement les activités de l'auteur de menace et à neutraliser la menace.
- Au même moment, le Centre pour la cybersécurité a avisé les victimes et leur a fourni des conseils en matière de cybersécurité.
- La menace a été détectée et contrecarrée dans l'espace de 48 heures.



La collecte, l'analyse et la diffusion de renseignement électromagnétique étranger

Le CST recueille, analyse et diffuse du renseignement électromagnétique étranger (SIGINT) afin de procurer au gouvernement du Canada de l'information au sujet des menaces étrangères à l'appui des intérêts nationaux. Le SIGINT désigne l'interception, le décodage ou le déchiffrement et l'analyse de communications et d'autres signaux électroniques. Il peut comprendre tout type de communication électronique.

Le SIGINT appuie également la prise de décisions et l'élaboration de politiques du gouvernement en matière de défense, de sécurité, de protection et d'affaires internationales en fournissant d'importants renseignements sur les événements mondiaux. Le CST développe une vaste gamme de capacités classifiées sophistiquées pour acquérir du renseignement étranger à l'extérieur du Canada afin de s'adapter aux technologies et aux capacités en évolution de ses adversaires.

Selon la *Loi sur le CST*, les activités de collecte de renseignement étranger du CST ne visent pas des Canadiennes et Canadiens ou des personnes se trouvant au Canada. Les activités de SIGINT à l'étranger sont strictement guidées par les priorités du gouvernement du Canada en matière de renseignement.

Les priorités du Canada en matière de renseignement

En tant que l'un des principaux organismes de renseignement du Canada, le CST appuie les priorités en matière de renseignement[2] du pays. Ces priorités guident la communauté canadienne du renseignement. Le CST oriente son travail de manière à se concentrer sur les menaces les plus pressantes et les plus importantes cernées par le gouvernement du Canada. En tant que producteur de renseignement, les efforts du CST visant à fournir du renseignement qui respectent les priorités du Canada en matière de renseignement appuient directement les intérêts nationaux.

La souveraineté dans l'Arctique

Le CST travaille d'arrache-pied avec ses partenaires nationaux et internationaux pour assurer la sécurité et la souveraineté du Canada dans l'Arctique – une priorité pour le gouvernement du Canada. La nouvelle Politique étrangère du Canada pour l'Arctique mentionne la collaboration du CST comme étant essentielle pour combler l'insuffisance de renseignement afin de contrecarrer la gamme complexe de menaces auxquelles fait face l'Arctique. Le CST continue d'investir pour répondre à la demande croissante de renseignement provenant de diverses parties prenantes de l'Arctique. Il travaillera en étroite collaboration avec ses partenaires nationaux et internationaux pour fournir du renseignement étranger et renforcer ses partenariats, notamment dans les domaines de la cyberdéfense, de la sécurité économique et de la lutte contre l'ingérence étrangère.

Cette année, le CST a communiqué 196 rapports de renseignement sur la sécurité dans l'Arctique à 20 ministères du gouvernement canadien ainsi qu'aux alliés internationaux du Canada. Les rapports comprenaient des informations 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'emploie également 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

Cette année, le CST a pris plusieurs mesures pour renforcer les partenariats qu'il a établis dans l'Arctique. Il a notamment :

- participé à une conférence annuelle sur la sécurité dans l'Arctique organisée à Yellowknife, aux Territoires du Nord-Ouest, avec d'autres organisations fédérales et gouvernements territoriaux;
- 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;
- poursuivi son rôle de premier plan dans les forums internationaux sur les questions polaires;
- organisé une conférence en personne à Ottawa dans le cadre d'un forum international sur le renseignement électromagnétique concernant les deux régions polaires :
  - » Le CST a créé ce forum et continue d'en assurer la direction;
- pris part à un forum sur le renseignement de toutes sources portant exclusivement sur l'Arctique.

Le CST continue d'apporter un soutien aux Forces armées canadiennes (FAC) tandis qu'elles surveillent et suivent les menaces des adversaires étrangers dans la région de l'Arctique. Il apporte notamment un soutien à la Marine royale canadienne et à l'Aviation royale canadienne tandis qu'elles patrouillent dans le Grand Nord et défendent la souveraineté du Canada contre des auteurs de menace étrangers. Il fournit également des indications et des avertissements concernant les aéronefs russes dans le cadre du commandement interarmées du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD) du Canada, et surveille les menaces navales dans un espace de plus en plus encombré.

La sécurité frontalière et les drogues synthétiques illicites

En décembre 2024, le gouvernement du Canada a annoncé son plan visant à renforcer la sécurité frontalière et le système d'immigration du Canada. En particulier, le gouvernement a annoncé un investissement de 180 millions de dollars sur 6 ans pour élargir les capacités de collecte de renseignement et de cyberopérations étrangères du CST, permettant à ce dernier de cibler plus efficacement le crime organisé transnational et le trafic de fentanyl. Les liens qu'entretient le CST en matière de renseignement essentiel au sein du gouvernement du Canada et avec ses partenaires internationaux constituent un atout alors que le CST met en œuvre le Plan frontalier du Canada.

Cette année, le CST a organisé de nouvelles campagnes pour repérer et perturber les réseaux criminels transnationaux responsables des chaînes d'approvisionnement en fentanyl et en opioïdes synthétiques au Canada. Il travaille en étroite collaboration avec ses partenaires nationaux et internationaux pour atteindre cet objectif prioritaire.

Le CST continue de collaborer étroitement avec ses partenaires de la collectivité des cinq, en particulier avec ses homologues américains, pour échanger de l'information et coordonner les opérations visant à perturber les réseaux criminels transnationaux impliqués dans la chaîne d'approvisionnement en drogues synthétiques illicites. Le CST est fier de ses solides partenariats alliés, qui sont essentiels à la sécurité collective du pays.

La Cellule de coordination des opérations et de renseignement

Le CST est un membre actif de la Cellule de coordination des opérations et de renseignement (CCOR) et y contribue de façon importante. Il travaille aux côtés des partenaires suivants du CCOR pour accroître la production, l'analyse, la communication et l'utilisation de renseignement opportun et pertinent auprès des organismes fédéraux d'application de la loi et des services de police compétents partout au Canada :

- Gendarmerie royale du Canada (GRC)
- Agence des services frontaliers du Canada
- Sécurité publique Canada (SP)
- Service canadien du renseignement de sécurité (SCRS)
- Centre d'analyse des opérations et déclarations financières du Canada

Les activités d'États hostiles

Le renseignement étranger du CST fournit d'importantes informations pour appuyer les efforts canadiens et alliés visant à contrer les activités d'États hostiles. Cette année, les rapports de renseignement étranger du CST ont continué de fournir au gouvernement du Canada et à ses alliés des analyses à l'appui des activités suivantes :

- la surveillance des activités d'ingérence étrangère et le renforcement des processus démocratiques;
- la protection de l'écosystème d'innovation du Canada contre les perturbations étrangères;
- le renforcement des infrastructures essentielles contre les tentatives d'espionnage sophistiquées.

La République populaire de Chine

La République populaire de Chine (RPC) exploite et continue d'élargir l'un des systèmes de sécurité et de renseignement les plus vastes et les plus dynamiques au monde. Les activités parrainées par la RPC sont en cause dans des opérations secrètes ciblant des pays démocratiques partout dans le monde, y compris au Canada.

La portée, la capacité et la visée du programme de cyberactivité de la RPC dans le cyberespace sont inégalées. En particulier, pour atteindre ses principaux objectifs politiques et commerciaux, la RPC cible les intérêts canadiens au moyen de cyberopérations, notamment :

- l'espionnage;
- le vol de propriété intellectuelle;
- l'influence malveillante;
- la répression transnationale.

Cette année, en réponse à cette menace, le CST a intensifié sa collaboration avec des partenaires du gouvernement et de l'étranger afin de recueillir du renseignement exploitable et opportun. Plus précisément, il a produit du renseignement étranger sur les auteurs de cybermenace parrainés par la RPC ciblant des institutions et des personnes :

- du gouvernement;
- de la société civile;
- des secteurs militaire et de la défense;
- des médias;
- des infrastructures essentielles;
- des secteurs de recherche et développement avancés.

Le renseignement étranger recueilli par le CST s'est avéré essentiel pour :

- protéger la sécurité relative à la recherche et les institutions démocratiques du Canada contre les menaces parrainées par la RPC;
- habiliter les responsables des politiques à prendre des décisions éclairées quant aux programmes de sécurité économique du Canada;
- permettre au Centre pour la cybersécurité et aux partenaires internationaux d'atténuer les campagnes de cyberespionnage ciblant les réseaux gouvernementaux et les infrastructures essentielles;
- fournir des renseignements opportuns sur les capacités de la RPC et doter les responsables de la cyberdéfense de renseignement exploitable;
- aider le Centre pour la cybersécurité à bloquer les activités de cybermenace provenant de réseaux zombies qui ont compromis des milliers de routeurs résidentiels et de petits bureaux, ou qui ont exploité des dispositifs d'accès vulnérables;
- aider les partenaires canadiens et alliés de la cyberdéfense à repérer une campagne de cyberespionnage ciblant les réseaux gouvernementaux et à y intervenir en tirant parti des vulnérabilités du jour zéro et des portes dérobées sur les dispositifs périmétriques.

La Russie

La Russie et les auteurs de menace alliés à la Russie continuent de repousser les limites d'un comportement acceptable sur la scène mondiale. Il s'agit notamment de mener des activités d'espionnage économique, de diffuser de la désinformation, de discréditer les pays occidentaux, de mener des cyberactivités malveillantes et de promouvoir des opérations d'influence contre le Canada et ses alliés.

Le CST continue de tirer parti du volet de son mandat touchant le renseignement étranger pour contrer ces menaces. Cette année, grâce au renseignement qu'il a recueilli et les rapports qu'il a fournis en temps utile, le CST :

- a contribué à orienter les objectifs stratégiques du gouvernement du Canada, notamment en repérant les entités financières et industrielles que le gouvernement russe utilise pour contourner les sanctions internationales afin de soutenir son économie et sa capacité de financer la guerre en Ukraine;
- a continué d'appuyer les efforts du Canada et de ses alliés pour lutter contre les efforts persistants de désinformation de la Russie dans le cadre d'une campagne plus vaste visant à promouvoir son discours sur la guerre en Ukraine, à discréditer les pays occidentaux, à promouvoir l'influence russe et à exercer des pressions pour mettre fin aux sanctions que les pays occidentaux lui ont imposées;
- a poursuivi ses efforts visant à empêcher les auteurs de menace de la Russie d'obtenir de l'information sensible sur les intérêts canadiens, de s'y ingérer et de les saboter, notamment au moyen de cyberattaques.

RT (Russia Today)

En septembre 2024, le Canada a publié une déclaration condamnant énergiquement les activités de l'entité médiatique russe RT (anciennement Russia Today). L'entité tentait notamment de réduire l'appui du public occidental à l'endroit de l'Ukraine, d'influencer les résultats d'élections dans les États occidentaux et non occidentaux, et de miner le soutien à un engagement envers l'ordre international fondé sur des règles.

Les organismes de renseignement canadiens, avec qui le CST a collaboré, ont indiqué que la Russie utilisait des ressources non traditionnelles pour provoquer des perturbations et solliciter le soutien pour ses activités hostiles à l'échelle internationale, y compris au Canada. Ce travail a dégagé des révélations selon lesquelles RT avait créé des plateformes médiatiques tierces et les utilisait comme outils pour diffuser secrètement du contenu aux auditoires internationaux et occidentaux.

Cybercriminalité

La cybercriminalité continue d'être une menace généralisée et perturbatrice, soutenue par un écosystème mondial de la cybercriminalité prospère et résilient. Le CST continue de surveiller et d'analyser l'écosystème étranger des menaces émanant de la cybercriminalité afin d'enrichir les connaissances du Canada et de la collectivité des cinq sur les auteurs de cybermenace et la souplesse de cet écosystème.

Le CST produit du renseignement sur les tactiques, techniques et procédures utilisées par des cybercriminelles et cybercriminels étrangers et des auteurs de menace étatiques. Ce renseignement procure au Centre pour la cybersécurité des données très fiables afin de freiner les tentatives d'analyse et de violation des systèmes du gouvernement du Canada et d'autres systèmes d'importance.

Cette année, le CST a cerné des milliers d'indicateurs de compromission, ce qui a permis de défendre les réseaux du gouvernement du Canada et de faciliter l'envoi rapide d'avis aux victimes. Il a également tiré parti de ses capacités de SIGINT pour guider les opérations menées par des organismes internationaux d'application de la loi afin de déstabiliser et de démanteler des groupes de cybercriminalité étrangers motivés par des intérêts financiers.

Lutte contre l'extrémisme violent

Le CST s'emploie à repérer les activités d'extrémistes étrangères et étrangers constituant une menace pour le Canada et ses alliés. Il fournit du renseignement étranger précieux pour protéger les Canadiennes et les Canadiens, de même que les intérêts du Canada, contre le terrorisme et l'extrémisme violent. Cela comprend des menaces émanant de l'extrémisme violent à caractère religieux (p. ex. al-Qaïda et ses groupes affiliés) et des

menaces émanant de l'extrémisme violent à caractère idéologique (p. ex. idéologies extrémistes xénophobes, antiautoritaires, fondées sur l'identité de genre et les récriminations personnelles).

Cette année, les efforts déployés par le CST pour contrer l'extrémisme violent se sont étendus au soutien aux victimes d'enlèvements, au signalement des menaces extrémistes envers les alliés et à la couverture des menaces pesant sur les événements publics ainsi que sur les ambassades et les missions canadiennes. Voici d'autres exemples des efforts déployés à cet égard cette année :

- une collaboration étroite avec des partenaires nationaux pour fournir des renseignements essentiels sur les extrémistes étrangères et étrangers qui cherchent à mener des attaques au Canada;
- l'identification des auteurs de menace responsables des alertes à la bombe contre des entités au Canada;
- une concertation avec des partenaires nationaux et internationaux pour produire du renseignement étranger permettant de repérer les auteurs de menace étrangers qui cherchent à influencer ou à inspirer des auteures et auteurs « solitaires » au Canada et ailleurs;
- un soutien aux partenaires internationaux, à de multiples occasions, pour atténuer et parer les menaces extrémistes violentes dans leurs pays respectifs;
- la surveillance des menaces extrémistes visant des événements internationaux;
- la création d'une équipe d'appoint qui a travaillé avec plusieurs partenaires étrangers pour défendre contre les menaces aux Jeux olympiques de Paris en 2024.

Soutien aux opérations militaires

Le CST joue un rôle essentiel dans le soutien aux opérations militaires en fournissant des avertissements ponctuels et une connaissance de la situation afin d'assurer la sécurité du personnel des FAC pendant les déploiements et les exercices. Cette année, le CST a fourni du renseignement en temps utile pour de nombreuses opérations, dont les opérations appelées UNIFIER, REASSURANCE et HORIZON. Le renseignement étranger qu'il a fourni a permis, notamment :

- le repérage de menaces de contre-ingérence à l'endroit du personnel des FAC;
- l'évacuation de Canadiennes et Canadiens des zones de conflit;
- l'examen des activités des entreprises d'État ayant des liens à des fins militaires, en particulier celles qui peuvent cibler les opérations et les exercices au Canada;
- l'identification de tactiques, techniques et procédures de guerre électronique ennemie pour donner aux FAC un meilleur aperçu des systèmes de guerre électronique antagoniste.

Cette année, le CST a appuyé un effort de renseignement visant à repérer les entités commerciales légitimes qui soutiennent secrètement les objectifs militaires, politiques et commerciaux des gouvernements étrangers pour perturber les opérations des FAC et des alliés.

De plus, le CST a poursuivi ses efforts pour repérer les opérations de commandement, de contrôle, de communication, d'informatique, de renseignement, de surveillance, de reconnaissance et de ciblage par des adversaires étrangers qui pourraient constituer une menace pour les forces canadiennes et alliées menant des opérations.

Le CST fournit également du renseignement précieux aux forces partenaires. Cette année, les efforts consentis par le CST en matière de renseignement ont permis aux FAC d'informer les forces partenaires des intentions et des capacités des adversaires et de protéger le personnel déployé.

Conduite de cyberopérations étrangères

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

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

Le CST a un cadre de gouvernance bien établi pour le guider en matière de cyberopérations étrangères et s'assurer que ces opérations sont conformes à la *Loi sur le CST* et aux autorisations ministérielles. Cela comprend 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[3].

Élargissement du portefeuille des cyberopérations étrangères

Dans son budget 2024, le gouvernement a annoncé un financement supplémentaire afin de permettre au CST et à AMC d'améliorer leurs programmes de renseignement et de cyberopérations pour répondre aux menaces changeantes et de plus en plus complexes pour la sécurité nationale, la prospérité et la démocratie du Canada. Ce financement a permis au CST d'élargir stratégiquement la portée et l'ampleur de ses cyberopérations étrangères.

Le premier ministre a également demandé au CST d'utiliser les fonds affectés dans le cadre de l'initiative de sécurité frontalière pour renforcer les cyberopérations visant à rompre les chaînes d'approvisionnement en drogues illicites (p. ex. le fentanyl).

Capacité conjointe en matière de cyberopérations

Dans le budget 2024 et la mise à jour de la politique de défense du gouvernement du Canada, le CST a reçu d'importants nouveaux investissements pour continuer d'élargir son programme de cyberopérations étrangères afin de contrer le nombre croissant de menaces qui pèsent sur la sécurité du Canada.

Dans cette politique mise à jour, le CST, le ministère de la Défense nationale (MDN) et les FAC ont reçu l'ordre de mettre sur pied une « capacité conjointe canadienne en matière de cyberopérations ». Cette capacité s'appuie sur les éléments fondamentaux du CST, qui s'emploie à promouvoir l'initiative en étroite collaboration avec le tout nouveau Commandement Cyber des Forces armées canadiennes (CAFCYBERCOM).

En investissant dans son personnel, ses outils et ses partenariats, le CST, le MDN et les FAC établissent la cyberforce de l'avenir tout en continuant à contrer les menaces auxquelles le Canada fait face à l'heure actuelle.

Cette année, le CST a mené de nombreuses cyberopérations étrangères pour :

- défendre la population canadienne contre les cybermenaces malveillantes parrainées par des États ou non;
- perturber les activités d'espionnage visant le gouvernement du Canada;
- contrecarrer les campagnes de désinformation étrangères;
- protéger les Canadiennes et Canadiens contre l'extrémisme violent.

Vous trouverez ci-après des exemples de cyberopérations étrangères menées cette année pour lutter contre les rançongiciels et déstabiliser les organisations extrémistes violentes.

Lutte contre les rançongiciels

Cette année, le CST a lancé une campagne visant à lutter contre les 10 plus importants groupes d'attaque par rançongiciel influant sur le Canada et ses alliés.

Il a également participé à une opération multinationale visant à nuire aux activités d'un tel groupe. Le CST a utilisé diverses techniques secrètes pour réduire et perturber les activités illicites de ce groupe, ce qui a grandement nui à la capacité de ce dernier de cibler des Canadiennes et Canadiens.

Déstabilisation des organisations extrémistes violentes

En plus de permettre de perturber concrètement des activités d'extrémistes étrangères et étrangers, le renseignement provenant du CST a servi à étayer ses cyberopérations actives contre des organisations extrémistes violentes. Selon une approche multidimensionnelle ciblant l'infrastructure technique et la présence en ligne d'organisations extrémistes violentes, le CST a mené des cyberopérations actives pour :

- miner la crédibilité et l'influence des chefs de groupe clés, réduisant ainsi leur capacité à inspirer et à diriger;
- affaiblir la confiance et la cohésion entre les chefs et les adeptes, pour compromettre l'unité et la force de ces organisations;
- mettre en lumière les risques juridiques et personnels associés à la participation aux activités d'organisations extrémistes violentes, pour potentiellement dissuader des personnes de participer;
- supprimer le contenu violent et extrémiste des plateformes en ligne, privant ainsi les organisations extrémistes violentes d'un outil essentiel à la radicalisation et au recrutement.

Ensemble, ces mesures ont affaibli la présence et l'influence en ligne des organisations extrémistes violentes, en entravant leur capacité à mener des opérations et en réduisant la menace qu'elles représentent pour le Canada et ses alliés.

Publication des évaluations des menaces

Dans le contexte de menace actuel en constante évolution, il est plus important que jamais de tenir les Canadiennes et Canadiens au fait de la situation. Le CST s'engage à faire en sorte que les ordres de gouvernement, les communautés autochtones, les parties prenantes des infrastructures essentielles, les professionnelles et professionnels des TI et le grand public comprennent les cybermenaces auxquelles fait face le Canada. C'est pourquoi il publie en temps utile des évaluations des cybermenaces non classifiées. Les évaluations permettent au CST d'établir ses priorités de mission, en plus de favoriser une meilleure compréhension des cybermenaces qui guettent le Canada, et des façons de les contrer, auprès de son lectorat.

Cette année, le CST a publié 2 évaluations des cybermenaces importantes, à savoir l'Évaluation des cybermenaces nationales 2025–2026 (une évaluation prospective) et une mise à jour du document « Cybermenaces contre le processus démocratique du Canada ». Le CST a également publié 5 évaluations des menaces non classifiées :

- Manipulation ciblée : Campagnes de piratage psychologique et de harponnage de l'Iran
- Bulletin sur les cybermenaces : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC
- La cybermenace ciblant des laboratoires de recherche
- Bulletin sur les cybermenaces : cybermenaces visant les grands événements sportifs internationaux
- Bulletin sur les cybermenaces : Cyberactivités parrainées par la République populaire de Chine et menées contre les gouvernements provinciaux, territoriaux et autochtones et les administrations municipales du Canada

Par suite de ces évaluations, le Centre pour la cybersécurité a répondu à des dizaines de demandes d'information et a donné plus de 100 séances d'information sur les menaces aux fournisseurs d'infrastructures essentielles et aux différents ordres de gouvernement.

Évaluation des cybermenaces nationales 2025-2026

L'Évaluation des cybermenaces nationales (ECMN) 2025-2026 fait état des principales cybermenaces provenant des États adversaires, des menaces émanant de la cybercriminalité de même que des tendances façonnant le contexte de cybermenace du Canada. L'ECMN présente les six avis principaux suivants :

- Les États adversaires du Canada recourent à des cyberopérations pour causer des perturbations et créer des divisions.
- Le vaste et vigoureux programme de cyberactivité de la RPC représente pour le Canada la cybermenace la plus active et la plus sophistiquée à l'heure actuelle.
- Le programme de cyberactivité de la Russie renforce l'ambition de Moscou de vouloir confronter et déstabiliser le Canada et ses alliés.
- L'Iran se sert de son programme de cyberactivité pour contraindre, harceler et réprimer ses adversaires et gérer les risques d'escalade.
- Le modèle opérationnel de cybercriminalité comme service (CaaS pour *Cybercrime-as-a-Service*) contribue sans doute au fait que la cybercriminalité se poursuit au Canada et dans le monde.
- Les rançongiciels constituent la principale menace émanant de la cybercriminalité à laquelle font face les infrastructures essentielles du Canada.

Portée et incidence de l'ECMN

La portée et l'incidence de l'ECMN s'avèrent essentielles, car il s'agit d'un produit phare du CST. Cette année, le lectorat de l'ECMN s'est grandement accru. En effet, durant la première semaine de publication, le rapport a été consulté 3 fois plus que son édition précédente. En une semaine seulement, plus de 7 500 personnes ont consulté l'ECMN. Le lectorat englobait des personnes habitant aux quatre coins du monde, mais vivant surtout dans les pays membres de la collectivité des cinq. L'augmentation du lectorat de l'ECMN de cette année remplit le CST de fierté et l'organisme explora de nouvelles façons de faire pour amplifier la consultation des prochains rapports.

Cybermenaces contre le processus démocratique du Canada

En mars 2025, le CST a publié une mise à jour sur les cybermenaces contre le processus démocratique du Canada qui soulignait l'utilisation croissante de l'IA par des adversaires étrangers afin de cibler les élections tenues partout dans le monde, notamment au Canada. Le rapport faisait état des conclusions principales suivantes :

- Des auteurs de menace étrangers, plus particulièrement des auteurs de menace affiliés à la Russie et à la RPC, tirent profit de l'IA pour semer la division et susciter la méfiance au sein des sociétés démocratiques.
- L'IA permet à des auteurs de menace étrangers hostiles d'inonder l'environnement de l'information de fausses informations, en créant entre autres de la désinformation et en mettant en place des réseaux zombies qui diffusent cette désinformation.
- Les auteurs de menace étrangers ont de plus en plus recours à l'IA générative pour créer et relayer de la désinformation de façon virale; les répercussions pourraient s'accroître parallèlement à l'évolution continue et à l'accessibilité accrue de ces méthodes.
- Des cybercriminelles et cybercriminels de même que des auteurs de menace parrainés par des États feront probablement appel à l'IA afin de perfectionner leurs attaques par piratage psychologique contre des personnalités politiques et des institutions électorales dans un futur proche.
- Des États-nations recueillent d'énormes quantités de données et exploitent l'IA pour en accélérer leurs analyses; ils améliorent ainsi leurs capacités à mener des campagnes d'influence et d'espionnage ciblées.
- L'IA permet de créer des hypertrucages pornographiques qui ciblent des personnalités publiques et politiques, principalement des femmes et la communauté 2SLGBTQIA+.

Lors de la première semaine de publication de la mise à jour, la page du rapport a été consultée près de 2 000 fois et les publications connexes sur les réseaux sociaux ont été vues plus de 16 000 fois. Les principaux médias ont beaucoup parlé du rapport et l'on estime que plus de 13 millions de personnes en ont entendu parler.

Protection des institutions démocratiques et des infrastructures essentielles du Canada

Les activités de cybermenace ciblant les processus démocratiques et les infrastructures essentielles sont à la hausse partout dans le monde. De 2024 à 2025, le CST a collaboré avec des partenaires clés pour aider à protéger l'intégrité des élections, des institutions démocratiques et des infrastructures essentielles du pays. L'organisme a entre autres offert des séances d'information pour sensibiliser les gens aux menaces croissantes, puis a coopéré avec des partenaires pour accroître la résilience en matière de cybersécurité dans ce contexte important.

Soutien aux institutions fédérales

Cette année, le CST et le Centre pour la cybersécurité ont continué d'apporter leur soutien aux institutions fédérales, en les aidant en cas de cyberincidents, en atténuant les cybermenaces, en fournissant de l'information aux ministères victimes de cyberincidents et en augmentant de façon générale la cyberrésilience à l'échelle du gouvernement fédéral. Ils ont collaboré avec 150 organisations du gouvernement du Canada et ont offert des séances d'information exhaustives en ciblant principalement les ministères et organismes de petite taille, étant donné que ces derniers courent un risque accru par rapport aux cybermenaces et aux cyberattaques.

Durant l'année, ils ont offert un soutien et des services variés aux institutions fédérales afin d'aider à accroître la cyberrésilience à l'échelle du gouvernement fédéral. Les services suivants ont entre autres été proposés :

- donner des avis et des conseils;
- évaluer l'intégrité des chaînes d'approvisionnement;
- soutenir les capacités de communications sécurisées;
- superviser et produire des évaluations des menaces pour appuyer des projets, des initiatives et des services gouvernementaux de priorité élevée, dont les répercussions et les risques sont accrus;
    - » Exemples : le projet Visibilité, sensibilisation et sécurité de point d'extrémité de Services partagés Canada (SPC), l'infrastructure secrète de prochaine génération du gouvernement du Canada, le programme de modernisation du versement des prestations d'Emploi et Développement social Canada (EDSC).

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

Le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (Groupe de travail MSRE) est un groupe pangouvernemental chargé de coordonner les efforts de collecte et d'analyse du gouvernement du Canada en ce qui a trait aux menaces visant les processus électoraux du gouvernement fédéral. En tant que membre du Groupe de travail MSRE, le CST collabore avec le SCRS, la GRC et AMC.

Cette année, le Groupe de travail MSRE a surveillé et évalué les menaces d'ingérence étrangère visant les élections partielles fédérales et, pour la toute première fois, une course à la direction d'un parti politique fédéral. Le personnel du programme de renseignement électromagnétique étranger du CST a cherché à obtenir du renseignement étranger concernant les sujets suivants :

- l'objectif ou les mesures prises par des auteurs de menace étatiques étrangers afin de s'ingérer dans les processus démocratiques du Canada ou de les influencer;
- les tentatives visant à influencer le résultat des processus démocratiques canadiens ou à miner la confiance du public par rapport à l'intégrité de ces processus;
- des cybermenaces étrangères ciblant des institutions démocratiques, dont l'infrastructure, les candidates et candidats ou les partis politiques associés aux élections.

Le Centre pour la cybersécurité a quant à lui contribué à assurer la cybersécurité lors de ces événements en menant les activités suivantes :

- surveiller les cyberactivités malveillantes ciblant Élections Canada ou l'infrastructure et l'information électroniques des institutions démocratiques (y compris des partis politiques);
- renseigner les partis politiques sur les cybermenaces courantes et sur les pratiques exemplaires en matière de cybersécurité;
- mettre en service, pour le signalement des cyberincidents, une ligne d'assistance que peuvent appeler en tout temps les partis et les candidates et candidats.

Soutien aux efforts de préparation liés à l'élection générale de 2025

Après le déclenchement de l'élection générale de 2025, le 23 mars 2025, le CST s'est aussitôt mis au travail pour soutenir Élections Canada. Son équipe a sécurisé les accréditations nécessaires, a organisé des séances de formation et s'est assurée que le personnel d'Élections Canada pouvait accéder rapidement au Réseau canadien Très secret (RCTS) pour consulter de l'information essentielle et classifiée.

La période d'élection générale s'est surtout déroulée après l'exercice 2024 à 2025 et n'est donc pas abordée dans le présent rapport. Le CST est impatient de fournir dans le prochain rapport annuel des détails sur les efforts déployés durant cette période, y compris sur le travail qu'il a mené en appui au Protocole public en cas d'incident électoral majeur et en réponse aux cas de répression transnationale qui ont été observés.

Stratégie nationale de cybersécurité

En février 2025, le gouvernement du Canada a publié sa nouvelle Stratégie nationale de cybersécurité (SNCS)[4]. La SNCS énonce le plan à long terme du Canada afin d'établir des partenariats avec les provinces et les territoires, les forces de l'ordre, les industries, les communautés autochtones et le milieu universitaire. Le pays sera ainsi plus à même de relever les défis en matière de cybersécurité auxquels il fait face.

Le CST joue un rôle important dans la SNCS et assume les responsabilités suivantes :

- protéger les systèmes gouvernementaux;
- diriger les efforts de défense de la cybersécurité et d'intervention en cas d'incident;
- servir d'autorité technique en matière de cybersécurité du Canada;
- offrir des avis, des conseils et des services à différents secteurs;
- promouvoir la collaboration, les partenariats, l'innovation et les cybercompétences au sein des secteurs.

En tant que leader opérationnel en cybersécurité du Canada, le Centre pour la cybersécurité fournit des orientations et du renseignement sur les menaces.

Contributions du CST dans le cadre de la SNCS

Les contributions apportées par le CST dans le cadre de la SNCS sont importantes. À titre d'exemple, de concert avec les partenaires de la collectivité des cinq, il a surveillé étroitement les activités malveillantes des auteurs de cybermenace parrainés par la RPC, dont Volt Typhoon et Salt Typhoon. Le Centre pour la cybersécurité a également communiqué directement avec des fournisseurs de services canadiens pour qu'ils comprennent bien la nature et l'importance de la menace que pose la campagne de piratage Salt Typhoon.

Collectif canadien de cyberdéfense

Dans le cadre de la SNCS, le gouvernement du Canada a établi le Collectif canadien de cyberdéfense (CCCD). Le CCCD a pour objectif de renforcer et de faire progresser la cyberrésilience du Canada par l'intermédiaire d'interventions directes de la part des secteurs public et privé, de sorte à répondre aux priorités politiques et aux défis nationaux relatifs à la cybersécurité, et à mener des opérations connexes.

Le CCCD s'assure que la population canadienne, les entreprises, les gouvernements provinciaux et territoriaux, les municipalités, les gouvernements autochtones et les opérateurs d'infrastructures essentielles profitent des bénéfices liés aux innovations, aux pratiques exemplaires et au renseignement communiqué. 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 2 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 et ainsi aider à protéger les systèmes d'importance et à réduire l'exposition aux cybermenaces du Canada.

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. La composition du Forum opérationnel sera appelée à changer selon les besoins opérationnels.

Sa mise sur pied est toujours en cours. Cette année, l'accent a été mis sur l'établissement des processus et des technologies nécessaires pour favoriser la réalisation d'activités coordonnées entre différents partenaires de l'industrie. L'un des sous-groupes du CCCD a eu une rencontre initiale en janvier 2025.

Le Forum stratégique, coprésidé par Sécurité publique et le Centre pour la cybersécurité, est le comité consultatif décisif 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 régler des enjeux de cybersécurité auxquels fait face le Canada. À l'instar du Forum opérationnel, le Forum stratégique est en voie d'être mis sur pied.

Soutien aux provinces et aux territoires

Les auteurs de cybermenace comme la RPC perçoivent presque certainement les gouvernements provinciaux, territoriaux et autochtones, et les administrations municipales comme des cibles précieuses de cyberespionnage. Les activités de cybermenace menées contre ces ordres de gouvernement reflètent probablement celles dont fait continuellement l'objet le gouvernement du Canada. Tous les réseaux gouvernementaux contiennent de l'information sur des prises de décisions et sur des dossiers régionaux, ainsi que des renseignements personnels sur des Canadiennes et Canadiens.

Le renforcement de la collaboration en matière de cybersécurité avec les provinces et les territoires demeure une priorité importante pour le CST. L'organisme collabore avec des partenaires provinciaux et territoriaux afin d'atténuer les compromissions constantes et de les aviser des possibles activités de cybermenace malveillantes menées par des auteurs dotés de moyens sophistiqués. Il aide aussi les autres ordres de gouvernement à mieux évaluer les menaces et à se remettre plus facilement de la compromission de leurs systèmes.

De 2024 à 2025, à la suite d'une série d'incidents de cybersécurité ciblant des établissements du nord du Canada et avec l'autorisation du ministre, 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 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.

Soutien aux provinces et aux territoires pour qu'ils comprennent mieux leur posture par rapport aux menaces à la cybersécurité

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 offerts par le Centre pour la cybersécurité et qui permet donc aux utilisatrices et utilisateurs de mieux comprendre leur posture unique par rapport aux menaces à la cybersécurité. Les rapports d'ObservationDeck sont étoffés d'analyses commerciales, internes et de source ouverte qui font le sommaire des biens TI du ministère visé et de leurs vulnérabilités.

Le Centre pour la cybersécurité a aussi accueilli sa deuxième table ronde annuelle sur la cybersécurité, qui est consacrée entièrement à la collaboration entre les responsables de la cybersécurité des gouvernements fédéral, provinciaux et territoriaux. Parmi les sujets de discussion abordés, notons la planification des interventions en cas d'incidents, la gestion des risques liés à la chaîne d'approvisionnement, le soutien en vue des élections et les menaces que posent les technologies perturbatrices.

Le Centre pour la cybersécurité a activement contribué à améliorer la compréhension des provinces et des territoires par rapport à leur posture de cybersécurité. Pour ce faire, il a entre autres présenté des séances d'information classifiées durant lesquelles ses partenaires ont reçu de l'information additionnelle sur les menaces actives et potentielles. Cette année, le Centre pour la cybersécurité a présenté aux provinces et aux territoires une séance d'information classifiée sur les menaces durant laquelle de l'information essentielle sur les cybermenaces actuelles et émergentes a été diffusée. Le Centre pour la cybersécurité a aussi offert des séances d'information de différents niveaux de classification à de hautes et hauts fonctionnaires provinciaux et territoriaux, notamment aux premières ministres et aux premiers ministres et à des membres du personnel électoral.

Soutien aux communautés autochtones

Le Centre pour la cybersécurité a une équipe des Partenariats autochtones qui se concentre sur l'établissement de relations avec les communautés autochtones en se concentrant sur la reconnaissance des droits, le respect et le partenariat. Elle respecte le principe « rien pour elles sans elles » et veille à ce que les initiatives et les projets soient axées sur les communautés, soient fondées sur la nation et visent à éliminer les obstacles. Cette année, l'équipe des Partenariats autochtones :

- a participé à un groupe de travail sur la sécurité dans l'Arctique qui a réuni les gouvernements fédéral, territoriaux et autochtones;
- a participé à la conférence de l'Alliance nationale autochtone des technologies de l'information;
- a offert les services du Centre pour la cybersécurité ainsi que des avis et conseils aux organismes autochtones;
- a bâti des relations avec des entités autochtones afin d'appuyer les activités d'intervention en cas d'incident.

Le Centre pour la cybersécurité a également publié un bulletin sur les cybermenaces concernant les cyberactivités parrainées par la RPC contre les gouvernements provinciaux, territoriaux et autochtones ainsi que les administrations municipales[5], une publication qu'il a également transmis aux gouvernements autochtones.

Soutien aux infrastructures essentielles

Il est essentiel de continuer de développer des partenariats solides avec les secteurs des infrastructures essentielles afin de prévenir toute perturbation qui pourrait engendrer des conséquences graves et généralisées pour la population canadienne. Des partenariats stratégiques avec des opérateurs et des propriétaires d'infrastructures essentielles du Canada ont été établis, ce qui permet de communiquer de l'information avancée sur les cybermenaces, de promouvoir l'intégration des technologies de cyberdéfense et de favoriser une collaboration profonde.

Cette année, le CST a collaboré et a établi des partenariats avec les secteurs des infrastructures essentielles des façons suivantes :

- collaborer avec des opérateurs de réseau mobile et des spécialistes de la sécurité mondiale pour cerner les nouvelles menaces et mettre en œuvre des activités visant à renforcer la cyberrésilience des réseaux 5G canadiens;
- prendre part à plus de 200 présentations auxquelles ont participé des secteurs des infrastructures essentielles, dont les suivants :
  - énergie (électricité, pétrole, mines, énergie nucléaire);
  - petites et moyennes entreprises;
  - eau;
  - base industrielle de défense;
  - santé;
  - transport;
  - finances;
  - télécommunications et technologies de l'information et des communications;
- présenter 38 séances d'information bimensuelles sur les menaces, dont l'auditoire comptait chaque fois plus de 600 participantes et participants du domaine de la sécurité des TI provenant des secteurs des infrastructures essentielles du Canada;
- participer à 13 exercices de simulation;
- tenir 7 séances « Passons à l'action » durant lesquelles étaient présentées des informations exploitables, et des séances spécialisées sur des sujets techniques comme l'IA, les menaces quantiques et la cryptographie post-quantique, de même que la cybercriminalité.

Accueil conjoint du premier Forum sur les menaces contre la sécurité nationale pour les institutions financières fédérales (IFF)

En février, le CST a eu l'honneur d'accueillir le premier Forum sur les menaces contre la sécurité nationale pour les IFF en collaboration avec ses partenaires du SCRS et du Bureau du surintendant des institutions financières Canada (BSIF). Plus de 150 représentantes et représentants des IFF, responsables aux niveaux provinciaux et fédéral et spécialistes en sécurité nationale y ont discuté de l'environnement de menace propre au secteur financier du Canada.

Des spécialistes en la matière du Centre pour la cybersécurité et des spécialistes du Centre de renseignement financier et du Centre de mission Sécurité économique et Technologie du SCRS ont présenté aux membres du secteur financier des séances d'information adaptées sur l'environnement de menace.

En plus de sensibiliser les membres d'un secteur important des infrastructures essentielles concernant l'environnement de menace, cet événement a ouvert la voie à l'établissement de partenariats solides et de nouvelles possibilités de collaboration avec d'autres ministères du gouvernement, dont le BSIF.

Évaluations des risques liés à la chaîne d'approvisionnement

Afin de soutenir et de protéger les infrastructures essentielles fédérales, le CST a mené des évaluations des risques pour la clientèle du gouvernement du Canada souhaitant se procurer de l'équipement de TI. Ces évaluations prennent en compte un grand nombre de facteurs, dont les vulnérabilités techniques des produits et les pratiques d'affaires, la cybermaturité et la question de la propriété étrangère relativement aux fournisseurs. Le CST travaille de plus en plus avec des partenaires qui ne font pas partie du gouvernement fédéral, comme des partenaires des provinces, des territoires et du secteur privé, en ce qui a trait aux risques liés à la chaîne d'approvisionnement.

Cette année, le CST a mené 1 371 évaluations des risques liés à la chaîne d'approvisionnement. Il a aussi publié les 2 documents d'orientation suivants concernant la sécurité de la chaîne d'approvisionnement :

- Cybersécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations (ITSAP.00.070)[6]
- Conseils conjoints sur le choix de technologies sécurisées et vérifiables[7]

Sécurité des communications

Le CST agit comme l'autorité en matière de sécurité des communications (COMSEC) du Canada. Conformément au volet de son mandat touchant l'assurance de l'information, il continue d'améliorer son programme COMSEC grâce aux membres de la collectivité COMSEC qui travaillent de façon collaborative et constructive à l'échelle du gouvernement du Canada.

Dans le cadre de son programme des communications sécurisées, le CST a procédé cette année à la mise en œuvre graduelle du Programme d'intégrateurs fiables[8]. Ce programme reconnaît des organisations tierces en matière de sécurité des TI qui ont su démontrer leur connaissance et leur expérience par rapport au développement, à la mise en œuvre et à la mise à l'essai de solutions sécurisées sur mesure.

Cette année, le CST a également organisé l'atelier annuel du Groupe des utilisatrices et utilisateurs des dispositifs de communications sécurisées, durant lequel des collectivités COMSEC opérationnelles et stratégiques se sont réunies pour cerner les synergies, améliorer les flux de travaux et renforcer les pratiques de sécurité.

L'équipe COMSEC du CST a aussi accueilli des dirigeantes principales et des dirigeants principaux de la Sécurité ainsi que des autorités COMSEC de différents ministères et de diverses entreprises lors d'un événement classifié qui a permis de parler du contexte cryptographique en pleine évolution et de l'importance de la collaboration si l'on souhaite conserver une longueur d'avance sur les menaces.

Préparation à la cryptographie post-quantique

La cryptographie est un fondement de la cybersécurité, et elle est essentielle à la sécurisation des données et des communications. On prévoit cependant que les ordinateurs quantiques deviendront assez gros pour déchiffrer la cryptographie qui est actuellement utilisée dans le monde, et ce, dès les années 2030.

Or, plutôt que de paniquer, le CST planifie l'avenir. Dans le cadre du volet de son mandat touchant l'assurance de l'information, le CST continue de moderniser ses systèmes cryptographiques. Il a aussi pris de nombreuses mesures afin de sensibiliser aux menaces quantiques les partenaires provenant du gouvernement, de l'industrie et des secteurs des infrastructures essentielles, et d'aider les parties prenantes à se préparer à la transition vers la cryptographie post-quantique. Cette année, parmi les activités principales qui ont été menées, nous comptons les suivantes :

- publier des documents d'orientation à jour sur la cryptographie;
- continuer de contribuer au processus de normalisation internationale pour la cryptographie post-quantique, par exemple, en offrant de la rétroaction publique sur 3 projets de normes menés par le US National Institute of Standards and Technology;
- travailler avec des partenaires fédéraux afin de planifier la mise en œuvre de la cryptographie post-quantique au sein du gouvernement du Canada, lorsque les normes internationales seront finalisées;
- présenter plus de 30 séances d'information à des partenaires provenant du gouvernement, de l'industrie et des secteurs d'infrastructures essentielles sur la menace quantique et sur la façon de se préparer à la transition vers la cryptographie post-quantique, en abordant entre autres l'importance de recourir à la cryptographie normalisée et validée pour éviter toute vulnérabilité de sécurité;
- prendre part à la Journée de l'industrie sur la migration vers la cryptographie post-quantique en donnant une présentation à des partenaires importants de l'industrie sur la stratégie de transition vers la cryptographie post-quantique du gouvernement du Canada.

Intervention en cas de cyberincidents et prévention des cyberincidents

Cette année, le Centre de réception du Centre pour la cybersécurité a reçu, trié et géré environ 13 500 demandes générales, notamment pour ce qui suit :

- des avis et des conseils en matière de cybersécurité;
- l'inscription à des services et à des outils du Centre pour la cybersécurité;
- des services de coordination et de soutien pour gérer les incidents.

Mon cyberportail

La hausse des demandes générales de cette année découle en partie des demandes d'inscription à de nouveaux services offerts sur Mon cyberportail[9], qui permet aux utilisatrices et utilisateurs de partout au Canada de signaler des cyberincidents et de soumettre des échantillons de maliciel.

Cette année, Mon cyberportail comptait plus de 1 000 utilisatrices et utilisateurs du gouvernement du Canada et plus de 2 600 utilisatrices et utilisateurs ne travaillant pas au gouvernement du Canada. Le CST a également entrepris des travaux pour élargir Mon cyberportail et rafraîchir son interface pour que les institutions fédérales puissent recevoir et consulter des cas de cyberincident.

Gestion des incidents

Cette année, le Centre pour la cybersécurité a aidé à répondre à 2 561 incidents de cybersécurité au sein du gouvernement du Canada (1 155) et des infrastructures essentielles du Canada (1 406). Il s'agit d'une augmentation comparativement à l'an dernier (2 192 incidents), qui est attribuable en grande partie à la hausse des cas ciblant les infrastructures essentielles.

Le Centre pour la cybersécurité a aussi reçu 843 rapports de cyberincident de la part d'institutions fédérales (463) et des infrastructures essentielles du Canada (380).

Selon le Centre pour la cybersécurité, la définition d'un cyberincident[10] englobe une grande variété de tentatives d'activité de menace, réussies ou non.

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

Les notifications de signes avant-coureurs d'une attaque par rançongiciel permettent d'avertir rapidement les victimes potentielles lors de la phase d'accès initial d'un incident lié à un rançongiciel. Elles permettent aux responsables de la défense des réseaux de localiser précisément la compromission et de la contrecarrer avant que ne survienne le chiffrement ou le vol des données.

Cette année, le Centre pour la cybersécurité a envoyé 336 notifications de signes avant-coureurs d'une attaque par rançongiciel à plus de 309 organisations canadiennes. Les cibles se trouvaient 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.

Les notifications de signes avant-coureurs d'une attaque par rançongiciel se fondent sur les 3 principales sources d'information suivantes :

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

Exemple d'une situation où des signes avant-coureurs d'une possible attaque par rançongiciel ont été observés

Voici un exemple des mesures prises par le Centre pour la cybersécurité lorsque des signes avant-coureurs d'une attaque par rançongiciel ont été observés cette année :

- Un partenaire de confiance a indiqué au Centre pour la cybersécurité qu'un système d'une institution d'infrastructures essentielles du Canada contenait un maliciel d'accès initial en vue d'une possible attaque par rançongiciel.
- Le Centre pour la cybersécurité a collaboré étroitement avec des partenaires canadiens spécialisés en intervention en cas de cyberincident pour transmettre à l'institution ciblée une notification concernant des signes avant-coureurs d'une attaque par rançongiciel après les heures de travail régulières.
- L'institution a rapidement désactivé et bloqué les comptes et les dispositifs concernés pour atténuer la menace immédiate.
- Le Centre pour la cybersécurité a rencontré les responsables de l'institution pour offrir des avis et des conseils sur la prévention d'incidents similaires.

Incidence financière liée aux notifications de signes avant-coureurs d'une attaque par rançongiciel

Selon le bulletin L'incidence du cybercrime sur les entreprises canadiennes[11] de Statistique Canada, 16 % des entreprises canadiennes ont été victimes d'un incident de cybersécurité en 2023. Parmi les victimes ayant payé une rançon, 84 % ont déboursé moins de 10 000 $ et 4 % ont payé plus de 50 000 $. Le total des coûts de reprise des activités en 2023 s'est élevé à environ 1,2 milliard de dollars.

Selon des hypothèses conservatrices et des estimations de coûts moyens de reprise des activités, on juge que les notifications de signes avant-coureurs d'une attaque par rançongiciel du Centre pour la cybersécurité pourraient avoir empêché entre 74 et 148 incidents liés à des rançongiciels de 2024 à 2025, ce qui aurait permis de réaliser des économies estimées de 6 à 18 millions de dollars. Il faut aussi ajouter que cette estimation ne tient compte que d'une partie du véritable avantage, car les données de Statistique Canada ne comprennent pas les coûts indirects, comme l'atteinte à la réputation, la période d'indisponibilité opérationnelle, les frais juridiques et les conséquences liées à l'assurance.

Prestation de soutien et d'expertise lors d'événements mondiaux

Des employées et employés du CST sont disponibles en tout temps pour contrer les menaces visant le Canada ainsi que la population canadienne à l'étranger. Le Centre opérationnel de production et de coordination du CST (COPCC) coordonne les interventions en cas de crises internationales et de cyberincidents graves. Cette année, le COPCC a réalisé ce qui suit :

- informer le Centre pour la cybersécurité de 94 incidents de cybersécurité après les heures de travail régulières;
- aviser les parties prenantes du CST de 18 incidents mondiaux ou terroristes importants;
- aviser les parties prenantes du CST de 82 possibles événements importants.

Soutien aux missions au Moyen-Orient

Dans la dernière année, le Moyen-Orient a connu la guerre et plusieurs bouleversements. Le COPCC a assuré la liaison à ce chapitre avec d'autres ministères du gouvernement du Canada et a communiqué de l'information sur le conflit se déroulant au Liban, le renversement du régime d'Assad en Syrie et la situation géopolitique générale du Moyen-Orient.

De plus, il a coordonné le soutien du CST en ce qui a trait aux options de vols commerciaux à offrir aux Canadiennes et Canadiens devant évacuer le Liban et s'est préparé à gérer une possible évacuation de non-combattantes et non-combattants en raison du conflit entre Israël et le Hezbollah.

Soutien aux Jeux olympiques de Paris de 2024

Le COPCC a coordonné les efforts de renseignement et de cybersécurité du CST afin d'assurer la sécurité des Jeux olympiques et des Jeux paralympiques qui ont eu lieu à l'été 2024. Il a entre autres assuré la liaison avec le Centre pour la cybersécurité pour offrir des séances d'information efficaces en matière de cybersécurité à des participantes et participants ainsi qu'à des parties prenantes importantes, puis a collaboré avec des partenaires internationaux afin d'échanger de l'information et des postures en soutien à l'événement.

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

Le Centre pour la cybersécurité s'efforce de soutenir l'Ukraine et la Lettonie en offrant des services de cybersécurité depuis 2022, soit depuis que la ministre de la Défense nationale a désigné les cybersystèmes de ces pays comme étant d'importance pour le Canada.

Soutien à l'Ukraine

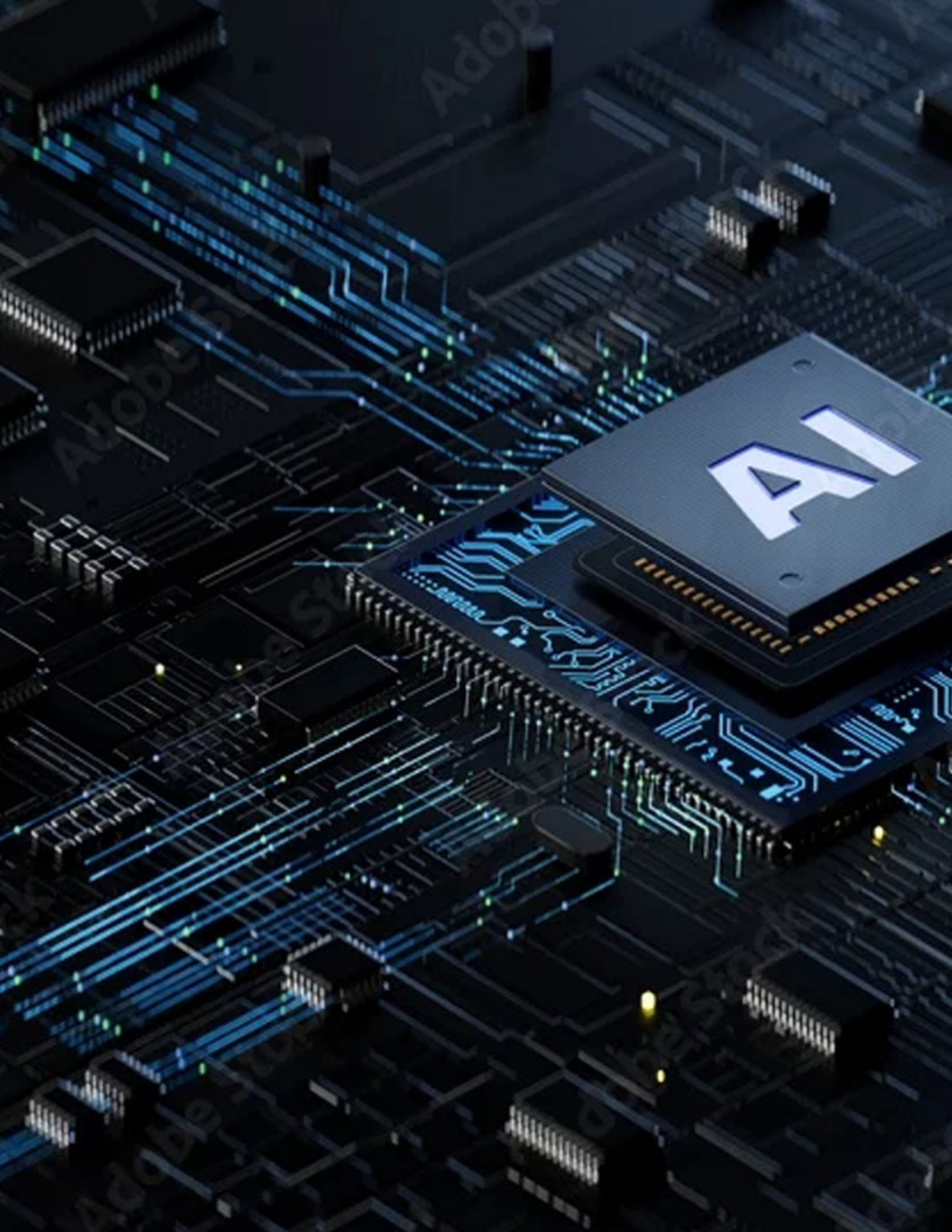
Le CST a continué de tirer parti du volet de son mandat touchant le renseignement étranger pour appuyer la résistance de l'Ukraine à son invasion injustifiable par la Russie, qui est toujours en cours. Dans le cadre de l'opération UNIFIER, le CST a commencé à mettre à la disposition des forces armées ukrainiennes sa plateforme d'analyse des maliciels et de triage des fichiers. Elles disposent donc des mêmes services de détection des maliciels approfondie qui servent à protéger les réseaux du gouvernement du Canada.

En exploitant la même plateforme, les analystes de l'Ukraine et du Canada (ministère de la Défense nationale et CST) peuvent coopérer sur des investigations de fichiers et échanger de l'information précieuse sur les maliciels nouvellement détectés.

Soutien à la Lettonie

Des équipes du Centre pour la cybersécurité ont été déployées en Lettonie 3 fois cette année dans le cadre d'activités concertées avec les FAC (opération REASSURANCE) et avec l'organisme de cybersécurité de la Lettonie, CERT.LV. Parmi les activités, nommons les suivantes :

- 5 semaines d'activités intensives en Lettonie;
- 2 semaines d'activités intensives pour aider une organisation d'infrastructures essentielles du secteur de l'énergie;
- 1 semaine de formation en Lettonie axée sur POLARIS, un outil de simulation avancée en cybersécurité du CST, en collaboration avec des participantes et participants des équipes d'intervention en cas d'urgence informatique de l'OTAN, des FAC et des forces militaires ukrainiennes.


AI

INNOVATION ET ÉVOLUTION DU CST

Le CST est un organisme en constant apprentissage. Ainsi, il recueille, interprète et analyse constamment de l'information et des données. L'innovation et la recherche sont primordiales à la réussite de sa mission. Son personnel s'efforce toujours de rester à l'avant-garde des avancées technologiques, non seulement pour défendre le Canada contre les menaces, mais aussi pour s'assurer de tirer profit de tous les outils disponibles pour réaliser le mandat de l'organisme.

Promotion de l'utilisation responsable de l'intelligence artificielle

L'IA fait partie intégrante des opérations du CST depuis longtemps et fait progresser la mission de l'organisme en favorisant la prestation améliorée et rapide d'informations dans un contexte de menace qui évolue rapidement. Le CST a réalisé de nombreux progrès intéressants en matière d'IA dans la dernière année, dont les suivants :

- la mise en œuvre de la Stratégie en matière d'IA;
- la participation aux efforts du gouvernement du Canada qui visent à élaborer des normes en matière d'IA;
- la réalisation d'activités de sensibilisation pour répondre aux préoccupations au sujet de l'utilisation croissante de l'IA;
- l'exploration de gains d'efficacité en milieu de travail grâce à l'IA.

Stratégie en matière d'intelligence artificielle du CST

Cette année, le CST a mis en œuvre sa Stratégie en matière d'intelligence artificielle[12]. Ce document fondateur est axé sur l'innovation intentionnelle, sur la prestation d'outils aux membres du personnel et sur l'élargissement des partenariats avec l'industrie, le milieu universitaire et des alliés internationaux.

La Stratégie en matière d'IA du CST repose sur un cadre 3+4+1. L'objectif du CST se définit par 3 principaux engagements : innover et intégrer l'IA pour assurer la sécurité nationale, promouvoir une IA responsable et sécurisée, et comprendre et contrer la menace liée à l'utilisation malveillante de l'IA. Les efforts de l'organisme reposent sur 4 fondements, à savoir les personnes, les partenariats, les principes d'éthique et l'infrastructure. C'est 1 effort unifié en matière d'IA qui orientera sa mise en œuvre, favorisant l'adoption d'une approche uniforme à mesure que le CST adaptera ses méthodes de travail pour atteindre les objectifs fixés par la stratégie.

La Stratégie en matière d'IA du CST fait en sorte que l'utilisation de l'IA par les membres du personnel est responsable et qu'elles et ils acquièrent un ensemble de compétences uniques au sein du gouvernement fédéral. Elle rejoint également les priorités pangouvernementales du Canada, comme celles de l'Institut canadien de la sécurité de l'intelligence artificielle (ICSIA) et de la Stratégie en matière d'IA pour la fonction publique fédérale.

Le CST s'engage à établir et à utiliser des capacités d'IA de façon éthique, responsable et sécurisée, en tenant compte des risques liés à l'IA et en tirant profit au maximum de ses avantages.

Utilisation de la science des données et de l'IA pour favoriser l'innovation à l'interne

Le CST organise un atelier annuel auquel participent des personnes du Canada et des pays membres de la collectivité des cinq dans le but de résoudre des problèmes complexes auxquels fait face la collectivité du SIGINT. Cette année, de nombreuses équipes ont misé sur l'IA et la science des données pour créer des outils capables d'analyser des ensembles de données très volumineux afin d'automatiser des tâches quotidiennes fastidieuses et de renforcer les capacités d'analyse.

À la suite de l'atelier de cette année, le CST a mis en place un prototype de génération améliorée par récupération d'information (GARI) pour le matériel de formation destiné aux analystes afin d'améliorer les processus analytiques et l'efficacité. Ce prototype a révolutionné l'expérience d'apprentissage des analystes, en leur offrant un accès instantané à l'information voulue et en accélérant le perfectionnement de leurs compétences. Parmi les autres résultats intéressants de l'atelier, nommons les suivants :

- appliquer des techniques de science des données pour explorer des ensembles de données et révéler de l'information importante sur les intentions d'auteurs de cybermenace malveillants;
- mettre en œuvre la recherche sémantique et la modélisation de sujets pour assurer un tri rapide des données afin de pouvoir cerner rapidement le renseignement critique et le prioriser, améliorant ainsi la production de rapports.

Contribution aux efforts du gouvernement du Canada dans le domaine de l'IA

En tant que leader en matière de recherche et d'innovation en IA, le CST contribue à différents efforts du gouvernement du Canada pour évaluer les risques liés à l'IA et les mesures d'atténuation connexes, de sorte à garantir une mise en œuvre de l'IA robuste et sécurisée. De 2024 à 2025, il a entre autres fait ce qui suit :

- être membre du programme de modernisation du versement des prestations d'EDSC;
- participer au Groupe de travail sur la gouvernance en matière d'IA de SPC;
- fournir de l'orientation stratégique sur les plans, les priorités et les projets de recherche pour l'ICSIA.

Institut canadien de la sécurité de l'intelligence artificielle

Mis sur pied en novembre 2024, l'ICSIA est une initiative pilotée par Innovation, Sciences et Développement économique Canada afin de favoriser le développement et la mise en œuvre sûrs et responsables de l'IA. L'ICSIA se consacre à la compréhension des risques liés à l'IA, en fournissant des outils pour atténuer ces risques et en s'assurant de l'adoption sûre et fiable de technologies d'IA.

Activités de sensibilisation relatives à l'intelligence artificielle

Pour répondre aux préoccupations croissantes concernant les menaces liées à l'IA, le CST et le Centre pour la cybersécurité coopèrent activement avec différentes parties prenantes. Cette année, l'organisme a donné des présentations à différents groupes, dont les suivants :

- la Conférence des gouvernements fédéral, provinciaux et territoriaux;
- Alberta Energy;
- BHP Saskatoon;
- Élections Canada;
- les cadres supérieures et supérieurs du gouvernement du Canada.

Ces présentations ont porté sur des sujets tels que les menaces liées à l'IA, les stratégies d'atténuation, les facteurs relatifs à la mise en œuvre, l'hameçonnage, les maliciels et l'hypertrucage.

Formation sur l'IA à l'intention des fonctionnaires

Cette année, le Carrefour de l'apprentissage du Centre pour la cybersécurité a mis en place 2 nouveaux cours portant sur des directives du gouvernement du Canada liées à l'utilisation de l'IA générative, à l'exploitation sûre de l'IA générative au travail de même qu'aux préoccupations éthiques et aux limites de l'IA générative.

Mise à l'essai de Microsoft 365 Copilot

À l'instar d'autres milieux de travail au Canada, le CST explore la manière dont l'IA peut améliorer l'efficacité de ses équipes et les aider. Cette année, dans le cadre du programme d'accès anticipé de Microsoft, 300 utilisatrices et utilisateurs du CST ont mis à l'essai Microsoft Copilot et l'assistant personnel. Parmi les utilisatrices et utilisateurs de Pilot, on comptait des cadres et des membres du personnel de niveau opérationnel.

Le CST a été en mesure d'adapter l'outil selon ses fonctions particulières, en préservant son environnement sécurisé et en tenant compte du contexte lié au besoin de connaître, tout en continuant de protéger l'information sensible. Grâce à ce projet pilote, le personnel du CST a pu mettre à l'essai différentes façons d'appliquer l'IA en toute sécurité afin d'appuyer les activités de travail au sein de l'organisme.

Amélioration de l'infrastructure et des services classifiés

Le CST est un organisme de sécurité et de renseignement et doit donc effectuer la majorité de ses activités à l'aide de réseaux et d'outils classifiés. De 2024 à 2025, le CST s'est consacré à l'innovation et à l'échange d'information souple avec des partenaires afin de réaliser des progrès intéressants dans ces domaines.

Projet SIGINT Canada

Cette année, le CST a entrepris une initiative sans précédent en ce qui a trait à l'intendance des données et de l'information. Il s'agit du projet SIGINT Canada. Ce projet a transformé la collecte, la gestion et l'échange sécurisé de données sensibles dans l'infrastructure de sécurité nationale du Canada.

SIGINT Canada a permis de moderniser l'infrastructure de TI et de faciliter l'échange de données et de services critiques entre le CST et CAFCYBERCOM. En intégrant des technologies avancées, SIGINT Canada a permis d'améliorer l'efficacité, la sécurité et l'interopérabilité des systèmes d'échange de données critiques au sein des collectivités civile et militaire SIGINT du pays.

Parmi les réalisations importantes liées au projet SIGINT Canada, notons les suivantes :

- amélioration de l'échange de données : mise en œuvre d'une infrastructure normalisée au sein de différents organismes pour que l'accès aux données et aux services critiques soit sûr et offert en temps réel à partir de plusieurs points terminaux, améliorant par le fait même la collaboration et les prises de décisions;
- efficacité opérationnelle : introduction de nouveaux systèmes et processus pour simplifier la gestion des données, ce qui a facilité et accéléré les prises de décisions;
- renforcement de la sécurité : mise en place de mesures de cybersécurité avancées pour que les données sensibles soient communiquées, protégées et gérées de façon sécurisée dans tous les réseaux de sécurité élevée et par tous les partenaires internationaux;
- amélioration de l'interopérabilité : création d'un modèle de prestation de services unifié qui permet l'intégration d'un volume accru de données et la collaboration entre les organismes, ce qui facilite les communications et l'échange de données entre les entités du gouvernement et les partenaires internationaux.

Expansion du Réseau canadien Très secret

Les ministères fédéraux ont de plus en plus besoin d'accéder à du renseignement pour remplir leur mandat respectif et mener leurs activités opérationnelles. Par conséquent, le CST a observé une croissance soutenue des services liés au réseau Très secret ainsi qu'une demande accrue pour ces services.

Le CST gère le RCTS, qui est le réseau de TI sécurisé qui permet la collaboration et la communication au niveau Très secret. Cette année, le CST a soutenu des expansions de site importantes pour la clientèle existante du RCTS, dont l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, le Bureau du Conseil privé, le ministère de la Justice Canada et la GRC, ce qui a accru de 20 % le nombre de points terminaux déployés.

Dans la prochaine année, le CST intégrera 3 nouveaux ministères gouvernementaux au RCTS, à savoir :

- Environnement et Changement climatique Canada;
- Service des poursuites pénales du Canada;
- Bureau du commissaire aux élections fédérales.

Le CST a aussi déployé un nombre important de ses terminaux Très secret à CAFCYBERCOM et de ses stations-satellites au Canada, de même qu'en soutien aux opérations militaires de déploiement.

Améliorations de systèmes classifiés de base importants

Cette année, un système qui fournit au Centre pour la cybersécurité des indicateurs sur l'infrastructure d'une cybermenace en temps quasi réel – dont la détection s'effectue grâce à des systèmes SIGINT du CST – a fait l'objet d'améliorations importantes. Grâce à ce système, les outils de cyberdéfense du gouvernement du Canada disposent de données hautement fiables pour perturber de manière dynamique des activités malveillantes.

Conformément au mandat du CST, un système similaire a été mis en place cette année. Il permet de détecter, par l'intermédiaire de systèmes SIGINT du CST, des Canadiennes et Canadiens qui ont été victimes de cybermenaces étrangères et de signaler ces activités au Centre pour la cybersécurité.

Grâce à ces systèmes, le Centre pour la cybersécurité reçoit de l'information exploitable acquise dans le cadre d'opérations de renseignement étranger du CST. En retour, les réseaux canadiens sont protégés et les entités canadiennes sont rapidement avisées de ces cybermenaces, ce qui permet d'atténuer les conséquences des cybermenaces étrangères.

Promotion de l'innovation et des partenariats par l'intermédiaire de sourçage libre

Dans la dernière année, le Centre pour la cybersécurité a poursuivi la réalisation de projets de source ouverte afin de soutenir la collectivité de cyberdéfense élargie. Le gouvernement du Canada, des responsables de systèmes d'importance et des organisations privées ont continué de tirer profit des outils de source ouverte du CST et de les mettre en œuvre afin de renforcer leurs infrastructures de cybersécurité.

L'engagement du CST concernant le sourçage libre a favorisé l'établissement de nouveaux partenariats, ce qui a permis d'améliorer les outils développés par l'organisme et d'accélérer les progrès accomplis sur le plan de la détection et du tri de maliciels. Le Centre pour la cybersécurité demeure en première ligne de la collectivité et se réjouit à l'idée de diffuser d'autres outils de source ouverte dans la prochaine année.

Recherche et renforcement des partenariats de recherche

La Direction générale de la recherche du CST établit des partenariats avec des groupes du CST et d'ailleurs pour stimuler l'innovation et développer de nouvelles capacités efficaces qui contribuent à la mission du CST.

Cette année, la Direction générale de la recherche a mis en œuvre une nouvelle vision et un plan stratégique pour guider ses activités de 2025 à 2027. Le plan stratégique est axé sur les fondements mathématiques de la cryptographie, sur les fondements de l'IA et de l'apprentissage automatique, sur l'entraînement, l'adaptation et la sécurité des modèles, et sur la recherche de vulnérabilités. La vision présente 5 défis principaux qui peuvent être surmontés par l'intermédiaire de la recherche. Les voici :

- améliorer constamment l'accès du CST aux systèmes et aux données;
- accroître la capacité du CST à traiter et à raffiner d'énormes quantités d'informations;
- améliorer l'efficience et l'efficacité de l'analyse des données et de l'information;
- protéger la sécurité et l'intégrité des systèmes et de l'information;
- conserver un avantage scientifique et technologique sur les adversaires du Canada.

Dans l'optique de réaliser sa mission, le CST met à contribution des outils et établit des partenariats de recherche innovants pour élargir les modèles et tirer parti du talent à sa disposition.

Institut Tutte pour les mathématiques et le calcul

Au cours de la dernière année, l'Institut Tutte pour les mathématiques et le calcul (ITMC)[13] a continué de développer des théories fondamentales, des techniques novatrices et des outils efficaces dans ses 2 principaux domaines d'étude : la cryptographie et la science des données.

Si possible, l'ITMC rend ses outils accessibles publiquement, publie ses résultats dans des revues spécialisées et fait des présentations lors de conférences. Cette année, la contribution de l'ITMC à la communauté de recherche universitaire a consisté à :

- publier 12 articles de revues;
- produire 5 versions de logiciels contenant du nouveau code ou modifiant du code;
- organiser 3 conférences;
- réviser les travaux de 1 congrès;
- participer à 1 entretien en baladodiffusion et à de multiples discussions en groupe;
- participer à 3 discussions et à 7 présentations lors de conférences externes;
- occuper des places au Conseil d'administration de la Société mathématique du Canada et des comités.

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

Favoriser des partenariats forts

L'ITMC s'engage à favoriser des partenariats forts avec la communauté scientifique du Canada. L'ITMC offre un soutien financier pour la tenue de conférences dans les domaines des mathématiques et de l'informatique proches de ses intérêts de recherche, en plus d'offrir un soutien financier aux événements organisés par des universités locales.

Cette année, l'ITMC a offert un soutien financier dans le cadre de 8 conférences dans les domaines des mathématiques et de l'informatique et de 8 événements organisés par des universités locales.

Centre de recherche sur les vulnérabilités

Le Centre de recherche sur les vulnérabilités (CRV)[14] du CST poursuit ses efforts de recherche appliquée sur les vulnérabilités à l'appui de son mandat et des mandats de ses partenaires fédéraux. Au cours de la dernière année, il a découvert de nombreuses vulnérabilités et a divulgué, de façon responsable, 10 vulnérabilités aux fournisseurs touchés.

Cette année, le CRV a établi de premiers partenariats avec l'Institut universitaire de technologie de l'Ontario et l'Université de Toronto. Le CRV poursuit son partenariat avec l'Université Concordia dans l'optique d'améliorer ses outils de recherche sur les vulnérabilités.

GeekWeek 9

Le Centre pour la cybersécurité a organisé pour une neuvième année consécutive l'atelier GeekWeek[15], un atelier annuel non classifié qui réunit des intervenantes et intervenants clés du domaine de la cybersécurité pour produire des solutions à des problèmes cruciaux auxquels est confrontée l'industrie. Le thème de cette année était **Animer la cybersécurité**[16]. Le Centre pour la cybersécurité était heureux d'accueillir des participantes et participants de la fonction publique, du secteur privé, des infrastructures essentielles et des partenaires internationaux.

Communauté de recherche du CST et du CRSNG sur les systèmes d'intelligence artificielle robustes, sûrs et sécurisés

Le CST poursuit également son partenariat avec le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) pour financer les communautés de recherche afin qu'elles puissent mener des recherches non classifiées sur les technologies de pointe dans des domaines d'importance stratégique pour le CST et le gouvernement du Canada.

Cette année voit la création de la communauté de recherche du CST et du CRSNG sur les systèmes d'IA robustes, sûrs et sécurisés dans le cadre du projet sur une approche de bout en bout pour rendre les systèmes d'IA sûrs et sécurisés. Sous la direction de l'Université de Toronto, ce projet comprend 19 copostulantes et copostulants provenant de 5 universités canadiennes. Le groupe élaborera des solutions aux problèmes liés à l'IA et en fera la preuve, notamment :

- en créant des méthodes pour entraîner des modèles d'IA dans des cas où des données fiables et étiquetées ne sont pas disponibles et s'appuient sur des modèles de base externes, non fiables et préentraînés;
- en élaborant des techniques pour s'assurer que les modèles d'IA sont robustes, justes et intelligibles;
- en établissant des lignes directrices pour utiliser l'IA afin d'assurer la conformité réglementaire et de soutenir le processus d'audit.

C'est la première de quatre communautés créées dans le cadre des subventions CRSNG-CST à l'appui des communautés de recherche[17].

LE CST HABILITE ET JOINT LES CANADIENNES ET CANADIENS

Le CST offre de la formation en cybersécurité et publie des avis clairs permettant aux Canadiennes et aux Canadiens de faire des choix éclairés et responsables. Le CST joint la population au moyen de ses activités de sensibilisation, des médias sociaux et de campagnes publicitaires innovantes afin de lui apprendre comment interpréter l'environnement de cybersécurité actuel.

De nouvelles manières de sensibiliser les Canadiennes et Canadiens

L'apprentissage et la formation en ligne

Le Carrefour de l'apprentissage du Centre pour la cybersécurité[18] est la source de formation en cybersécurité et en sécurité des communications. Les services sont accessibles aux 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, les inscriptions à des cours du Carrefour de l'apprentissage se sont élevées à 11 895.

Collaboration avec ChatterHigh

Cette année, le Carrefour de l'apprentissage a eu le plaisir de collaborer avec ChatterHigh dans le cadre d'un cours adressé aux élèves de tous âges, intitulé Assurer la sécurité du Canada! Découvrir les carrières dans le domaine de la cybersécurité. Accessible par l'entremise de ChatterHigh, le cours est offert gratuitement aux enseignantes et enseignants ainsi qu'aux élèves.

Découvrez la cybersécurité

Le Carrefour de l'apprentissage a conçu en collaboration avec l'École de la fonction publique du Canada le cours Découvrez la cybersécurité. Dans ce cours, les participantes et participants apprennent à reconnaître les menaces et à se protéger, ainsi qu'à protéger leurs renseignements numériques et les systèmes qu'ils utilisent. Les fonctionnaires de tous les échelons et le grand public peuvent suivre ce cours gratuitement.

Campagne Pensez cybersécurité

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

Pensez cybersécurité a produit plus de 46 ressources cette année, de sorte à accroître son catalogue de conseils sur les sujets liés à la cybersécurité, notamment des façons suivantes :

- enrichir le contenu concernant les escroqueries amoureuses dans un jeu-questionnaire pour découvrir comment utiliser son langage amoureux pour se protéger en ligne[19] et une publication de blogue décrivant les tactiques d'escroquerie dont il faut se méfier[20];
- ajouter de nouvelles ressources sur les fraudes par virement électronique[21];
- fournir de nouveaux renseignements sur les mesures de protection liées aux méthodes de paiement[22], en partenariat avec le Centre antifraude du Canada;
- créer une vidéo montrant comment signaler un message texte frauduleux[23] sur leur appareil.

On a également ajouté des ressources sur les nouvelles manières dont les cybercriminelles et cybercriminels utilisent l'IA pour tromper les gens, ainsi que des astuces pratiques pour se protéger :

- La prochaine génération : savoir reconnaître les contenus générés à l'aide de l'intelligence artificielle[24]
- Voici 9 façons de repérer du contenu créé à l'aide de l'intelligence artificielle[25]
- Des cybermenaces encore plus sophistiquées grâce à l'IA[26]
- Pourquoi vous ne devriez jamais partager vos informations personnelles avec l'IA[27]

Pensez cybersécurité pour les publics autochtones

Afin de mieux servir les publics inuits, métis et des Premières Nations au Canada, le CST a continué d'élargir ses activités de sensibilisation en offrant des ressources pertinentes sur le plan culturel. Comme l'année dernière, Pensez cybersécurité a fait traduire ses infographies les plus téléchargées en ojibwé, en cri, en inuktitut et en micmac.

Cette année marque également le lancement d'une stratégie de sensibilisation structurée par l'entremise de Indigenous Link, une firme de communications autochtone de confiance qui a une forte présence dans les communautés rurales, urbaines et éloignées. Le partenariat comprend :

- la distribution d'affiches sur les babillards des communautés;
- des campagnes ciblées par courriel à plus de 22 000 abonnées et abonnés;
- la création d'une page d'accueil présentant le matériel traduit[28].

Ces efforts visaient à accroître la sensibilisation et la confiance au sein des communautés autochtones et à assurer un accès équitable à l'information concernant la cybersécurité.

Pensez cybersécurité pour les petites entreprises

Aucune entreprise, même la plus petite, n'est à l'abri des cybercriminelles et cybercriminels. Cependant, il n'est pas toujours réaliste pour un grand nombre de petites entreprises d'investir dans des solutions de cybersécurité coûteuses ou complexes. Cette année, le CST a ajouté une série de ressources à l'intention des petites entreprises[29], y compris un modèle de plan d'intervention en cas d'incident et des sujets d'apprentissage pour aider les propriétaires d'entreprise à fournir la bonne formation à leur personnel.

Mois de sensibilisation à la cybersécurité

En octobre, le CST dirige le Mois de la sensibilisation à la cybersécurité[30] (Mois de la cybersécurité) au Canada. Le thème de cette année était Génération Pensez cybersécurité : parce que la sécurité en ligne n'a pas d'âge[31]. La campagne encourageait les Canadiennes et Canadiens de partout à prendre des mesures

simples et importantes pour se protéger en ligne. La campagne a suscité des discussions à l'échelle du pays grâce à des vidéos sympathiques, à des refrains publicitaires accrocheurs et à du contenu multiplateforme.

Des partenaires nationaux des secteurs public et privé ont contribué à produire et à transmettre le contenu, et plus de 300 organisations ont repris le contenu du Mois de la cybersécurité pour entrer en contact avec leur public. La portée et l'incidence de la campagne de cette année sont source de fierté. Au cours du Mois de la cybersécurité, le contenu de la campagne :

- a été vu plus de 293 000 fois;
- a été partagé par 410 comptes de médias sociaux uniques;
- a entraîné 26 millions d'expositions et a joint 3,8 millions d'utilisatrices et utilisateurs;
- a entraîné 73 801 visites sur les sites Web, soit une augmentation par rapport aux 63 338 visites enregistrées l'année précédente.

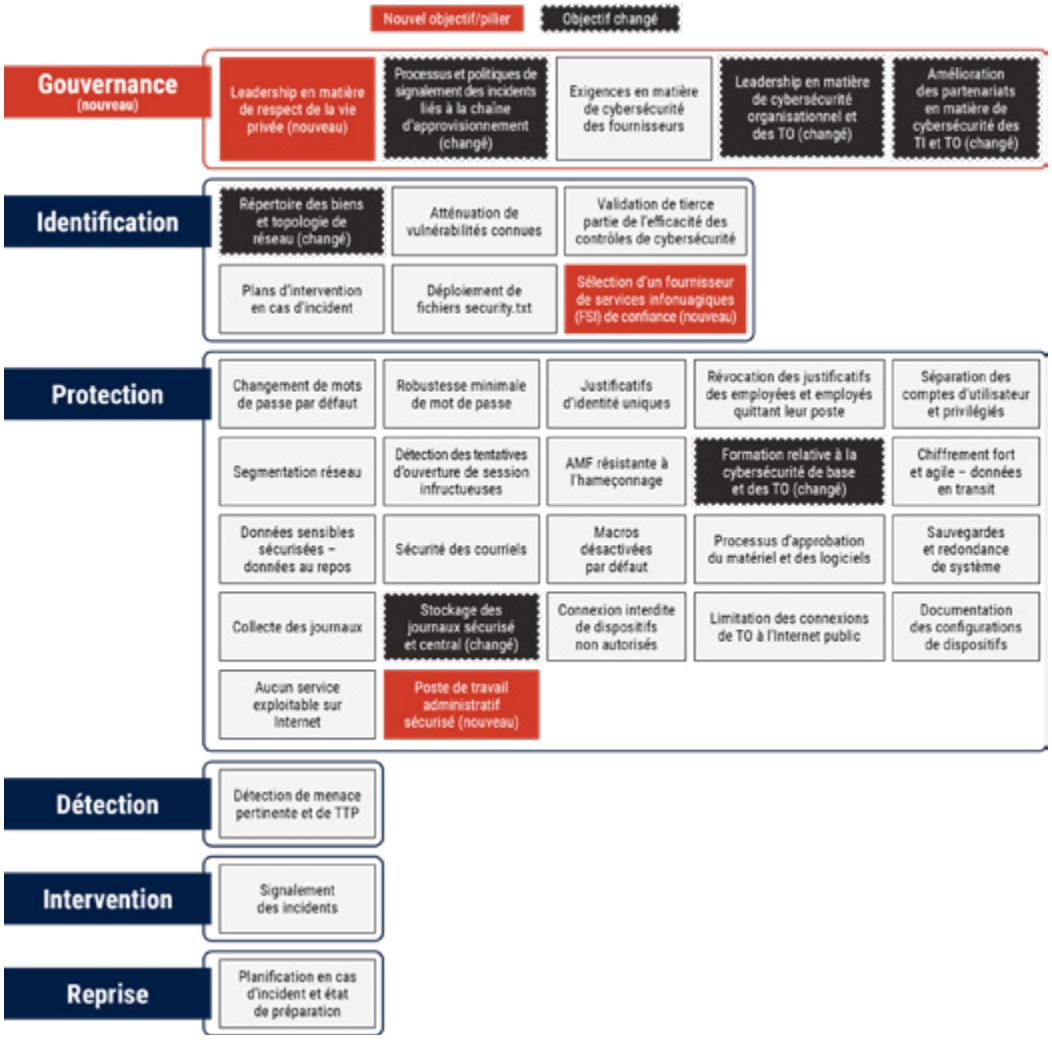
Objectifs relatifs à l'état de préparation en matière de cybersécurité

Cette année a vu le lancement des objectifs relatifs à l'état de préparation en matière de cybersécurité[32] (OEPC), des objectifs réalistes et atteignables pour renforcer la cybersécurité des organisations canadiennes, en particulier celles des infrastructures essentielles.

Les OEPC décrivent les principaux objectifs et les étapes importantes que les organisations peuvent suivre pour améliorer la posture de cybersécurité des systèmes de technologie de l'information et de technologie opérationnelle dans le contexte en évolution des cybermenaces de plus en plus complexes.

Constitués de 36 objectifs fondamentaux et volontaires, les OEPC consolident les avis et les conseils de base du Centre pour la cybersécurité sur la prévention, la détection et l'intervention concernant les menaces à la cybersécurité.

Le Centre pour la cybersécurité a déjà offert des séances d'information sur les OEPC à plus de 1 000 partenaires de différents secteurs clés, notamment l'énergie, les finances et le transport.



Documents d'orientation

Un autre important service que proposent le CST et le Centre pour la cybersécurité pour renseigner le public canadien est la publication de conseils concernant les menaces, les techniques d'atténuation et d'autres sujets sur la page Web des conseils sur la cybersécurité[33]. Ces publications s'adressent à des auditoires divers, comme le grand public, les praticiennes et praticiens des TI, les institutions démocratiques fédérales et provinciales, les cadres du secteur privé et les alliés.

Il y a eu 29 publications de conseils en matière de cybersécurité cette année, ainsi que 20 autres publications conjointes avec les partenaires de la collectivité des cinq.

Dispositifs d'accès

Cette année, le Centre pour la cybersécurité a publié des conseils sur les facteurs relatifs à la sécurité à considérer pour les dispositifs d'accès[34] dans le cadre d'une campagne d'orientation de la collectivité des cinq. Pour une première fois, le Centre pour la cybersécurité a rédigé des conseils appuyés conjointement par ses partenaires de la collectivité des cinq.

Étendre les activités de sensibilisation

Même s'il peut paraître contre-intuitif qu'un organisme de renseignement mène des activités de sensibilisation et de mobilisation, au CST, on reconnaît la valeur de travailler avec la communauté élargie. La cybersécurité, c'est un sport d'équipe. Rien ne se fait en vase clos.

Cette année, le CST et le Centre pour la cybersécurité ont continué de mener des activités de sensibilisation communautaire, de s'associer avec d'autres ministères et d'établir des relations fortes avec les médias.

Sensibilisation communautaire

Le programme d'approche communautaire en pleine croissance du CST, qui comprend le parrainage de programmes sans but lucratif, la participation de bénévoles à des ateliers à l'intention d'élèves du primaire et du secondaire, est conçu de sorte à encourager le perfectionnement des compétences dans la science, la technologie, l'ingénierie et les mathématiques (STIM) et l'intérêt envers les carrières connexes aux STIM. Le programme a pour but de présenter des occasions en STIM aux groupes qui sont confrontés à des obstacles ou qui sont sous-représentés dans le domaine. Voici certains programmes et événements que le CST a soutenus cette année :

- Hackergal
- CyberSci
- BlackBoys Code
- Raspberry Pi

Cette année, le Centre pour la cybersécurité a également organisé le championnat national de CyberSci pour plus de 100 élèves. Il s'agissait de la troisième année où le CST a parrainé et encadré l'équipe canadienne, qui s'est classée pour une troisième année consécutive en première place dans la catégorie des pays invités lors du European Cybersecurity Challenge 2024.

Sensibiliser les communautés autochtones à la cybersécurité

Le Centre pour la cybersécurité collabore avec des communautés autochtones pour les sensibiliser davantage à la cybersécurité et assurer leur résilience. Ces efforts permettent de renforcer la sécurité numérique et d'appuyer les approches communautaires liées à la cybersécurité en favorisant les pratiques exemplaires, une cyberhygiène robuste et l'établissement de capacités locales de soutien.

En mars 2025, le programme Manitoba First Nations SchoolNet a organisé un atelier de cybersécurité à Churchill, au Manitoba. L'atelier a réuni plus de 30 jeunes Autochtones de 18 à 24 ans qui représentaient les communautés des Premières Nations de partout dans la province. Les participantes et participants étaient des stagiaires qui appuyaient leur communauté dans le cadre d'initiatives liées aux TI, à la connectivité et au numérique.

Le Centre pour la cybersécurité a organisé une séance pratique axée sur la cybersécurité et la sensibilisation. L'initiative avait pour but de doter les jeunes de compétences pratiques en cybersécurité afin de renforcer la résilience numérique de leurs communautés, tout en faisant progresser la connectivité et l'équité numérique dans les communautés des Premières Nations du Manitoba.

Engagements auprès de l'ensemble du gouvernement du Canada

En plus des engagements opérationnels, l'organisme a pris part cette année à la coordination de services et à l'amélioration de la cyberrésilience auprès de plus de 100 organismes fédéraux. Ces efforts ont entraîné :

- 25 séances d'information individuelles auprès d'organismes fédéraux;
- des séances d'information permanentes tous les deux mois ouvertes à toutes et tous les cadres supérieurs et à toutes les équipes de TI et de cybersécurité du gouvernement du Canada.

Le Centre pour la cybersécurité a lancé un appel à la communauté d'intérêts à l'échelle du gouvernement du Canada pour établir une plateforme d'échange des connaissances entre le Centre pour la cybersécurité et les professionnelles et professionnels des TI et de la cybersécurité au gouvernement du Canada. Cette initiative appuie les stratégies de cybersécurité au sein du gouvernement en fournissant des informations sur les nouvelles cybermenaces visant le gouvernement du Canada, en communiquant les principales mises à jour concernant les initiatives du Centre pour la cybersécurité et en soulignant les programmes essentiels qui améliorent la posture de cybersécurité du gouvernement.

Afin de mieux faire connaître ses services au sein du gouvernement du Canada, le Centre pour la cybersécurité a également publié cette année sa toute première brochure. Celle-ci a été distribuée partout au gouvernement du Canada et comprenait des explications sur les services et les coordonnées du Centre pour la cybersécurité.

Présentation sur la cybersécurité pour les journalistes canadiennes et canadiens

Cette année a eu lieu une présentation sur la cybersécurité à l'intention des journalistes canadiennes et canadiens. Cette présentation en personne de nature non classifiée coïncidait avec la publication Atténuation des menaces avec des ressources limitées : Conseils à l'intention de la société civile[35], une publication conjointe du CST et de partenaires internationaux qui informait la société civile des menaces réelles et croissantes visant sa cybersécurité. Des médias accrédités de partout au pays étaient représentés.

L'objectif n'était pas de donner du contenu aux fins de couverture médiatique, mais bien d'informer les personnes de l'audience des mesures à prendre pour améliorer leur cybersécurité personnelle et professionnelle. Au total, 15 journalistes ont assisté à la présentation offerte dans les deux langues officielles.

Projet pilote de présence nationale à Montréal

En août 2024, le Centre pour la cybersécurité a ouvert un bureau à Montréal, le premier à l'extérieur de la région de la capitale nationale. Ce bureau permettra de collaborer étroitement avec des partenaires dans les domaines de la cybersécurité et des infrastructures essentielles de la région de Montréal, et ce, afin d'offrir des programmes et des services, de tisser des relations et de faciliter l'échange d'information. En plus de favoriser les partenariats avec les infrastructures essentielles et d'autres importantes parties prenantes, ce projet pilote permettra d'évaluer les répercussions et les avantages d'agrandir la présence nationale du CST, y compris la possibilité d'ouvrir des bureaux à d'autres endroits au Canada.

LE CST CROÎT ET APPREND

Le CST adopte une approche axée sur l'embauche de personnes talentueuses, la promotion de ces personnes et l'amplification des talents, en vue de renforcer son effectif et d'assurer la disponibilité du soutien nécessaire aux membres du personnel. Afin de mener à bien notre mission et notre travail, il faut un effectif robuste, diversifié et sain. Cette année, l'effectif total du CST à atteint 3 841 employées et employés, une augmentation de 5,9 % comparativement à l'année dernière. Cette croissance nous permet de continuer à mener à bien notre mission, en plus d'offrir du renseignement critique et des services de cybersécurité au Canada.

L'équité, la diversité, l'inclusion et l'accessibilité (EDIA) sont des principes fondamentaux dans tout ce que nous faisons. Notre effectif moderne est composé d'ingénieures, ingénieurs, expertes et experts en science des données, spécialistes de la cybersécurité, analystes du renseignement, conseillères et conseillers en politiques, gestionnaires de projets, conseillères et conseillers, comptables, avocates et avocats, spécialistes des communications, spécialistes des ressources humaines et beaucoup plus encore. La diversité d'expérience, de compétences, de talents ou de motivations fait notre force. Le CST est fier des réalisations accomplies cette année pour croître et apprendre en tant qu'organisme inclusif. Voici quelques faits saillants importants :

- intégrer l'EDIA dans les évaluations de renseignement et dans les processus de promotion en fonction du mérite, de sorte à indiquer que l'inclusivité n'est pas seulement une valeur, mais une priorité mesurable pour tout le personnel;
- mettre sur pied une division axée sur l'EDIA pour souligner l'approche stratégique de l'intégration de l'EDIA dans la planification et la croissance à long terme;
- accorder plus de 5 % des contrats d'approvisionnement à des entreprises autochtones, afin de réaliser des efforts proactifs pour faire progresser la réconciliation économique et les partenariats autochtones;
- se procurer et afficher des œuvres d'art d'artistes autochtones pour que les employées et employés autochtones se sentent accueillis dans l'organisme et exposer tout le personnel du CST à la culture autochtone;
- intégrer des fonctions visant à encourager le respect et l'inclusion dans les interactions quotidiennes, comme un outil de prononciation des noms dans MS Teams;
- accueillir une diversité de conférencières et conférenciers invités inspirants dans le cadre d'événements et de célébrations.

Grâce à ces efforts, le CST crée un environnement inclusif pour appuyer son effectif, tandis que celui-ci apporte des contributions à la fois importantes et novatrices dans le cadre de la mission.

Le CST est parmi les meilleurs employeurs

Nous pensons que notre organisme, notre environnement de travail et notre équipe sont fantastiques, et d'autres aussi! Cette année encore, le CST a été nommé l'un des meilleurs employeurs pour les jeunes au Canada. Il reçoit fièrement cette reconnaissance chaque année depuis 2017. Le CST a également été nommé un des meilleurs employeurs de la région de la capitale nationale pour une 10e année.

Améliorer les activités d'embauche, de recrutement et de sensibilisation

L'équipe de Prospection de candidates et candidats a participé à 178 événements partout au Canada cette année, notamment des salons professionnels, des marathons de programmation, des séances d'information, des conférences, des webinaires et des événements de réseautage.

Parmi les activités de sensibilisation, 24 % d'entre elles étaient axées sur l'EDIA et les 4 groupes concernés par l'équité en matière d'emploi. Nous avons veillé à ce que les spécialistes en la matière internes à ces événements de recrutement représentaient les groupes concernés. Ces efforts ont permis de diversifier l'effectif, notamment en dépassant la disponibilité au sein de la population active pour 2 des 4 groupes désignés (personnes ayant un handicap et Autochtones).

Le CST a également organisé 2 événements de recrutement internes pour les femmes et les personnes non binaires étudiant dans des programmes de STIM au Canada.

Spécialiste en inclusion agréée

Cette année, le CST a embauché une spécialiste en inclusion agréée pour veiller à ce que tous les éléments et les documents de communications externes liés au recrutement soient examinés en fonction de l'Analyse comparative entre les sexes Plus (ACS Plus) et favorisent l'équité et l'accessibilité. Le résultat a été le lancement d'initiatives comme des espaces de stationnements réservés aux personnes enceintes.

Navigatrice de carrière autochtone

Le CST était heureux d'accueillir sa première navigatrice de carrière autochtone cette année. Cette personne travaille avec les employées, employés, candidates et candidats autochtones pour les aider à cheminer dans leur carrière et à établir des objectifs professionnels à atteindre. Elle travaille également avec les gestionnaires pour veiller à ce qu'on tienne compte des employées et employés autochtones dans toutes les décisions d'embauche et de dotation, y compris les promotions et les occasions de mentorat.

Programme de parrainage pour les employées et employés racisés et autochtones

En 2023, le CST a lancé un programme de parrainage pour les employées et employés racisés et autochtones, qui a aidé 90 % des participantes et participants à mériter des occasions de perfectionnement professionnel. Cette année, le CST a relancé le programme et l'a élargi pour inclure les personnes ayant un handicap.

La nouvelle édition du programme a presque doublé le nombre de protégées et protégés, à différentes étapes de leur carrière, par rapport au programme pilote original. Par exemple, 48 % des participantes et participants signalaient se trouver au début de leur carrière, tandis que 26 % se disaient plus avancés dans leur parcours. Pour ce qui est de l'auto-déclaration :

- 15 % s'auto-identifiaient comme une personne neuroatypique ou ayant un handicap;
- 11 % s'auto-identifiaient comme une personne autochtone;
- 18 % s'auto-identifiaient comme une personne noire;
- 56 % s'auto-identifiaient comme une personne racisée.

Mises à jour du programme de sécurité

La sécurité est primordiale dans les opérations du CST. Il est donc important que les processus et les politiques de sécurité tiennent compte des valeurs et des priorités de l'organisme. Au cours de l'année, l'équipe responsable de la sécurité a collaboré étroitement avec les partenaires internes pour améliorer l'inclusivité et la transparence des processus de sécurité du CST, tout en assurant leur intégrité. Les consultations ont donné des résultats encourageants :

- Le processus d'entrevue de sécurité a été modifié pour améliorer l'inclusivité.
- Le questionnaire de filtrage de sécurité a été examiné en fonction de l'ACS Plus pour cerner et éliminer les éléments biaisés, de sorte à garantir un accès égal et un traitement juste pour tous les groupes.
- Les affiches de poste en sécurité ont été examinées, et on a accru la diversité des équipes chargées de la sécurité pour favoriser des processus d'embauche équitables et éliminer les obstacles systémiques.

Par ailleurs, cette année, le CST a terminé de participer à l'examen par l'OSSNR du programme de polygraphie. Le CST continuera d'adopter de nouvelles pratiques et des pratiques améliorées pour renforcer ses processus de sécurité et en assurer la robustesse, tout en protégeant la vie privée des candidates et candidats.

L'inclusivité dans toutes les activités

La diversité et l'inclusion sont à la base de toute étape des processus au CST, du recrutement à l'élaboration de politiques. Le CST est déterminé à assurer l'inclusivité, la représentativité et le soutien dans tout ce qu'il accomplit. La mission en dépend. Toutes les formes de diversité nous aident à résoudre des problèmes complexes afin de protéger le Canada et les Canadiennes et Canadiens.

Bilinguisme et langues officielles

Le CST est fier de son environnement de travail où chaque personne peut s'exprimer dans la langue officielle de son choix. La dualité linguistique et le bilinguisme au travail demeurent des priorités au CST. L'organisme est fier de ses réalisations dans ce domaine, notamment les suivantes :

- élaborer de nouvelles procédures d'organisation d'événements pour garantir une expérience équivalente dans les deux langues officielles;
- étudier et mettre à l'essai des capacités de traduction simultanée pour les événements virtuels et en personne;
- ajouter les accents dans les noms dans Outlook et dans Teams;
- prendre des mesures proactives de ressources humaines pour préparer l'organisme aux changements à venir à la *Loi sur les langues officielles*.

Le groupe d'affinité du Réseau franco du CST a également entamé une collaboration avec l'équipe des Langues officielles afin de concevoir une vision et un plan pour les langues officielles au sein de l'organisme. De plus, le Centre d'expertise en apprentissage en langue seconde a continué de fournir une grande variété d'outils et de ressources pour aider les membres du personnel à gagner des compétences et de la confiance dans leur langue seconde.

L'inclusivité dans la représentation externe

La passion du CST pour favoriser l'EDIA dépasse les murs de ses édifices. Il a travaillé fort cette année pour intégrer l'EDIA dans toutes les facettes de son travail, y compris ses témoignages parlementaires et sa participation aux événements externes. Par exemple, le CST a pris les mesures suivantes :

- mentionner les pronoms et la reconnaissance des territoires traditionnels dans les mots de bienvenue lors des témoignages parlementaires;
- faire découvrir les engagements parlementaires et encourager les membres d'une diversité de communautés de leadership du CST d'envisager de se proposer pour possiblement apparaître devant un comité parlementaire, ce qui a entraîné un grand nombre de témoignages par des personnes pour qui c'était une première expérience;
- augmenter graduellement la place de l'EDIA dans les programmes et les ordres du jour des grandes rencontres multilatérales;
- tenir compte de la diversité de représentation au moment de sélectionner les membres de délégations à l'étranger;
- lancer de nouvelles voies de collaboration avec la collectivité des cinq en organisant le premier Sommet sur l'EDIA de la collectivité des cinq, qui a permis d'échanger sur les pratiques exemplaires avec les partenaires et d'ouvrir la porte à de futurs échanges de connaissances;
- commencer à intégrer les pratiques exemplaires en matière d'EDIA à l'échelle institutionnelle dans le cadre des partenariats avec la collectivité des cinq par l'entremise de 2 délégations axées sur l'EDIA.

Analyse comparative entre les sexes Plus

Le CST s'est transformé au moyen de l'ACS Plus en façonnant sa culture organisationnelle et en améliorant ses politiques. La formation sur l'ACS Plus est obligatoire pour tout le personnel, de sorte que l'ensemble de l'effectif comprenne l'influence du genre et des facteurs intersectionnels, comme l'âge, l'appartenance ethnique et les limitations, sur les expériences et les résultats. Ces connaissances fondamentales ont renforcé la capacité du CST à cerner les biais et les obstacles dans ses processus, de sorte à créer des pratiques favorisant l'inclusion.

Le CST a intégré l'ACS Plus dans son travail des façons suivantes cette année :

- effectuer l'ACS Plus dans le cadre des présentations au Conseil du Trésor, des politiques opérationnelles et de la politique concernant l'obligation de prendre des mesures d'adaptation de sorte à encourager l'inclusivité, à éliminer les obstacles systémiques et à créer des politiques qui sont équitables et pratiques;
- intégrer l'ACS Plus dans les mémoires au Cabinet et les processus décisionnels, afin de tenir compte de l'intersectionnalité et des expériences des Canadiennes et Canadiens pour améliorer les résultats de la mission;
- insérer l'ACS Plus dans le Code de conduite pour renforcer l'engagement du CST envers l'EDIA en tant que principes centraux de l'organisme.

L'ACS Plus est plus qu'un outil au CST, elle est enracinée dans ses réflexes et lui permet de diriger par l'exemple et d'accroître sa crédibilité et son influence à l'interne et à l'externe.

Prix phare d'excellence en communication

Le CST est très fier des membres de ses équipes en communications qui ont reçu le prix Phare d'excellence en communication[36] pour leur travail exceptionnel dans le cadre du jeu Un CST intégré : la collection. Il s'agissait d'une initiative panorganisationnelle qui a vu la création d'un jeu effectuant la promotion des principes d'EDIA. Au fil d'une année, cette initiative a encouragé les membres du personnel à adopter des mesures concrètes qui ont permis d'enregistrer des progrès considérables au titre de l'EDIA au CST. Des cartes à jouer représentant les mesures d'EDIA ont permis aux secteurs de gagner des points en même temps qu'elles favorisaient la camaraderie. Cette initiative est l'une des nombreuses façons qui permettent au CST de favoriser le mieux-être au travail. Nous visons constamment à ce que notre environnement soit sain, diversifié et équitable.

Groupes d'affinité

Les groupes d'affinité offrent du soutien aux communautés et aident le CST à faire progresser les objectifs et priorités du CST en faisant part de leurs points de vue et en défendant leurs besoins. Ils proposent également un environnement sécuritaire à l'effectif diversifié et créent des occasions uniques de collaboration et d'unité. Les groupes d'affinité collaborent souvent pour organiser des événements et mettre sur pied des initiatives. Les groupes d'affinité sont invités aux tables de décision et leurs responsables présentent chaque année leurs défis, leurs besoins et leurs progrès aux cadres du CST. Il y a 11 groupes d'affinité au CST :

- Réseau de la Fierté
- Cybersécurité et renseignement au féminin (CRAF)
- 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
  - le groupe du patrimoine asiatique et sud-asiatique
- Groupe de la neurodiversité
- Groupe des personnes handicapées
- Groupe d'affinité juif
- Groupe d'affinité musulman
- Réseau franco
- Cercle des transmetteurs en code (patrimoine autochtone)
- Minorités audibles

Mise à jour de la Charte des valeurs et de l'éthique

Cette année, à la suite d'une année d'examens et de consultations à l'échelle de l'organisme, le CST a lancé sa charte des valeurs et de l'éthique actualisée. L'objectif était que la charte permette la mise en œuvre d'importantes priorités du CST, comme la vérité et la réconciliation. Nous voulions également qu'elle reflète mieux la diversité de l'effectif, la culture organisationnelle, le milieu de travail moderne et la fonction publique du Canada.

Apprenez-en plus sur la mise à jour de la Charte des valeurs et de l'éthique à la section « Le CST est transparent et rend des comptes ».


LE CST EST
TRANSPARENT
ET REND DES
COMPTES

Étant donné la nature du mandat du CST, une bonne partie de son travail est classifiée. Mais il reconnaît l'importance de transmettre autant d'informations que possible aux Canadiennes et Canadiens. Le CST est déterminé à faire preuve d'ouverture, de transparence et de reddition des comptes. Pour ce faire, il participe à des examens externes, procède à la surveillance et à la mesure de la conformité interne en plus de répondre aux demandes d'accès à l'information et de protection des renseignements personnels (AIPRP), mène des audits et bien plus.

Maintenir l'engagement envers la transparence et la reddition des comptes

Dans le cadre de son engagement envers la transparence et la reddition de comptes, le CST est un partenaire à part entière du Plan d'action et des activités du gouvernement du Canada pour un gouvernement ouvert. Il a téléversé 5 jeux de données et 47 éléments d'actif informationnel dans le portail du gouvernement ouvert cette année.

Autorisations ministérielles

En vertu de la *Loi sur le CST*, certaines activités doivent être autorisées par la ou le ministre de la Défense nationale. Il y a différentes autorisations selon les volets du mandat du CST. Les autorisations sont valides pendant 1 an et peuvent.

Avant d'entreprendre une activité en vertu d'une autorisation de renseignement étranger ou de cybersécurité, le CST doit recevoir l'approbation de la ou du commissaire au renseignement[37]. Cette année, le CST a présenté 8 demandes d'autorisations auprès du commissaire au renseignement, et toutes ont été approuvées.

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

Le nombre d'autorisations de cyberopérations[38] étrangères cette année est resté le même que l'année précédente. Les autorisations sont valides pendant un an et peuvent couvrir plusieurs opérations ou aucune.

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

Arrêtés ministériels

La ou le ministre de la Défense nationale signe des arrêtés ministériels pour désigner des personnes ou des organisations auxquelles le CST peut transmettre de l'information ou offrir du soutien adapté en matière de cybersécurité. En date du 31 mars 2025, 5 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 touchant la cybersécurité;
- l'information électronique et les infrastructures d'information importantes pour le gouvernement du Canada;
- l'information électronique et les infrastructures d'information du gouvernement de la Lettonie comme étant importantes pour le gouvernement du Canada;
- l'information électronique et les infrastructures d'information du gouvernement de l'Ukraine comme étant importantes pour le gouvernement du Canada.

Aucun nouvel arrêté n'a été émis cette année et aucun arrêté n'a été modifié.

Examens externes

Les activités du CST, à l'instar de celles des autres ministères fédéraux, font l'objet d'un examen par des organes d'examen fédéraux, comme le Commissariat à la protection de la vie privée et le Bureau du vérificateur général. Ces organes d'examen externe veillent, au nom des Canadiennes et Canadiens, à ce que les activités du CST respectent la loi. Le CST est en faveur de ces examens indépendants, puisqu'ils assurent la transparence et la reddition de comptes de son important travail. Il attache de l'importance aux commentaires qui découlent des examens et en tient compte pour améliorer ses processus.

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

Cette année, le CST a commencé à publier ses réponses aux recommandations des organes d'examen[39] sur son site Web afin d'accroître la transparence. Il a publié les réponses aux recommandations de 3 rapports d'examen de l'OSSNR cette année.

Contribuer aux examens externes sur l'ingérence étrangère

Parmi les 25 examens externes auxquels a contribué le CST cette année, 3 étaient des examens sur l'ingérence étrangère dans les élections fédérales au Canada. Les examens étaient menés par l'OSSNR, le CPSNR et l'enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques.

Le CST a contribué à l'achèvement et à la publication des rapports suivants portant sur l'ingérence étrangère, qui ont été déposés au Parlement :

- Examen de la diffusion du renseignement ayant trait à l'ingérence politique étrangère exercée par la République populaire de Chine de 2018 à 2023[40] de l'OSSNR
- Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada[41] du CPSNR

Conformité interne

L'équipe responsable de la conformité au CST a effectué des activités de surveillance afin de garantir la conformité aux politiques internes. Toutes les évaluations et conclusions en matière de conformité interne au CST sont accessibles aux organes d'examen externe.

Les statistiques de cette année comprennent une nouvelle catégorie : incidents de conformité qui ne concernent pas l'information de Canadiennes ou Canadiens. Ce faisant, on améliore le suivi et l'analyse de tous les incidents de conformité opérationnelle du CST. En 2024, l'équipe chargée de la conformité au CST a dénombré les incidents suivants :

- 22 incidents de conformité opérationnelle ne concernant pas l'information de Canadiennes et Canadiens;
- 119 incidents de conformité opérationnelle concernant l'information de Canadiennes et Canadiens.

Exemple d'incident opérationnel et des mesures d'atténuation

Tous les incidents opérationnels sont triés et évalués avant que des mesures d'atténuation soient mises en œuvre. Certains incidents exigent des breffages supplémentaires auprès des cadres du CST, voire de la ou du ministre. Par exemple, cette année, nous avons informé le ministre d'un incident où le CST a mal transmis de l'information. Le CST a découvert une activité pour laquelle, entre 2020 et 2023, il a transmis de l'information à des partenaires étrangers sans retirer adéquatement l'information canadienne qui avait été acquise par inadvertance en visant des cibles valides de renseignement étranger. Même si l'information était protégée, l'activité ne respectait pas les exigences de la politique du CST.

Le CST a agi rapidement pour contenir le problème. Les mesures correctives nécessitaient de placer des limites strictes sur l'échange d'information et d'obtenir l'assurance des partenaires de confiance du CST que l'information a été supprimée. Le CST continue de mettre à jour ses politiques et ses procédures pour empêcher que des incidents continuent de survenir.

L'incident ne représentait pas une atteinte substantielle à la vie privée, qui aurait dû être signalée dans le rapport annuel au Parlement sur l'application de la *Loi sur l'accès à l'information*[42]. Toutefois, le CST a proactivement signalé l'incident aux organes d'examen et de surveillance, dont le Commissariat à la protection de la vie privée, et a informé ces organismes des résultats de ses examens internes.

Plaintes

Cette année, le CST a reçu 3 plaintes externes à l'intention de la chef du CST et a répondu à 1 plainte envoyée à l'OSSNR concernant ses activités.

Le CST a également répondu aux conclusions et aux recommandations de l'examen de l'OSSNR concernant une plainte sur le processus de recrutement et de sécurité du CST. Le rapport de l'OSSNR concluait que les allégations étaient infondées, à l'exception d'une allégation qui était partiellement fondée. Le CST s'engage toujours à s'améliorer et à répondre aux recommandations de l'OSSNR.

Audit et évaluation

Les équipes chargées des audits et des évaluations donnent des conseils et services impartiaux fondés sur des preuves directement à la haute direction afin d'aider le CST à atteindre ses objectifs stratégiques.

Cette année, le CST a réalisé 2 audits et 3 évaluations de programmes, en vue d'améliorer l'efficacité et l'efficience des activités opérationnelles du CST. Les fonctions d'audit et d'évaluation sont elles-mêmes assujetties à des examens, et, cette année, les équipes ont fait l'objet d'un examen externe et d'une évaluation indépendante.

Le programme d'audit et d'évaluation est appuyé par le Comité ministériel d'audit (CMA) du CST, qui prodigue des conseils et propose une orientation stratégique. Dans son rôle de conseiller, le CMA s'informe et demeure pertinent pour offrir une perspective professionnelle, indépendante et non biaisée, en laquelle la ou le chef et les autres cadres supérieures et supérieurs peuvent avoir confiance.

Programme d'audit de la cybersécurité

Depuis 2018, le CST propose une gamme d'outils gratuits[43] aux responsables des audits afin qu'elles et ils évaluent la posture de cybersécurité des organisations. Jusqu'à maintenant, le CST a reçu plus de 200 demandes d'accès à ces outils de partout au gouvernement et dans le secteur privé.

Innovation dans les audits au CST

Lors de la conférence nationale de l'Institut des auditeurs internes Canada en 2024, l'équipe chargée de l'audit et de l'évaluation du CST a eu le plaisir de présenter un outil novateur aux fins d'audit de la sécurité infonuagique. L'équipe continuera de publier des conseils pour les responsables des audits au sein du gouvernement du Canada et à l'externe.

Valeurs et éthique

La mise à jour de la Charte des valeurs et de l'éthique du CST tient compte des commentaires reçus d'employées et employés demandant des clarifications quant aux obligations et une charte qui reflète la valeur de la fonction publique centrale « Respect envers les personnes ».

Le respect est l'une des 6 valeurs organisationnelles du CST qui met l'accent sur l'accessibilité, la lutte contre le racisme, l'équité, l'inclusion et la réconciliation. La charte actualisée comprend des principes pratiques qui guident les membres du personnel dans leurs activités et interactions quotidiennes.

Employée en parallèle avec le nouveau Code de conduite du CST, qui apporte des précisions à la charte en décrivant les attentes sur le plan comportemental, la charte propose au personnel du CST un plan moderne et complet pour effectuer leurs tâches de façon éthique et responsable en tant que représentantes et représentants du CST et du gouvernement du Canada.

Le CST a également mis en œuvre cette année un processus annuel de soumission des rapports confidentiels. Toutes et tous les employés doivent remplir annuellement une déclaration de conflits d'intérêts. Cette mesure assurera la responsabilisation de chaque personne et le respect de la charte.

Au cours de la prochaine année, le Bureau de l'éthique du CST poursuivra la mise à jour de sa formation sur l'éthique fondée sur des scénarios et la prestation de conseils sur des sujets comme les conflits d'intérêts, l'utilisation personnelle des médias sociaux, l'impartialité et l'utilisation de l'IA.

Contribuer à l'Enquête publique sur l'ingérence étrangère

En janvier 2025, le rapport final de l'Enquête publique sur l'ingérence étrangère[44] a été rendu public. Cette enquête a examiné les questions d'ingérence par des États étrangers ou des auteurs non étatiques et a évalué la capacité des entités fédérales de protéger les processus démocratiques du Canada. Le rapport présente 51 recommandations. Le CST, en coordination avec le gouvernement du Canada, examine soigneusement les conclusions et les recommandations pour prendre les bonnes mesures.

Le CST était heureux de coopérer et de contribuer à l'Enquête. Le CST a collaboré avec le BCP et le SCRS pour former des équipes à Montréal, à Toronto et à Ottawa qui ont mis en place des connexions réseau et des équipements sécurisés dans le cadre de l'Enquête.

Par ailleurs, le CST a produit plus de 85 000 documents pour contribuer à la commission et a permis à des membres de la haute direction, y compris sa chef, de témoigner devant public et à huis clos en soutien aux efforts.

Notes en fin de texte

1 https://laws-lois.justice.gc.ca/fra/lois/c-35.3/page-1.html#h-1170321
2 https://www.canada.ca/fr/conseil-prive/services/publications/priorites-canada-renseignement.html
3 https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=fra
4 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-fr.aspx
5 https://www.cyber.gc.ca/fr/orientation/cyberbulletin-cyberactivites-parrainees-republique-populaire-chine-menees-contre-gouvernements-provinciaux-territoriaux-autochtones-administrations-municipales-canada
6 https://www.cyber.gc.ca/fr/orientation/cybersecurite-chaine-approvisionnement-pour-petites-moyennes-organisations-itsap00070
7 https://www.cyber.gc.ca/fr/nouvelles-evenements/conseils-conjoints-choix-technologies-securisees-verifiables
8 https://www.cyber.gc.ca/fr/outils-services/solutions-communications-securisees
9 https://portal-portail.cyber.gc.ca/fr/
10 https://www.cyber.gc.ca/fr/glossaire#c
11 https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-fra.htm
12 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/centre-securite-telecommunications-canada-strategie-matiere-dintelligence-artificielle
13 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/institut-tutte-mathematiques-calcul
14 https://www.cse-cst.gc.ca/fr/mission/recherche-cst/centre-recherche-vulnerabilites
15 https://www.cyber.gc.ca/fr/geekweek
16 https://www.cyber.gc.ca/fr/geekweek/geekweek-9
17 https://www.cse-cst.gc.ca/fr/cst-crsng-communautes-subvention
18 https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage
19 https://www.pensezcybersecurite.gc.ca/fr/ressources/comment-utiliser-langage-amoureux-se-proteger-ligne
20 https://www.pensezcybersecurite.gc.ca/fr/blogues/tactiques-descroquerie-dont-il-faut-se-mefier-saint-valentin
21 https://www.pensezcybersecurite.gc.ca/fr/blogues/protegez-transactions-ligne-fraudes-virement-electronique
22 https://www.pensezcybersecurite.gc.ca/fr/methodes-paiement
23 https://www.pensezcybersecurite.gc.ca/fr/ressources/video-numero-7726
24 https://www.pensezcybersecurite.gc.ca/fr/prochaine-generation-savoir-reconnaitre-contenus-generes-laide-lintelligence-artificielle
25 https://www.pensezcybersecurite.gc.ca/fr/ressources/voici-9-facons-reperer-contenu-cree-laide-lintelligence-artificielle
26 https://www.pensezcybersecurite.gc.ca/fr/blogues/cybermenaces-encore-plus-sophistiquees-grace-lia
27 https://www.pensezcybersecurite.gc.ca/fr/blogues/pourquoi-vous-ne-devriez-jamais-partager-vos-informations-personnelles-lia
28 https://indigenous.link/cse-cybersecurite/
29 https://www.pensezcybersecurite.gc.ca/entreprises
30 https://www.pensezcybersecurite.gc.ca/fr/mois-de-la-sensibilisation-la-cybersecurite
31 https://www.pensezcybersecurite.gc.ca/fr/ressources/faites-partie-generation-pensez-cybersecurite
32 https://www.cyber.gc.ca/fr/etat-preparation-matiere-cybersecurite/objectifs-relatifs-letat-preparation-matiere-cybersecurite-securiser-systemes-plus-essentiels
33 https://www.cyber.gc.ca/fr/orientation
34 https://www.cyber.gc.ca/fr/orientation/facteurs-relatifs-securite-considerer-dispositifs-dacces-itsm80101
35 https://www.cyber.gc.ca/fr/nouvelles-evenements/attenuation-menaces-ressources-limitees-conseils-lintention-societe-civile
36 https://www.canada.ca/fr/gouvernement/systeme/communications-gouvernementales/bureau-collectivite-communications/prix-excellence-communication/prix-equipe.html#t4
37 https://www.canada.ca/fr/commissaire-renseignement.html
38 https://www.cse-cst.gc.ca/fr/mission/cyberoperations
39 https://www.cse-cst.gc.ca/fr/reddition-comptes/transparence/reponses-rapports-examens
40 https://nsira-ossnr.gc.ca/fr/examens/nos-examens/examen-de-la-diffusion-du-renseignement-ayant-trait-a-lingerence-politique-etrangere-exercee-par-la-republique-populaire-de-chine-de-2018-a-2023/
41 https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/rapport-special-ingerence-etrangere.pdf
42 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports
43 https://www.cyber.gc.ca/fr/outils-services/programme-audit-cybersecurite
44 https://commissioningerenceetrangere.ca/rapports/rapport-final

Canada