

Le Centre de la sécurité des télécommunications Canada (CST)

Préparé pour la ou le ministre de la Défense nationale

Printemps 2025



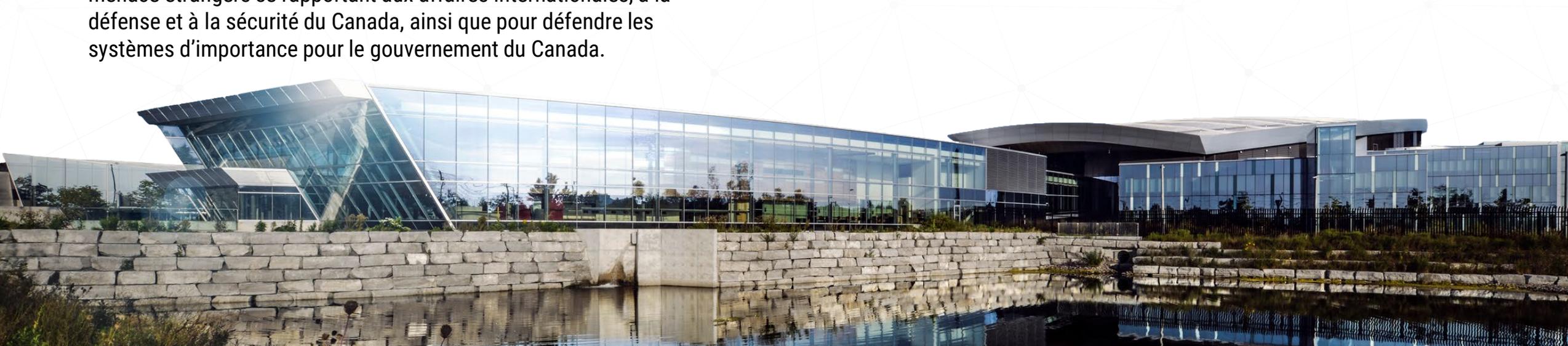
Le CST dans l'appareil de sécurité nationale actuel du Canada

- La collectivité de la sécurité et du renseignement du Canada défend la sécurité du territoire, du gouvernement, de l'économie et de la population du Canada. Elle fournit également de l'information en vue de favoriser les intérêts canadiens et de les protéger.
- L'appareil de sécurité nationale s'emploie à :
 - produire du renseignement;
 - analyser les principaux enjeux et événements;
 - réduire les menaces;
 - renforcer la résilience;
 - effectuer un contrôle des personnes et des investissements préoccupants sur le plan de la sécurité.
- Les organismes de renseignement et d'application de la loi collaborent avec divers ministères et avec des partenaires étrangers.



Le rôle du CST

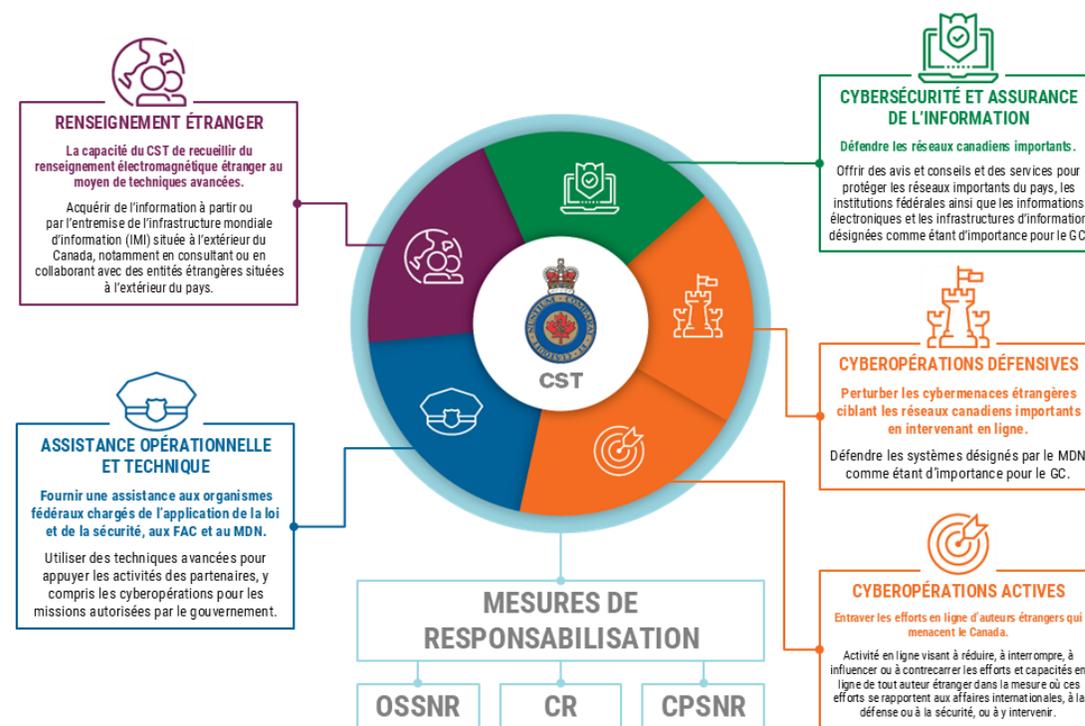
- **Recueillir du renseignement étranger et produire des rapports à ce sujet** conformément aux priorités du gouvernement du Canada en matière de renseignement.
- **Assurer la cybersécurité**, procurer l'assurance de l'information et des communications sécurisées au gouvernement du Canada, et lui offrir des conseils et des services pour protéger les systèmes qu'il juge importants.
- **Prendre des mesures en ligne** par voie de **cyberopérations étrangères** pour **interrompre et réduire** les activités d'auteurs de menace étrangers se rapportant aux affaires internationales, à la défense et à la sécurité du Canada, ainsi que pour défendre les systèmes d'importance pour le gouvernement du Canada.
- **Fournir une assistance technique et opérationnelle** aux organismes fédéraux chargés de l'application de la loi et de la sécurité, ainsi qu'au MDN et aux FAC.
- **Diriger le Centre canadien pour la cybersécurité**, qui offre des conseils en matière de cybersécurité aux parties prenantes externes et au public.



Le mandat du CST

- Le mandat du CST est défini dans la [Loi sur le Centre de la sécurité des télécommunications \(Loi sur le CST\)](#), édictée en 2019.
- À titre de ministre de la Défense nationale, **vous influencez directement sur la façon dont le CST exécute son mandat** en délivrant des autorisations ministérielles, des ordonnances et des directives qui donnent effet aux autorisations législatives du CST.
- Il est explicitement **interdit au CST de faire porter ses activités sur des Canadiennes et Canadiens** n'importe où dans le monde ou sur toute personne se trouvant au Canada.
- Les activités du CST **font l'objet d'une surveillance indépendante** par la ou le commissaire au renseignement (CR) et d'exams rétroactifs de la part de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR).

LA LOI SUR LE CST | UN MANDAT À CINQ VOILETS



Exécution du mandat : Objectifs en matière de renseignement étranger

- Le CST acquiert et analyse des renseignements électroniques afin de détecter les activités d'entités étrangères qui cherchent à miner la sécurité nationale et la prospérité du Canada et d'informer le gouvernement du Canada à ce sujet. Le renseignement étranger recueilli par le CST permet également de conférer aux responsables des politiques du Canada un avantage en matière d'information.
- Les rapports de renseignement du CST offrent notamment :
 - des renseignements uniques sur les menaces étrangères qui pèsent sur le Canada et des avertissements à cet égard afin d'éviter des surprises qui pourraient nuire à la population et aux institutions canadiennes, ou à leurs alliés;
 - des connaissances particulières pour étayer la politique étrangère et économique et la prise de décisions;
 - des renseignements pour appuyer le commerce, la sécurité économique, l'application de la loi et les opérations militaires en fournissant de l'information qui provient de sources autres que les sources publiques.

Cycle du renseignement



Exécution du mandat : Renseignement étranger – mesures et mécanismes

- En 2024-2025, le CST a transmis **2 878 rapports** à **3 016 clientes et clients** de plus de 32 ministères et organismes fédéraux.
- **Les rapports ne peuvent être lus que par les personnes autorisées** du gouvernement du Canada et de la collectivité des cinq. Des mécanismes robustes permettent de communiquer cette information de façon sécuritaire :
 - **Diffusion électronique**
 - Les rapports sont transmis par l'intermédiaire du Réseau canadien Très secret (RCTS), géré par le CST et utilisé aux fins de collaboration et de communication au niveau Très secret.
 - **Agentes et agents des relations avec la clientèle (ARC)**
 - Il s'agit d'employées et employés du CST intégrés dans les institutions du gouvernement du Canada qui fournissent des rapports de renseignement aux personnes autorisées, comme les ministres.
 - **Agentes et agents de diffusion du SIGINT (ADS)**
 - Il s'agit d'employées et employés d'autres ministères du gouvernement du Canada accrédités par le CST pour transmettre les rapports de renseignement aux clientes et clients autorisés de leurs ministères respectifs.
- Guidés par les priorités du gouvernement du Canada, les sujets abordés comprennent les suivants :
 - les activités d'États hostiles (p. ex. cybermenaces, espionnage, ingérence étrangère et influence malveillante, contre-ingérence et vol de propriété intellectuelle);
 - le terrorisme et l'extrémisme violent;
 - les actions et les intentions de la République populaire de Chine;
 - l'invasion de l'Ukraine par la Russie;
 - la souveraineté dans l'Arctique.



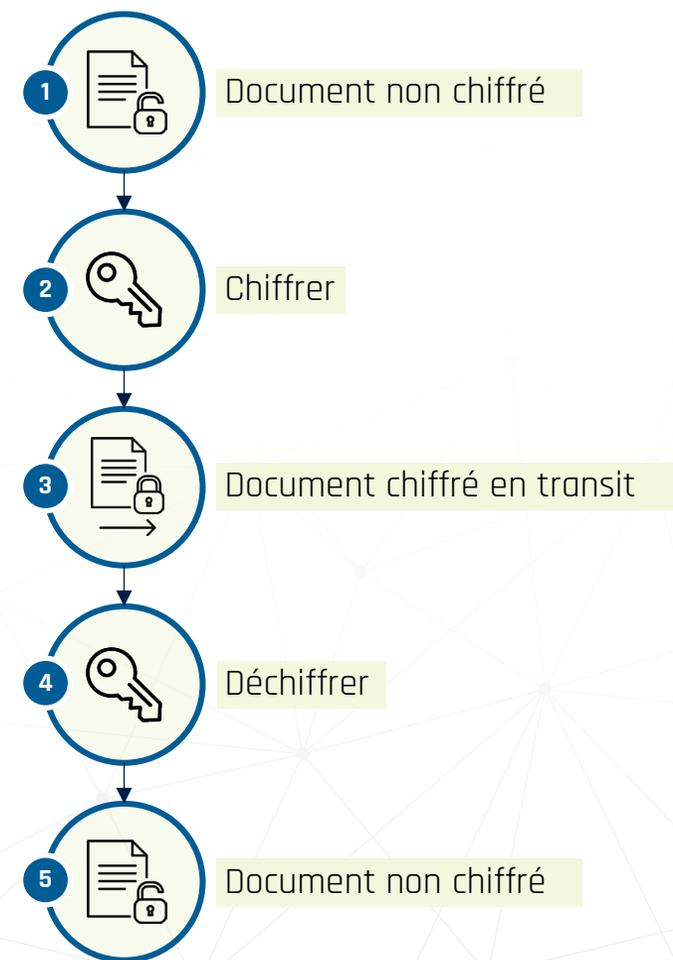
Exécution du mandat : Cybersécurité

- Le Centre canadien pour la cybersécurité du CST fournit des avis et conseils de même que des services afin d'aider à défendre le Canada contre les cybermenaces et de favoriser un cyberspace canadien fort et résilient.
- Le Centre pour la cybersécurité :
 - **défend les réseaux du gouvernement fédéral** – par exemple, il déploie des capteurs sur les points terminaux (comme des serveurs, des portables) qui détectent automatiquement des activités malveillantes, comme des maliciels, et offrent une protection contre les menaces;
 - **mène les interventions du Canada** lorsque se produisent des événements de cybersécurité;
 - **procure une source unifiée d'avis**, de conseils, de services et de soutien spécialisés en matière de cybersécurité et d'évaluation des menaces à la population et aux organisations canadiennes;
 - **collabore** avec tous les ordres de gouvernement, le secteur privé, l'industrie, le milieu universitaire, les infrastructures essentielles et les partenaires internationaux;
 - **appuie les efforts de cyberrésilience** dans les activités économiques et de recherche et d'investissement menées au Canada.



Exécution du mandat : Assurance de l'information

- Le CST est responsable de l'assurance de l'information, connue sous le nom de sécurité des communications (COMSEC), pour le gouvernement du Canada. Il s'agit d'un élément fondamental de la cybersécurité qui protège l'information sensible et empêche les adversaires d'y accéder. Pour ce faire, le CST recourt au chiffrement, qui :
 - transforme les données en code illisible, accessible uniquement par **clé** – une solide défense contre les cybermenaces;
 - permet de s'assurer que les données n'ont pas été modifiées durant la transmission;
 - instaure la confiance entre les parties prenantes, les partenaires et le public.
- En tant que pilier de la sécurité de l'information, le chiffrement permet, au moyen du matériel militaire, d'identifier qui est un ami et qui est un ennemi. Il protège également les opérations de sécurité nationale et les délibérations du Cabinet contre toute atteinte.
- Au cœur de COMSEC, le CST :
 - fournit au gouvernement du Canada et à certains partenaires de l'industrie **du matériel, des logiciels et des clés cryptographiques sécurisés**;
 - collabore avec des partenaires fédéraux et internationaux pour **assurer des normes rigoureuses en matière de cryptographie**;
 - travaille à **se préparer à l'émergence des ordinateurs quantiques**. Ces ordinateurs, qui pourraient permettre le déchiffrement, seraient accessibles dès 2030.



Exécution du mandat : Cyberopérations étrangères

- Le CST peut prendre des mesures en ligne à l'appui des affaires internationales, de la défense et de la sécurité du Canada, ainsi que pour défendre les systèmes fédéraux et les systèmes d'importance pour le gouvernement du Canada.
- **À titre de ministre de la Défense nationale**, vous autorisez le CST à mener des cyberopérations actives et défensives. Vous ne pouvez délivrer l'autorisation de cyberopérations défensives que si vous avez consulté la ou le ministre des Affaires étrangères, qui doit aussi consentir à toute cyberopération active.
- **Les cyberopérations défensives (COD)** perturbent les activités étrangères visant des institutions fédérales et des systèmes d'importance (p. ex. réseaux énergétiques, réseaux de télécommunications, bases de données de soins de santé, systèmes bancaires). Par exemple, le CST peut empêcher des cybercriminelles et cybercriminels de voler de l'information sur un réseau du gouvernement du Canada en désactivant leur serveur étranger.
- **Les cyberopérations actives (COA)** sont des mesures proactives visant à perturber les menaces étrangères à la défense, à la sécurité ou aux affaires internationales du Canada. Par exemple, le CST a mené des cyberopérations actives pour empêcher les groupes étrangers de diffuser en ligne des documents sur l'extrémisme violent.
- Les **FAC** et le **CST** sont partenaires de longue date dans le développement de capacités techniques et spécialisées de transmission de renseignement pour soutenir les opérations militaires. Au cours de la dernière décennie, le partenariat a évolué pour inclure la collaboration dans les domaines de la cybersécurité et des cyberopérations défensives et actives. Par l'entremise du COMCYBERFAC (Commandement Cyber des Forces armées canadiennes), le CST continue de mener des cyberopérations conjointes avec les FAC à l'appui des objectifs de mission.
- **Les cyberopérations ne doivent pas :**
 - cibler des Canadiennes et Canadiens ou des personnes se trouvant au Canada;
 - contrecarrer le cours de la justice;
 - contrecarrer le cours de la démocratie;
 - entraîner la mort ou des lésions corporelles.

En 2023, le CST a utilisé des capacités de COD contre un groupe étranger à l'origine de rançongiciels qui ciblait un grand nombre d'organisations du secteur canadien des infrastructures essentielles.

Le Centre pour la cybersécurité a pris des mesures pour réduire le risque de compromission au Canada, tandis que l'équipe des cyberopérations étrangères est intervenue dans le cyberspace pour perturber les serveurs étrangers des cybercriminelles et cybercriminels, réduisant ainsi l'efficacité et la rentabilité de leurs activités.

Exécution du mandat : Assistance opérationnelle et technique

- En tant qu'organisme national de cybersécurité et de renseignement étranger du Canada, le CST possède des capacités techniques et opérationnelles toutes particulières qui peuvent aider d'autres organismes fédéraux à assurer la sécurité de la population canadienne.
- Le CST est autorisé à aider :
 - les organismes fédéraux chargés de la sécurité et de l'application de la loi :
 - Gendarmerie royale du Canada (GRC)
 - Service canadien du renseignement de sécurité (SCRS)
 - Agence des services frontaliers du Canada (ASFC)
 - le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC)
- Lorsqu'il aide des partenaires fédéraux, le CST agit en vertu des autorisations légales qui lui sont conférées (p. ex. mandats judiciaires).
- En 2024-2025, le CST a donné suite à 51 demandes d'assistance de partenaires fédéraux.



National
Defence

Défense
nationale

La collaboration à l'œuvre : Coordonner les mandats du CST

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



La collaboration à l'œuvre : Alliance de la collectivité des cinq

- Le CST est un membre fier et estimé de la collectivité des cinq, l'alliance d'échange de renseignement la plus ancienne et la plus étroite du monde.
- La collectivité des cinq est un élément clé dans le domaine du renseignement et de la sécurité au Canada, offrant un avantage stratégique permettant de comprendre les événements mondiaux et d'y réagir.
- Ce partenariat durable continue de produire des résultats qui améliorent la sécurité des citoyennes et citoyens des cinq pays, notamment :
 - **l'échange de renseignement étranger;**
 - **le soutien aux cyberopérations étrangères;**
 - **l'assurance d'interopérabilité et de redondance des systèmes;**
 - **la réalisation de recherches classifiées d'importance stratégique;**
 - **la communication conjointe de menaces et de conseils.**
- En s'exprimant d'une seule voix, la collectivité des cinq renforce les communications publiques. Le message est amplifié dans les publications conjointes sur des sujets comme la cybercriminalité, l'intelligence artificielle et les menaces contre les infrastructures essentielles.
- Le CST collabore également étroitement avec des alliés aux vues similaires dans le cadre de partenariats bilatéraux et de forums multilatéraux.



Comment le CST accomplit sa mission

Au CST, le personnel est la plus grande force. Son effectif est composé de personnes dévouées, qui prennent appui sur leurs divers parcours, compétences, perspectives et expériences pour protéger le Canada, et ce, en tout temps.

Pour résoudre les problèmes complexes auxquels il fait face, le CST doit les aborder selon des perspectives, des compétences et des points de vue divers. Par conséquent, **il accorde la priorité à une plus grande représentativité à tous les échelons de l'organisme.**

Comptant **plus de 3 700 employées et employés**, l'effectif du CST est composé d'un large éventail de spécialistes qui se consacrent à assurer la sécurité du Canada et de sa population.

Le CST fait figure de **leader éclairé et de pionnier** dans les domaines des nouvelles technologies numériques et de la cybersécurité, grâce notamment à son programme de recherche axé sur la cryptographie quantique, l'intelligence artificielle et l'analytique évoluée.



L'innovation et la souplesse sont essentielles à la façon dont le CST exécute sa mission et représentent de plus en plus la clé de son avenir.

Le CST **évolue dans un solide système de surveillance et d'examen** et maintient une culture de conformité, de respect de la loi et de transparence dans l'exécution de son mandat visant à préserver la confiance des Canadiennes et Canadiens.

Le CST **veille à protéger les Canadiennes et Canadiens**, à défendre les valeurs canadiennes et à renforcer le rôle du Canada en tant que partenaire de confiance à l'échelle internationale.