Centre de la sécurité des télécommunications

Rapport institutionnel

1 APERÇU ET MANDAT

1.1 Histoire du CST

Le Centre de la sécurité des télécommunications (CST) est l'organisme de renseignement électromagnétique étranger ainsi que l'autorité technique en matière de cybersécurité et d'assurance de l'information au Canada. Le CST intercepte et analyse des communications électroniques étrangères pour fournir des informations uniques au gouvernement du Canada au sujet des menaces étrangères contre la sécurité et la prospérité du Canada, ainsi que des connaissances importantes à l'appui des politiques étrangères et des prises de décisions.

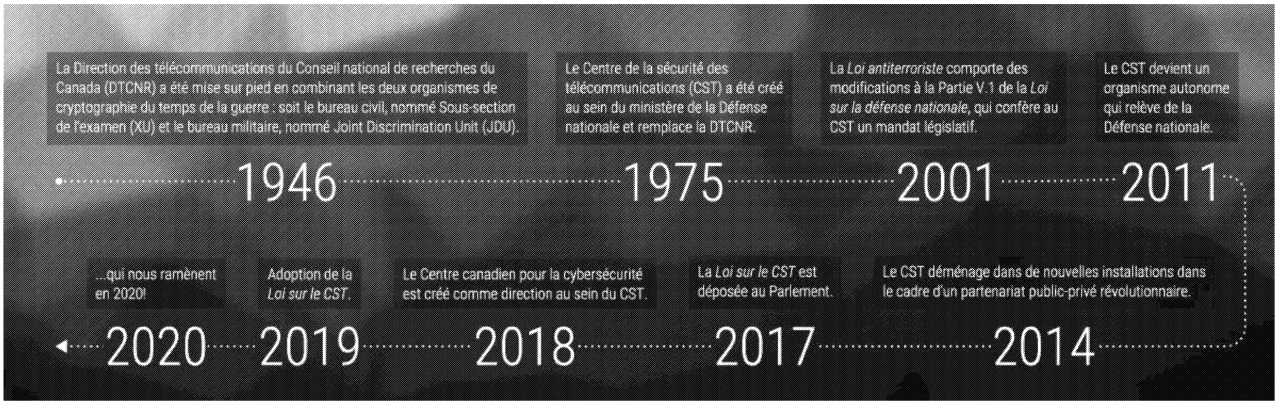
Les activités de collecte de renseignement étranger du CST sont menées exclusivement selon les priorités du gouvernement établies annuellement par le Cabinet.

La riche histoire du CST en matière de renseignement électromagnétique (SIGINT) étranger et de sécurité des communications (COMSEC) remonte à la Seconde Guerre mondiale et aux débuts du SIGINT canadien (voir image 1). Initialement mis sur pied pour appuyer l'effort de guerre britannique, le corps de signaux militaires s'est rapidement acquitté d'une opération conjointe militaire et civile. En 1946, la Direction des télécommunications du Conseil national de recherches (DTCNR) est devenue le tout premier organisme de cryptologie du Canada en temps de paix. En 1975, la DTCNR devient la responsabilité du ministère de la Défense nationale et change de nom pour devenir le Centre de la sécurité des télécommunications (CST).

Depuis plus de 75 ans, le CST est un atout précieux pour le gouvernement du Canada et ses partenaires alliés et a toujours maintenu son engagement à l'égard de sa mission principale, c'est-à-dire fournir au gouvernement fédéral le SIGINT essentiel à la sécurité nationale du pays et protéger les communications du gouvernement du Canada.

En août 2019, la *Loi sur le CST*, un jalon capital pour le CST, est entrée en vigueur. Aujourd'hui le CST est un organisme autonome, qui mène des opérations 24 heures sur 24 et sept jours sur sept pour recueillir du renseignement étranger, protéger les systèmes importants pour le Canada, mener des cyberopérations et aider nos partenaires fédéraux dans l'exécution de leurs mandats respectifs.

Image 1 : Jalons de l'histoire du CST



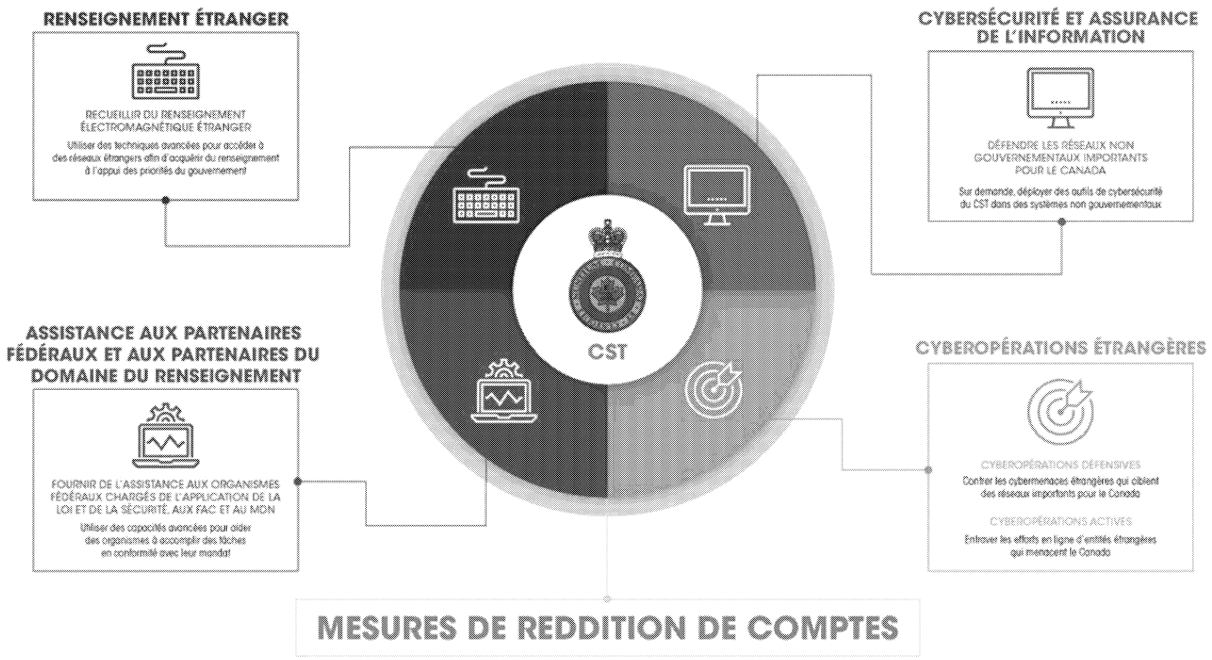
1.2 Mandat du CST

Le paragraphe 15 de la *Loi sur le CST* définit le mandat du CST en tant que l'organisme national de renseignement électromagnétique responsable de fournir du renseignement étranger de même que l'autorité technique responsable de la cybersécurité et de l'assurance de l'information.

Il est à noter que la loi interdit explicitement au CST de mener des activités contre des Canadiennes ou Canadiens ou des personnes se trouvant au Canada. De plus, les activités du CST ne doivent pas contrevenir à la *Charte canadienne des droits et libertés*[1]. Le CST ne peut pas demander à ses alliés de mener des activités en son nom qu'il n'est pas lui-même autorisé à mener.

Pour en savoir plus, consultez l'*annexe 1* : « Aperçu de la *Loi sur le CST* ».

Image 3 : Aperçu du mandat du CST



MANDAT (S.15) : L'organisme national du renseignement électromagnétique en matière de renseignement étranger et l'expert technique de la cyber sécurité et de l'assurance de l'information.

[1] En vertu du paragraphe 22(1) de la *Loi sur le CST* : Les activités menées par le Centre dans la réalisation des volets de son mandat touchant le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives ou les cyberopérations actives ne peuvent viser des Canadiens ou des personnes se trouvant au Canada et ne peuvent porter atteinte à la Charte canadienne des droits et libertés.

1.3 Pouvoirs du CST

Le ministre de la Défense nationale oriente et autorise les activités du CST à l'aide des mécanismes suivants qui définissent les paramètres opérationnels et les attentes envers l'organisme :

- Autorisations ministérielles (AM)
- Arrêtés ministériels
- Directives ministérielles (DM)

1.3.1 Autorisations ministérielles

En vertu de la *Loi sur le CST*, le ministre de la Défense nationale doit autoriser le CST à mener certains types d'activités à l'appui des volets de son mandat touchant le renseignement ou la cybersécurité, si ces activités :

- risquent de contrevenir à toute autre loi fédérale (ou loi d'un État étranger en vertu des articles 16 et 18-19 seulement); ou
- pourraient porter atteinte à une attente raisonnable de protection en matière de la vie privée d'un Canadien ou d'une personne au Canada.

Les AM de renseignement étranger et de cybersécurité doivent démontrer ce qui suit :

- l'autorisation est nécessaire et les activités sont raisonnables et proportionnelles;
- l'information ne peut pas raisonnablement être obtenue d'une autre manière (c.-à-d. que l'activité est nécessaire);
- l'information ne sera pas conservée plus longtemps que ce qui est nécessaire; et
- des mesures sont en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada.

Quatre types d'AM correspondent aux volets du mandat du CST : renseignement étranger (art. 16), cybersécurité et assurance de l'information (art. 17) et cyberopérations actives et défensives (art. 18 et 19).

Le commissaire au renseignement[2] doit approuver les autorisations liées au renseignement étranger et à la cybersécurité avant que le CST puisse entamer ces activités. Chaque autorisation est valide pour une durée maximale d'un an.

Toutefois, le commissaire au renseignement n'approuve pas les cyberopérations actives (COA) ni les cyberopérations défensives (COD) (collectivement appelées les cyberopérations étrangères [COE]), conformément à la *Loi sur le CST*. Les COE sont aussi approuvées grâce à un système «à deux niveaux» dans le cadre duquel le ministre de la Défense nationale doit consulter ou obtenir le consentement de la ministre des Affaires étrangères avant d'émettre l'autorisation. Les demandes d'autorisations de COE au ministre de la Défense nationale doivent aussi démontrer

[2]Le commissaire au renseignement est chargé de procéder à un examen quasi-judiciaire des conclusions sur lesquelles reposent certaines autorisations accordées ou modifiées et certaines déterminations effectuées au titre de la *Loi sur le Centre de la sécurité des télécommunications* et de la *Loi sur le Service canadien du renseignement de sécurité*.

que l'autorisation est nécessaire et que les activités autorisées sont raisonnables et proportionnelles.

Les AM ne sont pas nécessaires en ce qui a trait au volet du mandat du CST qui touche l'assistance technique et opérationnelle à un organisme fédéral chargé de l'application de la loi ou de la sécurité, aux Forces canadiennes ou au ministère de la Défense nationale. Dans le cas, le CST a, quant à l'exercice d'une activité, les mêmes pouvoirs qu'auraient l'organisme fédéral, les Forces canadiennes ou le ministère s'ils menaient cette activité et est assujetti aux limites que la loi leur impose, y compris aux exigences de tout mandat applicable.

Chaque fois qu'une AM est abrogée ou arrive à sa date d'échéance, le CST doit présenter au ministre de la Défense nationale un rapport de fin d'autorisation dans lequel on décrit les résultats des activités menées. Les rapports de fin d'autorisation liés au renseignement étranger ou à la cybersécurité doivent être communiqués au commissaire au renseignement. En ce qui concerne les autorisations liées aux COE, on doit présenter le rapport de fin d'autorisation au ministre de la Défense nationale et à la ministre des Affaires étrangères.

Enfin, le ministre de la Défense nationale ne peut pas autoriser des activités qui ne font pas partie de la *Loi sur le CST*, ni accorder des pouvoirs au CST qui ne sont pas énoncés dans la *Loi sur le CST*.

1.3.2 Arrêtés ministériels

En vertu de la *Loi sur le CST*, le ministre de la Défense nationale peut avoir recours à un arrêté ministériel pour désigner des personnes ou des organismes avec lesquels le CST peut échanger de l'information ou auxquels le CST peut fournir des services de cybersécurité. À titre d'exemple, pour que le CST puisse fournir des services de cybersécurité à une institution non fédérale, le ministre doit d'abord désigner les cybersystèmes de cette institution comme étant «importants pour le gouvernement du Canada». Les arrêtés ministériels du CST servent à :

- désigner des cybersystèmes non fédéraux comme étant «importants pour le gouvernement du Canada»;
- désigner des entités auxquelles le CST peut communiquer de l'information se rapportant à une Canadienne ou un Canadien ou à une personne se trouvant au Canada si c'est nécessaire pour protéger les informations ou les systèmes d'institutions fédérales ou des infrastructures essentielles;
- désigner des entités auxquelles le CST peut communiquer de l'information susceptible d'identifier une Canadienne ou un Canadien si c'est essentiel aux affaires internationales, à la défense ou à la sécurité.

1.3.3 Directives ministérielles

La chef du CST reçoit des instructions sur les activités de l'organisme de la part du ministre de la Défense nationale sous forme de directives ministérielles (DM). Ces directives servent à établir les lignes directrices, les paramètres régissant les activités et les attentes du ministre à l'égard du CST relativement à différents enjeux. Le CST peut mener uniquement les activités qui s'inscrivent dans son mandat et les pouvoirs qui lui sont conférés, et ces activités doivent être conformes aux directives ministérielles.

À l'heure actuelle, le CST a seulement une directive en vigueur : la DM sur les priorités du gouvernement du Canada en matière de renseignement. Les activités de collecte de renseignement étranger du CST sont liées par la loi aux priorités du gouvernement du Canada en matière de renseignement, qui sont établies annuellement par le MDN par l'intermédiaire d'une DM. C'est donc dire que le CST peut uniquement recueillir du renseignement qui se rapporte aux priorités établies par le Cabinet.

Il en résulte ensuite un processus interministériel dirigé par le BCP qui vise à traduire les priorités en matière de renseignement en besoins de renseignement plus détaillés; la DM du CST énonce les besoins qui sont ensuite transformés en priorités et plans internes.

Une DM ne peut accorder au CST un pouvoir qui n'est pas prévu dans la *Loi sur le CST*.

2 DESCRIPTION DES PROGRAMMES, POLITIQUES ET PROCÉDURES MIS EN PLACE POUR CONTRER LES MENACES ET LES INCIDENTS LIÉS À L'INGÉRENCE ÉTRANGÈRE LORS DES 43E ET 44E ÉLECTIONS GÉNÉRALES

2.1 Réponse du CST contre les menaces d'ingérence étrangère

Les auteures et auteurs étatiques hostiles tentent par différents moyens, dont l'espionnage, les cyberactivités malveillantes et la désinformation en ligne, d'influencer et de perturber la société et la démocratie du Canada. L'ingérence étrangère est une menace constante qui n'est pas seulement liée aux périodes d'élections. Contrer ces activités nécessite une approche pangouvernementale que le CST appuie ainsi :

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

Depuis les élections fédérales de 2015, le CST s'assure que des mesures de cyberdéfense robustes et efficaces sont en place pour protéger les systèmes et les réseaux d'Élections Canada, de même que les processus démocratiques du pays. En raison de son expérience liée à la surveillance des activités d'ingérence et de ses enquêtes connexes, l'organisme a produit de nombreux rapports sur les risques que représente l'ingérence contre le processus démocratique du Canada et sur les moyens de nous protéger de ces menaces.

2.2 Contrer les activités de pays hostiles et l'ingérence étrangère

Le CST prend tous les moyens dont il dispose en vertu de son mandat (renseignement étranger, cybersécurité, cyberopérations étrangères et assistance technique et opérationnelle) pour contrer les activités étatiques hostiles. Ces activités menaçantes comprennent l'espionnage, les cyberactivités malveillantes et l'ingérence étrangère.

2.2.1 Cyberactivités menées par des auteurs de menaces parrainés par un pays étranger

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

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

2.2.2 Répression transnationale

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

Le CST, de pair avec des partenaires étrangers et fédéraux, s'emploie à atténuer les risques que représentent ces activités de répression transnationale. Il y parvient en procédant à la collecte de renseignement électromagnétique (SIGINT) et en appuyant la collectivité canadienne de la sécurité et du renseignement.

2.2.3 Désinformation et démocratie

La désinformation est une fausse information qui vise délibérément à causer du tort. Souvent conçue pour susciter une réponse émotionnelle, elle se propage très rapidement dans les médias sociaux. Il est ainsi difficile pour les Canadiennes et Canadiens d'évaluer la véracité de ce qu'ils lisent ou la fiabilité de la source de l'information. Le CST croit qu'il est très probable que les cybermenaces contre les processus démocratiques à l'échelle mondiale soient plus nombreuses et plus sophistiquées au cours de l'année à venir, et peut-être même à plus long terme.

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

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

Le CST contribue à une campagne de sensibilisation pangouvernementale sur la désinformation en ligne qui comprend ce qui suit :

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

2.2.4 Attributions publiques

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

En 2017, le CST a estimé que des auteurs de menace en Russie étaient responsables du développement de *NotPetya*, un maliciel destructeur qui ciblait sans distinction des entités des secteurs financier, énergétique et gouvernemental et du secteur des infrastructures partout dans le monde.

En décembre 2017, le CST s'est joint à ses alliés et partenaires pour attribuer WannaCry à la Corée du Nord, un maliciel de demandes de rançons et d'extorsion qui a interrompu certains services à l'échelle mondiale.

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

Les rapports de renseignement et les analyses de cybersécurité du CST ont contribué aux attributions publiques suivantes :

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

Avec des partenaires de la collectivité des cinq, le Centre pour la cybersécurité a aussi fait paraître trois bulletins de cybersécurité conjoints pour informer le lectorat des techniques employées par les auteures et auteurs de menaces œuvrant pour le compte de la Russie, ainsi que les rapports, alertes et documents d'orientation suivants :

- Bulletin de cybersécurité conjoint sur les cybermenaces criminelles et parrainées par la Russie qui planent sur les infrastructures essentielles (avril 2022)
- Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie (juillet 2022)

- Conseils en matière de cybersécurité en cas de niveaux de menace élevés (juillet 2022)
- Risques de cyberactivités malveillantes contre les nations alliées de l'Ukraine (février 2023)

2.2.5 Autres rapports et documents d'orientation à l'intention des Canadiennes et Canadiens

Le Centre pour la cybersécurité du CST publie des rapports sur les menaces et des conseils en ligne afin que toute la population puisse accéder à de l'information de qualité sur la cybersécurité. Ces rapports et ces ressources sont produits depuis 2017.

En 2018, le Centre pour la cybersécurité publie la première édition de l'*Évaluation des cybermenaces nationales* (ECMN).

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

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

En guise de complément à l'ECMN, le Centre pour la cybersécurité publie régulièrement des conseils liés à ces cinq tendances.

Partout dans le monde, les processus démocratiques sont ciblés par des auteurs de cybermenaces. C'est dans ce contexte que le Centre pour la cybersécurité du CST a publié en 2017, 2019, 2021 et 2023 le rapport intitulé «*Cybermenaces contre le processus démocratique du Canada*». Dans ces rapports, le CST examine les tendances à l'échelle mondiale en matière de cybermenaces contre les processus démocratiques (qui comprennent l'électorat, les partis politiques et les élections) et évalue la menace envers le Canada.

2.3 Réponse du CST contre les menaces d'ingérence étrangère liées aux élections canadiennes

Partout dans le monde, les processus démocratiques continuent d'être touchés par les activités de cybermenace. Les activités de cybermenace ciblent les participantes et participants aux processus démocratiques, et les événements connexes, et sont causées par les auteurs de menace parrainés par des États étrangers, des cybercriminels, des auteurs de menace qui ont des motifs politiques, des hacktivistes et des amateurs et amatrices de sensations fortes. Le ciblage des processus démocratiques demeure largement une activité stratégique. Nous constatons que des auteures et auteurs de cybermenace étatiques ayant des liens avec la Russie, la Chine et l'Iran continuent d'être à l'origine de la plupart des activités de cybermenace visant les processus démocratiques dans le monde.

Les auteures et auteurs de menace ont de nombreuses occasions de cibler les processus démocratiques du Canada, mais il est important de noter qu'au cours des dernières années on a fait de grandes avancées en vue de protéger ces processus, notamment au cours des deux dernières élections générales (les 43e et 44e élections générales tenues en 2019 et en 2021 respectivement).

2.3.1 Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GTMSRE)

Le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GTMSRE) est un groupe de travail interministériel qui rassemble des représentantes et représentants du CST, du Service canadien du renseignement de sécurité (SCRS), de la Gendarmerie royale du Canada (GRC) et d'Affaires mondiales Canada (AMC) qui :

- examine et échange du renseignement, effectue des évaluations et des analyses de source ouverte liées à l'ingérence étrangère dans le processus démocratique du Canada de façon coordonnée;
- fournit une connaissance de la situation à nos partenaires du gouvernement, aux cadres de la fonction publique et à d'autres partenaires pertinents;
- fait la promotion des processus électoraux en échangeant avec nos partenaires ou, lorsque nos mandats respectifs le permettent, prend des mesures pour atténuer les menaces.

De plus, durant toute la période des élections de 2019 et de 2021, le GTMSRE a diffusé des rapports de situation (RAPSIT) quotidiens par courriel à sa liste de distribution, qui comprend le Protocole public en cas d'incident électoral majeur (PPIEM) du Canada.

Le rôle du CST au sein du GTMSRE consiste à éplucher le SIGINT et les cyberactivités dans les réseaux du gouvernement du Canada pour trouver des indications d'ingérence étrangère dans le processus électoral. Le CST a dirigé le GTMSRE de sa conception en 2018 jusqu'en 2022 où le SCRS s'est mis à occuper ce rôle.

Durant les périodes électorales, les partenaires du GTMSRE ont offert régulièrement des mises à jour à un panel de hauts dirigeants, conformément au PPIEM. Le PPIEM est un processus simple, clair et impartial qui servirait à indiquer aux Canadiennes et Canadiens qu'un incident ou une série d'incidents menace la capacité du Canada à avoir des élections justes et libres. Plus de détails sur le panel du PPIEM se trouvent dans le rapport institutionnel du Bureau du Conseil privé. Les membres du GTMSRE continuent de se réunir pour maintenir leurs liens à titre de collectivité et pour surveiller les activités d'ingérence étrangère en cours.

2.3.2 Protéger les infrastructures électorales

Dans le cadre de son mandat, le CST peut mener des cyberopérations défensives (COD) en réponse à des cyberattaques sur les systèmes essentiels.

À l'approche des élections fédérales de 2019 et de 2021, le MDN a émis une autorisation de COD qui visait notamment à protéger les infrastructures électroniques d'Élections Canada. Il s'agissait d'une mesure de prévention en cas de cyberactivité malveillante durant les périodes

électorales. À titre d'exemple, si un auteur de menace étranger compromettait le site Web d'Élections Canada, le CST pourrait utiliser ses capacités en matière de cyberopérations pour viser le serveur utilisé pour lancer l'attaque. Dans ces deux cas cependant, aucune activité nécessitant de COD n'a eu lieu. Toutefois, les COD sont un outil important afin de contrer les cybermenaces visant les processus démocratiques du Canada.

Le CST avait planifié deux COD afin de prévenir les menaces d'ingérence étrangère dans les institutions et les processus démocratiques du Canada. La COD liée aux élections fédérales de 2019 était planifiée et approuvée, mais n'a jamais été menée, étant donné que la menace ne s'est pas concrétisée. La COD a été remise sur pied et planifiée en prévision des élections fédérales de 2021, mais aucune autorisation n'a été sollicitée et elle n'a jamais été menée, étant donné que la menace ne s'est pas concrétisée.

Bien que ces deux opérations soient liées aux menaces d'ingérence étrangère dans les institutions et les processus électoraux canadiens, il faut noter que le point de mire du CST dans le cadre de ces COD était de perturber les cybermenaces qui visaient précisément les infrastructures d'Élections Canada, et seulement si les trois conditions de l'AM de COD étaient satisfaites. Les objectifs des opérations étaient de perturber ou d'interrompre les éléments étrangers sur l'infrastructure mondiale de l'information (IMI) utilisés à des fins de cyberactivité malveillante contre les infrastructures d'Élections Canada afin de les protéger.

2.3.3 La cybersécurité dans les institutions démocratiques

Les institutions démocratiques représentent une part fondamentale des infrastructures essentielles du Canada. Le Centre pour la cybersécurité collabore avec les organismes électoraux et les partis politiques fédéraux pour les aider à renforcer leur cybersécurité, en plus de travailler avec Élections Canada et ses homologues provinciaux et territoriaux afin de veiller à ce que leurs réseaux soient bien protégés.

À l'approche des élections fédérales de 2019 et de 2021, le Centre pour la cybersécurité a organisé des breffages à l'intention des partis politiques fédéraux pour les renseigner sur les cybermenaces et les conseiller quant à l'adoption de pratiques exemplaires en matière de cybersécurité. Pour ces deux événements, le Centre pour la cybersécurité a mis sur pied une ligne d'information pour répondre aux préoccupations des candidates et candidats en matière de cybersécurité. En dehors des périodes d'élections, le Centre pour la cybersécurité a un point de contact affecté aux questions de cybersécurité des partis politiques, notamment pour que les candidates et candidats puissent recevoir des avis et des conseils spécialisés, qui sont également accessibles sur le site Web du Centre pour la cybersécurité.

Durant chacune de ces élections, le CST a mis en œuvre des efforts visant à surveiller, à prévenir et à atténuer les activités étrangères hostiles en lien avec les élections.

Durant les 43e et 44e élections générales, en plus de ses activités habituelles, le Centre pour la cybersécurité a également :

- offert du soutien aux organismes électoraux en prévision des élections provinciales dans l'ensemble du pays

- transmis des ressources d'orientation aux municipalités
- fournis aux organismes électoraux :
    - des séances d'information sur l'Évaluation des cybermenaces nationales,
    - des conseils techniques,
    - des ressources d'orientation,
    - des services de cybersécurité.

2.3.4 Information sur les cybermenaces visant les élections

En mai 2022, dans le cadre de sa réponse à la suite des 43e et 44e élections générales, le CST a créé une page Web sur les cybermenaces visant les élections. La page donne un aperçu des façons dont les auteurs de menaces peuvent perturber les processus démocratiques, notamment :

- perturber les infrastructures électorales au moyen d'attaques par déni de service distribué (DDoS pour *distributed denial of service*);
- imiter les identités d'utilisatrices et utilisateurs afin de diffuser de l'information fausse sur les médias sociaux;
- compromettre les systèmes TI des partis politiques;
- lancer des campagnes d'influence étrangère en ligne afin de discréditer les processus démocratiques;
- utiliser des rançongiciels afin de perturber l'accès aux données des élections.

La page Web contient des liens vers les rapports du Centre pour la cybersécurité portant sur les cybermenaces contre les processus démocratiques du Canada. Elle fournit également des avis et des ressources d'orientation à jour à l'intention des partis politiques, des organismes électoraux et de l'électorat.

2.3.5 Directive de septembre 2023 de la chef du CST sur les menaces contre la démocratie

Au début de septembre 2023, la chef adjointe du SIGINT et le dirigeant principal du Centre pour la cybersécurité ont reçu une directive de la chef du CST détaillant les attentes sur la manière dont le CST contribuera aux efforts globaux du gouvernement du Canada afin de protéger la démocratie canadienne. La directive soulignait plus précisément l'orientation de la chef voulant que le CST continue de mener des opérations pour assurer la prestation en temps opportun de renseignement étranger sur les menaces au Parlement, aux députés, à leurs familles et au personnel (de même que sur les menaces en matière de cybersécurité liées à des députés en particulier) afin d'éclairer la prise de décisions.

Veuillez consulter l'*annexe 2* pour prendre connaissance de la *directive de septembre 2023 de la chef du CST sur les menaces contre la démocratie*.

3 PRINCIPAUX CADRES SUPÉRIEURS

3.1 Chef du CST

Nom(s) des cadres supérieurs

- Caroline Xavier (31 août 2022 – présent)
- Shelly Bruce (27 juin 2018 – 30 août 2022)

Rôles et responsabilités

Gérer et administrer le CST et tous les dossiers connexes.

3.2 Chef associé, CST

Nom(s) des cadres supérieurs

- Daniel Rogers (janvier 2022 – février 2023)
- Daniel Rogers a été le seul chef associé du CST au cours de cette période et le poste a été supprimé après son départ.

Rôles et responsabilités

Aider à la supervision et à la gestion des efforts déployés par le CST.

3.3 Dirigeant principal, Centre pour la cybersécurité, CST

Nom(s) des cadres supérieurs

- Sami Khoury (septembre 2021 – présent)
- Scott Jones (octobre 2019 – août 2021)

Rôles et responsabilités

Assurer la supervision des activités du Centre pour la cybersécurité, qui constitue la source unifiée de conseils spécialisés, d'avis, de services et de soutien sur la cybersécurité à l'intention des Canadiennes et Canadiens.

3.4 Dirigeant associé, Centre pour la cybersécurité, CST

Nom(s) des cadres supérieurs

- Rajiv Gupta (2021 – présent)
- André Boucher (2018 – 2021)

Rôles et responsabilités

Participer à l'avancement des activités et de la gestion du Centre pour la cybersécurité.

3.5 Chef adjoint, Renseignement électromagnétique (SIGINT), CST

Nom(s) des cadres supérieurs

- Alia Tayyeb (2022 – présent)
- Daniel Rogers (2018 – 2022)

Rôles et responsabilités

Assurer la surveillance et la gestion des volets renseignement électromagnétique étranger et cyberopérations étrangères du mandat du CST. Répondre aux demandes d'assistance des partenaires fédéraux, conformément à l'article 20 de la *Loi sur le CST*.

3.6 Chef adjoint associé, Renseignement électromagnétique (SIGINT), CST

Nom(s) des cadres supérieurs

- Artur Wilczynski (2020 – 2022)
- Artur Wilczynski a été le seul chef adjoint associé du SIGINT au cours de cette période et le poste a été supprimé après son départ.

Rôles et responsabilités

Aider à la supervision et à la gestion des volets du mandat du CST touchant le renseignement électromagnétique étranger et les cyberopérations étrangères, et faciliter la réponse aux demandes d'assistance des partenaires fédéraux en vertu de l'article 20 de la *Loi sur le CST*.

3.7 Chef adjoint, Pouvoirs, conformité et transparence (PCT), CST

Nom(s) des cadres supérieurs

- Christopher Williams (p. i.) (décembre 2023 – présent)
- Nabih Eldebs (2021 – décembre 2023)
- Le poste n'existait pas avant 2021. Il s'agissait auparavant du poste de directeur général, Politiques, divulgations et examens. Nabih Eldebs a occupé ce poste de 2019 à 2021.

Rôles et responsabilités

Mener à bien et appuyer le processus d'approbation, le cadre de gouvernance et les exigences stratégiques des autorisations ministérielles qui permettent l'exécution des opérations liées à la mission, ainsi que les activités complémentaires qui permettent d'effectuer et de maintenir les activités opérationnelles du CST (politiques opérationnelles, programme de conformité opérationnelle, transparence et échange d'information et examen externes et plaintes). Le CA PCT fait également office de chef de la protection des renseignements personnels du CST.

3.8 Président, Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GTMSRE)

Nom(s) des cadres supérieurs

- Lyall King (2018 – 2022)
- Le poste a été supprimé au CST.

Rôles et responsabilités

Le GTMSRE a réuni des spécialistes et responsables opérationnelles et opérationnels du CST, du SCRS, d'AMC et de la GRC dans le but d'améliorer la sensibilisation, la collecte, la coordination et la prise de mesures visant à contrer l'ingérence étrangère qui cible les élections fédérales du Canada. Le président du GTMSRE était responsable de l'administration et de la coordination globales du groupe, ce qui comprend l'administration des réunions, l'organisation et la préparation du travail du GTMSRE pour les prochaines élections, la tenue de séances d'information et la rédaction de rapports.

4 CANAUX D'INFORMATION POUR LE BUREAU DU MINISTRE ET LE MDN

Les exigences politiques du CST sur la façon d'autoriser ses produits de renseignement aux fins de diffusion sont énoncées dans l'ensemble des politiques relatives à la mission (EPM). Plus précisément, l'article 26.2 de l'EPM en matière de renseignement étranger mentionne les exigences pour tous les produits SIGINT communicables (PSC) :

«Tous les PSC doivent être diffusés au moyen des systèmes ou processus approuvés et respecter les six exigences suivantes :

- *inclure toute information jugée comme ayant une valeur en tant que renseignement étranger à l'appui des priorités du GC en matière de renseignement;*
- *être modifiés afin de protéger la vie privée des Canadiens et des personnes au Canada;*
    - *respecter les règles de protection de la vie privée des ressortissants des pays de deuxième part ou des personnes se trouvant sur le territoire d'un pays de deuxième part, conformément aux politiques de l'entité de deuxième part concernée;*
- *être expurgés pour protéger les méthodes, les techniques et les actifs SIGINT (conformément à la classification);*
- *être numérotés et récupérables;*
- *porter une mise en garde, au besoin;*
- *être approuvés aux fins de communication par l'autorité concernée responsable de la diffusion.*

En raison de ces exigences, les produits de renseignement du CST ne peuvent être diffusés que par l'entremise de certains systèmes et mécanismes, peu importe la ou le destinataire.

4.1 Information produite par le CST ou des organismes de deuxième part

Le CST diffuse le renseignement recueilli aux membres de la collectivité de la sécurité et du renseignement du Canada sous forme de produits de renseignement publiés dans les applications de production de rapports du CST sur le réseau canadien Très secret (RCTS).

Dans le cours normal des activités, le bureau du MDN est informé des rapports pertinents du CST et de ses partenaires par les agentes et agents des relations avec la clientèle (ARC) du CST. Les ARC fournissent les rapports pertinents au moyen de solutions électroniques sécurisées ou sur papier. De plus amples renseignements sur le programme des ARC se trouvent à la section 5.

Le MDN peut également être informé des rapports pertinents du CST par la chef du CST durant des réunions planifiées, des réunions spéciales ou des appels. Selon les besoins et le degré d'urgence, la ou le chef du personnel ou l'agente ou agent de liaison ministérielle du CST peut aviser le BMND des rapports pertinents importants par téléphone ou par courriel.

4.2 Information produite par d'autres ministères

Lorsque de l'information sur une ingérence étrangère possible est produite par d'autres ministères, l'information peut être fournie par divers moyens :

1. les ministères produisant l'information envoient des copies numériques des rapports pertinents à une liste de distribution en particulier;
2. les ministères produisant l'information peuvent en fournir des copies électroniques ou papier à des fins de sensibilisation et de discussion lors des réunions hebdomadaires ou spéciales du sous-ministre, du Comité du Cabinet ou de réunions ministérielles.

Au besoin, la ou le chef du personnel du CST peut signaler cette information pour sensibiliser le BMDN par téléphone ou par courriel dans le cadre de réunions régulières planifiées et de réunions spéciales. L'agente ou agent de liaison ministérielle ou la chef du CST peut également signaler cette information directement au MDN ou à son bureau durant les réunions hebdomadaires régulières ou de façon opportune, selon le cas.

Au besoin, les représentantes ou représentants du CST peuvent rencontrer une ou un ministre afin de lui communiquer du renseignement dans un endroit sécurisé et accrédité.

5 CANAUX D'INFORMATION POUR LE BCP ET LE CPM

Contrairement aux rapports des autres organismes du gouvernement du Canada chargés de la sécurité et de l'application de la loi, les rapports de renseignement étranger du CST sont essentiellement des représentations factuelles des données de communications électroniques. Le CST n'utilise pas l'information qu'il collecte pour évaluer le renseignement dont il fait rapport ou formuler des conclusions. Le CST peut inclure des commentaires analytiques dans ses PSC, qui servent à fournir un contexte supplémentaire aux détails contenus dans les rapports. Il revient donc aux destinataires des rapports de renseignement du CST d'évaluer la pertinence et la signification globales de l'information mentionnée. L'évaluation de l'information par des partenaires et des clientes et clients, ou le contexte dans lequel ils évaluent cette information, dépend entièrement de ces clients et partenaires. Le Centre pour la cybersécurité utilise le renseignement étranger obtenu par le CST en plus d'autres sources d'information pour étayer ses évaluations liées aux cybermenaces.

Tel qu'il est indiqué à la section 4, les produits de renseignement du CST ne peuvent être diffusés que par l'entremise de certains systèmes et mécanismes, peu importe la ou le destinataire. Les outils de production de rapports du CST sont utilisés pour diffuser, gérer et suivre l'information qu'il produit ou qui lui est communiquée à des fins de diffusion ultérieure.

Les clientes et clients du gouvernement du Canada qui sont titulaires d'un compte dans l'outil de production de rapports du CST peuvent accéder directement aux produits de renseignement correspondant à leur habilitation de sécurité et à leurs endoctrinements. Ces clientes et clients, dont font partie les cadres supérieures et supérieurs du BCP, peuvent alors utiliser ce renseignement dans leurs processus de prise de décisions, leurs analyses et leurs rapports dérivés.

Les clientes et clients du gouvernement du Canada qui sont autorisés selon leur habilitation de sécurité et leurs endoctrinements à accéder aux produits de renseignement, mais qui ne sont pas titulaires d'un compte dans l'outil de production de rapports du CST peuvent tout de même recevoir les produits de renseignement par l'intermédiaire des ARC du CST. Les ARC fournissent alors les produits de renseignement à ces clientes et clients en format papier ou électronique (au moyen d'une solution sécurisée). Les ARC utilisent l'outil de production de rapports du CST pour ensuite faire le suivi du lectorat et de la rétroaction sur les produits qu'elles et ils ont présentés ou fournis aux clientes et clients du GC. Les hauts fonctionnaires du BCP, le premier ministre et le personnel du bureau du premier ministre ont accès aux produits de renseignement correspondant à leur habilitation de sécurité et à leurs endoctrinements par l'intermédiaire des services offerts par les ARC du CST.

Le CST fournit également l'accès à ses produits de renseignement à d'autres ministères du GC par l'intermédiaire de ses agentes et agents de diffusion du SIGINT (ADS). Ces ADS sont des employées et employés du gouvernement du Canada qui sont titulaires d'un compte dans l'outil de production de rapports du CST et à qui on a confié des tâches semblables à celles des ARC dans leurs ministères respectifs uniquement. Les ADS font un suivi lorsqu'elles et ils ont diffusé des rapports à leurs clientes et clients internes ou reçu des commentaires sur ces rapports.

5.1 Flux typique de diffusion par une ou un ARC

Les ARC interagissent avec leurs clientes et clients pour définir leurs exigences et s'assurer de bien les comprendre au fil du temps. Ces derniers peuvent également demander qu'on les informe sur des sujets particuliers en fonction des besoins.

Lorsqu'un produit présente un intérêt pour une cliente ou un client, l'ARC l'imprime et le remet à la cliente ou au client si elle ou il a accès à un coffre-fort accrédité. L'ARC indiquera par la suite dans l'outil de production de rapports que la personne a eu accès au produit. Bien que l'accès ait été fourni à la cliente ou au client, cela ne signifie pas de façon définitive qu'elle ou il a lu le produit de renseignement. Si la cliente ou le client n'a pas accès à un coffre-fort approprié, l'ARC s'assoira avec elle ou lui pendant la consultation du produit de renseignement, puis reprendra ce dernier. De plus, toute rétroaction fournie par la cliente ou le client, en ce qui concerne la valeur et l'utilisation du produit de renseignement, sera consignée par l'ARC dans l'outil de production de rapports du CST.

Les ARC assurent toujours le contrôle intégral des copies imprimées et consignent leur destruction. Ces registres sont vérifiés régulièrement pour assurer l'intégrité de l'information cloisonnée.

Le CST peut aussi évoquer des rapports à des fins de sensibilisation et de discussion lors des réunions hebdomadaires ou spéciales du sous-ministre, du Comité du Cabinet ou de réunions ministérielles.

6 BREFFAGES VERBAUX OU ÉCRITS SUR LES QUESTIONS ABORDÉES PAR LES POINTS (A)(I)(A) ET (A)(I)(B) DU MANDAT CONFÉRÉ PAR LA COMMISSION POUR LE GTMSRE, LE PANEL DU PPCIEM, LES SOUS-MINISTRES, LES CSNR, LE GREFFIER DU CONSEIL PRIVÉ, LE CPM OU LE PREMIER MINISTRE DEPUIS SEPTEMBRE 2018

Au cours des 43e (2019) et 44e (2021) élections générales, le CST a présidé le GTMSRE (voir la section 2.3.1 pour de plus amples renseignements à ce sujet. Le GTMSRE a tenu des breffages avant et après les deux élections.

De plus, tout au long des élections de 2019, des élections de 2021 et en réponse aux mesures prises pendant les élections partielles de 2023, le GTMSRE a diffusé des rapports de situation sur une base régulière aux membres de sa liste de distribution, qui comprend le PPIEM.

Veuillez consulter la version classifiée du présent rapport pour obtenir la liste complète de ces breffages.

7 CONSEILS ET RECOMMANDATIONS FORMULÉES AUX MINISTRES OU AUX BUREAUX DES MINISTRES

Depuis janvier 2019, le CST n'a fourni ni conseil ni recommandation à une ou un ministre ou à un bureau de ministre en réponse à du renseignement particulier sur de l'ingérence étrangère touchant des processus et institutions démocratiques, notamment de l'ingérence dans des affaires parlementaires.

8 STRUCTURE DE GOUVERNANCE DE LA SÉCURITÉ ET DU RENSEIGNEMENT

Dirigé et présidé par le CST :

Comité canadien chargé des systèmes de sécurité nationale (CCSSN) : L'équipe du Secrétariat agit au nom du CCSSN pour offrir de la surveillance, de l'orientation et de la gestion opérationnelles à la collectivité canadienne des systèmes de sécurité nationale. Le Secrétariat produit, toujours au nom du CCSSN, la feuille de route stratégique des activités qui comprend l'élaboration d'instruments de politique et la surveillance de la conformité. Ces activités visent à assurer l'application uniforme et appropriée des mesures de protection à l'ensemble des actifs de sécurité nationale, à déterminer les niveaux de risque acceptables, et à maintenir des relations de confiance et l'interopérabilité avec les alliées.

Comité des directeurs généraux sur les cyberopérations : Afin d'appuyer la mise en œuvre de la Stratégie nationale de cybersécurité du Canada, et conformément aux politiques nationales applicables, le gouvernement, par l'entremise du Comité des directeurs généraux sur les cyberopérations (DG Cyber Ops), aide à veiller à ce que les principaux ministères et organismes fédéraux responsables de la cybersécurité travaillent de concert à la protection du Canada.

Le Comité des DG sur les cyberopérations a été mis sur pied pour assurer une intervention fédérale coordonnée en cas de cybermenace et de cyberincident d'intérêt national et pour assurer l'avancement des enjeux liés aux politiques opérationnelles nationales.

- Le Comité des DG sur les cyberopérations est le sous-groupe opérationnel du Comité des DG sur la cybersécurité. Le Comité des DG sur les cyberopérations est différent de celui sur la cybersécurité, en ce sens qu'il est axé sur les opérations et qu'il compte moins de membres. La participation se limite aux organismes à qui des fonctions opérationnelles de cybersécurité ont été confiées.
- Le Comité des DG sur les cyberopérations concentre principalement ses efforts sur les cyberévénements d'intérêt national ou les événements touchant les systèmes non fédéraux. L'intervention en cas de cyberévénement touchant l'infrastructure et les systèmes du gouvernement du Canada sera effectuée conformément au Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC).

Bien que le CST dirige le CCSSN, les hauts fonctionnaires du BCP seraient mieux placés pour donner une description complète de la structure interministérielle de gouvernance de la sécurité nationale et du renseignement du Canada.

9 PRODUITS DE RENSEIGNEMENT PORTANT SUR L'INGÉRENCE ÉTRANGÈRE

Le CST a produit différents types de produits de renseignement depuis janvier 2019. La section 2 contient de plus amples renseignements sur les programmes qui ont élaboré ces produits.

Veuillez consulter la version classifiée du présent rapport pour obtenir la liste et la description des produits de renseignement portant sur l'ingérence étrangère.

10 ACTIVITÉS VISANT À RÉDUIRE LES MENACES

Le CST n'a rien à signaler, puisqu'il ne détient pas de pouvoir conféré par la loi de mener des activités visant à réduire les menaces. Les activités de cyberopérations défensives (COD) du CST ont été décrites ci-dessus.

Annexe 1 : Guide éclair sur la *Loi sur le CST*

Annexe 2 : Directive de la chef du CST sur les menaces contre la démocratie

DIRECTIVE DE LA CHEF DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

MENACES CONTRE LA DÉMOCRATIE

En tant que chef du Centre de la sécurité des télécommunications (CST), je suis l'auteure de la présente directive, à l'intention de la chef adjointe, Renseignement électromagnétique (SIGINT) et du dirigeant principal du Centre canadien pour la cybersécurité (CCC). Protéger la démocratie du Canada est l'une des principales responsabilités du gouvernement du Canada et le CST joue un rôle clé pour aider à assumer cette responsabilité. Par conséquent, dans cette directive, je présente mes attentes sur la façon dont le CST contribuera aux efforts du gouvernement du Canada.

Le CST apportera une contribution essentielle en continuant d'exercer tous les volets de son mandat visant à :

- **Détecter** les menaces contre la démocratie du Canada en recueillant du renseignement étranger;
- **Défendre** la démocratie du Canada contre les cybermenaces grâce à des mesures de cybersécurité;
- **Contrer** les menaces étrangères contre la démocratie du Canada en menant des cyberopérations étrangères; et
- **Assister** les autres ministères dans l'exercice des mandats que la loi leur confère.

S'assurer que le renseignement étranger sur les menaces contre le Parlement, les députés, leurs familles, leur personnel, et les cybermenaces contre des députés en particulier, soit transmis aux bonnes personnes, en temps opportun, pour éclairer la prise de décisions est un élément essentiel du travail effectué par le CST. Plus précisément, le CST continuera de faire ce qui suit :

- Assurer la diffusion en temps opportun de ses produits aux clients qui ont besoin du renseignement, comme le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GT MSRE), la Chambre des communes[1], les comités pertinents au niveau des sous-ministres (et les forums des sous-ministres adjoints subordonnés) ainsi que tout autre forum actuel ou futur saisi de cette question, le cas échéant.

- Tirer parti des mécanismes de diffusion et soutenir les mécanismes qui seront mis en place à l'avenir. De plus, le CST soutiendra particulièrement le Service canadien du renseignement de sécurité, conformément à la *Loi sur le CST*, dans l'exercice de ses fonctions conférées par la loi, à l'appui des Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires du ministre de la Sécurité publique.

[1] La collaboration avec la Chambre des communes se fera d'une manière qui respecte pleinement l'indépendance du pouvoir législatif du gouvernement.

- Faire le suivi et consigner de manière centralisée le lectorat des produits du CST.

Toutes les activités du CST seront menées conformément à la *Loi sur le Centre de la sécurité des télécommunications* et de manière à respecter les principes suivants :

- **Respect de la loi** – Le CST applique les principes et les exigences qui découlent des lois canadiennes, du cadre législatif et des politiques régissant nos activités, y compris le respect et la protection de la vie privée des Canadiennes et Canadiens.
- **Transparence** – Le CST reconnaît qu'il est essentiel à la démocratie que les Canadiennes et Canadiens comprennent ce que le gouvernement fait pour protéger la sécurité nationale, comment il le fait et pourquoi un tel travail est important.
- **Reddition de comptes** – Le CST appuie les mesures de reddition de comptes qui sont essentielles au système de gouvernement du Canada et au maintien de la confiance des Canadiennes et Canadiens. Le CST rendra des comptes au ministre de la Défense nationale, au Cabinet, au Parlement et aux Canadiennes et Canadiens.

DATE D'ENTRÉE EN VIGUEUR : La présente directive entrera en vigueur à la date de la signature.

Publié à Ottawa, en ce 8 septembre 2023.

Annexe 3 : Breffages du CST

Veuillez consulter la version classifiée du présent rapport pour obtenir de plus amples renseignements.

Annexe 4 : Produits de renseignement liés à la menace ou à l'incidence de l'ingérence étrangère dans les institutions et processus démocratiques du Canada depuis janvier 2019

Veuillez consulter la version classifiée du présent rapport pour obtenir de plus amples renseignements.