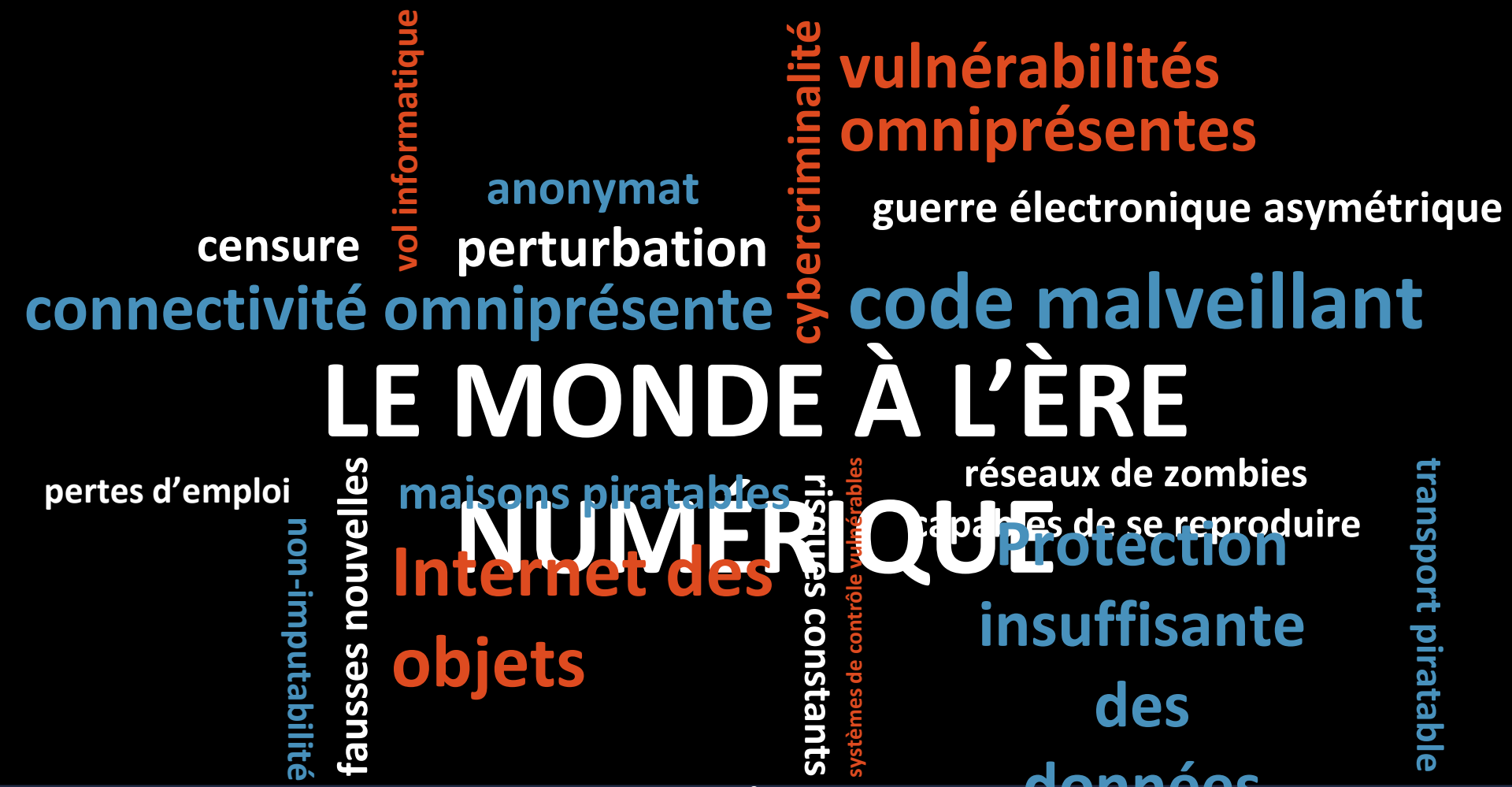
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

ISACA

Assemblée générale annuelle

Évaluation des cybermenaces nationales 2018

13 juin 2019


vol informatique
cybercriminalité
vulnérabilités omniprésentes
anonymat
guerre électronique asymétrique
censure
perturbation
connectivité omniprésente
code malveillant
LE MONDE À L'ÈRE
NUMÉRIQUE
pertes d'emploi
maisons piratables
réseaux de zombies
capables de se reproduire
non-imputabilité
fausses nouvelles
Internet des objets
risques constants
systèmes de contrôle vulnérables
Protection insuffisante des données
transport piratable

67 % des répondants canadiens au sondage de l'ACEI impartissent au moins une partie de leur empreinte de cybersécurité à des fournisseurs externes (ACEI)

La cybersécurité représente 1,7 milliard de dollars du PIB du Canada et génère plus de 11 000 emplois bien rémunérés (ACEI)

Écosystème de cybersécurité canadien

30 % des organisations déploient une plateforme de commerce électronique (ACEI)

Les organisations canadiennes devront embaucher environ **8 000** professionnels en cybersécurité supplémentaires entre 2016 et 2021 (Deloitte)

La Stratégie nationale de cybersécurité de 2018, *Vision du Canada pour la sécurité et la prospérité dans l'ère numérique*, présente la nouvelle

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Nous représentons la seule source unifiée d'avis, de conseils, de services et de soutien spécialisés en matière de cybersécurité pour le gouvernement, le secteur privé, les Canadiens ainsi que les propriétaires et exploitants d'infrastructures essentielles.

Résultats nationaux	Information et systèmes d'information importants	Complément des capacités publiques et commerciales

Centre de la sécurité des télécommunications

- Le Centre pour la cybersécurité fait partie du Centre de la sécurité des télécommunications (CST).
- Le CST mène ses activités dans le respect des dispositions de toutes les lois canadiennes, dont la ***Loi sur la protection des renseignements personnels***, le ***Code criminel*** et la ***Charte canadienne des droits et libertés***.
- Le mandat et les pouvoirs du CST sont énoncés dans la ***Loi sur la défense nationale***.

A. Fournir du **renseignement étranger**, conformément aux priorités du gouvernement du Canada en matière de renseignement.

B. Fournir **des avis, des conseils et des services** pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada.

C. Fournir une **assistance technique et opérationnelle** aux organismes fédéraux chargés de l'application de la loi et de la sécurité.

Centralisation de l’expertise en cybersécurité

À qui s’adressent nos services

Nous accueillons les partenariats visant à créer un cyberespace canadien fort et résilient. Nous offrons des espaces polyvalents et non classifiés que peuvent employer conjointement le gouvernement, l’industrie privée et le milieu universitaire.

Gouvernement

- pour les hauts dirigeants du gouvernement pour tout ce qui touche à la

Partenaires externes

- Nous représentons le point de contact principal du gouvernement fédéral en matière de cybersécurité pour les partenaires externes, notamment dans le cadre de la coordination et de l’intervention en cas d’incident.

Application de la loi

- Nous sommes la seule source autorisée à fournir de l’expertise technique en matière de cybersécurité qui vient appuyer les organismes responsables dans le cadre de leurs fonctions policières et de leurs activités de sécurité et de renseignement.

Canadiens

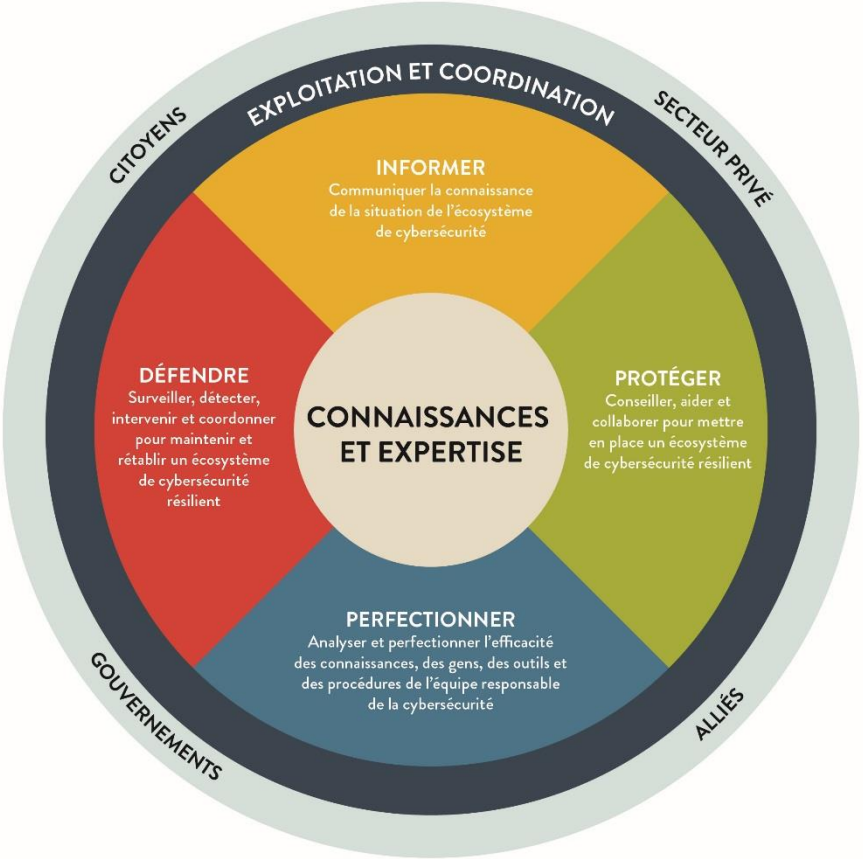
- Nous informons et sensibilisons les Canadiens sur les enjeux de cybersécurité, et nous communiquons avec eux à ce sujet, en leur fournissant des conseils clairs et des pratiques qui sont appuyés par une expertise et des renseignements uniques.

Rôle vital du Centre pour la cybersécurité dans la protection du Canada et des Canadiens

FONCTIONS

Informer le Canada et les Canadiens des questions de cybersécurité, dont les menaces à la cybersécurité.

Défendre les réseaux et les systèmes qui relèvent de sa responsabilité.

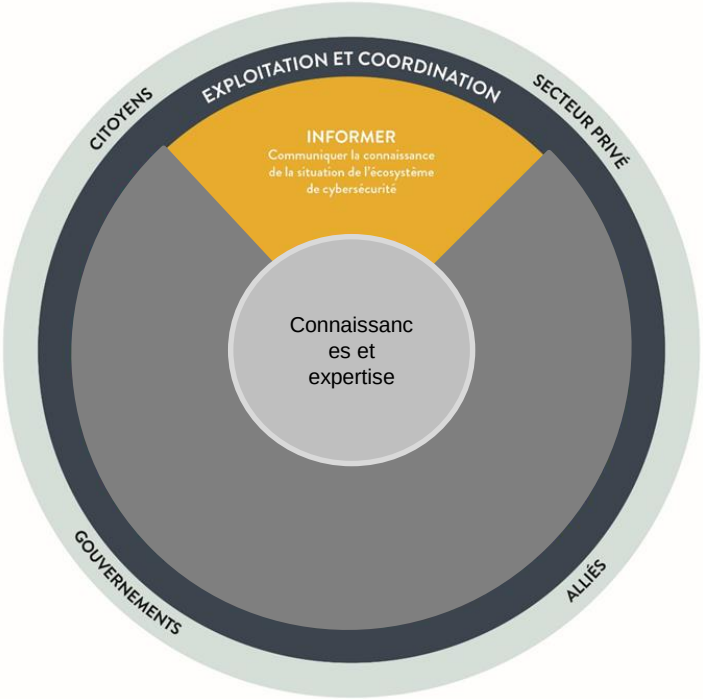


Protéger les intérêts des Canadiens en offrant des conseils et de l'assistance et en collaborant avec ses partenaires à l'échelle du pays et à l'étranger.

Perfectionner les connaissances et compétences voulues et mobiliser le personnel nécessaire pour assurer une amélioration continue de la cybersécurité pour les Canadiens.

Informer

- Campagne de sensibilisation Pensez cybersé
- Avis et conseils techniques
- Évaluation des cybermenaces nationales
- Cyberstabilité et rapports sur les tendances
- Rapports et notifications d’événements de cybersécurité



Campagne Pensez cybersécurité

PENSEZCYBERSECURITE

5 CONSEILS POUR DIRIGER UNE #ENTREPRISECYBERSÉCURITAIRE

Dans chaque entreprise, les employés représentent à la fois le plus grand risque ET la meilleure protection contre la cybercriminalité.

Les connaissances et la formation peuvent faire toute la différence.

Protégez-vous et signalez les escroqueries

Pensez cybersécurité vous offre des conseils pour vous protéger contre les cybermenaces. Mais que devez-vous faire si vous êtes victime d'un cyberincident? Les mesures à prendre dépendront de sa nature

5 façons de protéger votre vie privée sur un nouvel appareil intelligent

Les appareils qui se connectent à Internet (aussi appelés « appareils intelligents ») sont amusants et nous simplifient la vie, mais ils peuvent aussi permettre aux pirates informatiques d'accéder à des renseignements personnels ou confidentiels. Suivez ces conseils pour assurer votre protection et celle de votre entourage.

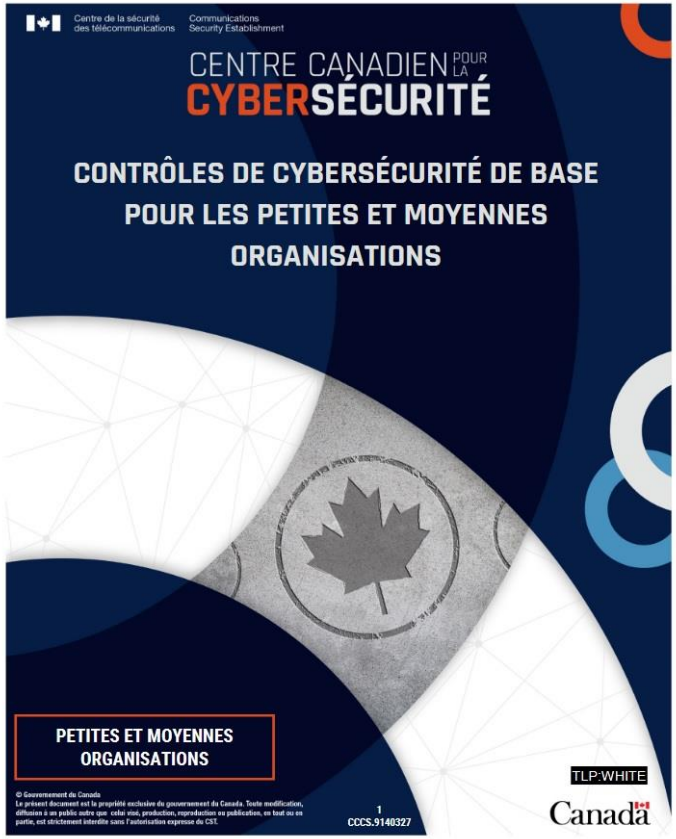
Trois éléments à considérer avant d'acheter un appareil intelligent

Les assistants intelligents, les casques de réalité virtuelle et les montres intelligentes sont parmi les cadeaux les plus convoités en cette période des fêtes. Avant d'acheter un appareil qui se connecte à Internet, renseignez-vous afin de vous protéger, vous et le destinataire de votre cadeau, des cybercriminels.

NON CLASSIFIÉ

Contrôles de cybersécurité de base

- Publication destinée aux petites et moyennes organisations (499 employés et moins)
- Fournit des avis et des conseils sur des pratiques faciles en matière de cybersécurité
- Adaptée de façon à équilibrer les investissements et la cybersécurité



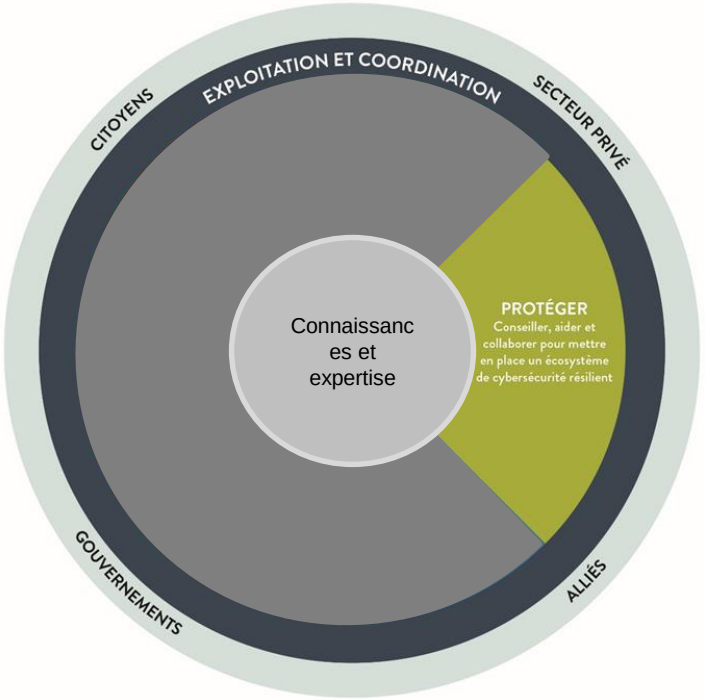
Les 10 mesures du CST

- Ensemble complet de mesures visant à atténuer les cybermenaces et s'appliquant à tous les types d'organisation

- Mesures fondées sur l'analyse des tendances en matière de cybermenaces en vue de contrer les cybermenaces les plus récentes

Protéger

- Assurance des produits
- Programmes d’atténuation des risques
- Soutien des activités de gestion des incidents
- Services d’échange d’information automatisé

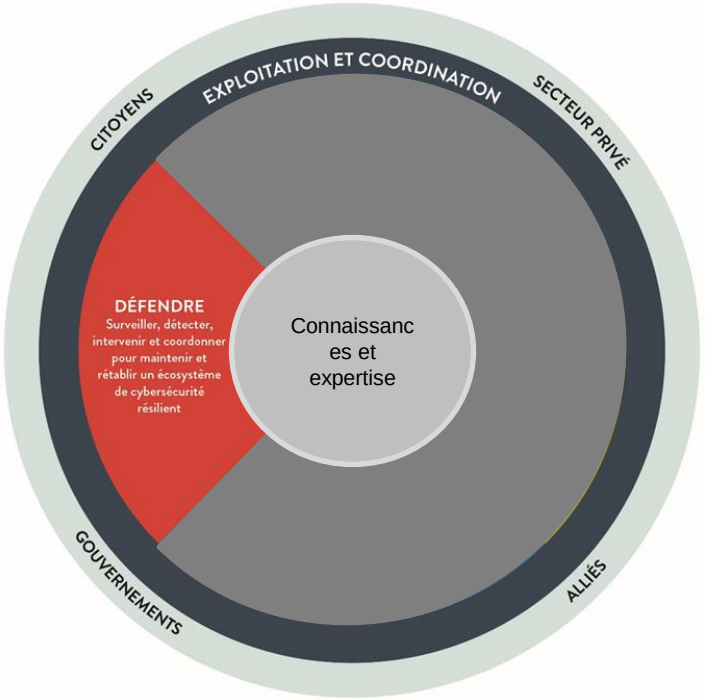


Programme des Critères communs

- Programme international dans le cadre duquel des laboratoires d'essais agréés mettent à l'essai des produits TI en fonction de spécifications standards en matière de cybersécurité que l'on appelle Profils de protection (PP).
  - Ces PP représentent les exigences d'assurance de la sécurité pour des classes de technologie.
- Le Centre pour la cybersécurité gère le Programme canadien lié aux Critères communs qui vise
  à certifier les produits mis à l'essai par les laboratoires d'essais selon les Critères communs canadiens.
  - Les servi

Défendre

- Gestion des opérations de sécurité pour le gouvernement fédéral
- Défense réseau
- Services cryptographiques
- Solutions de communications sécurisées
- Projets collaboratifs de cyberdéfense



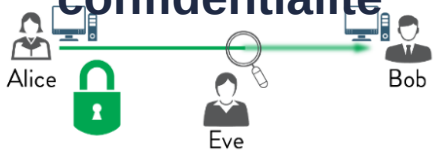
Protection des réseaux du gouvernement du Canada

- Nous avons détecté et confirmé une cyberintrusion perpétrée au moyen de méthodes hautement sophistiquées par une entité parrainée par le gouvernement de la Chine visant les systèmes informatiques du Conseil national de recherche du Canada (CNRC).
- Pour y arriver, nous avons collaboré avec le CNRC, SPC et d'autres partenaires en sécurité des TI du GC.
- Nous avons fait appel à de nombreuses méthodes de cyberdéfense pour assurer le suivi et l'atténuation de cette cyberintrusion.
  - Les leçons apprises dans le cadre de cet incident ont contribué à améliorer et à perfectionner nos outils et techniques.

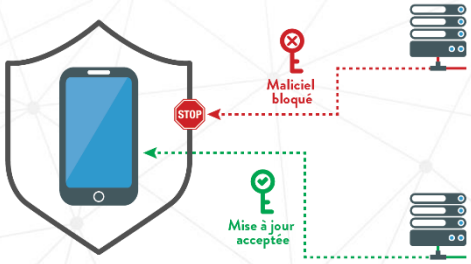
Assembly Line est un outil de source ouverte du Centre pour la cybersécurité qui a été employé lors de la compromission du CNRC.

Une cryptographie robuste est à l'avant-plan de la cyberdéfense

Protéger la confidentialité



Protection contre les cyberattaques



D'ici les années 2030, les ordinateurs quantiques pourraient casser les mesures cryptographiques que nous utilisons aujourd'hui.
En vue de se préparer à ces nouvelles capacités, le Centre pour la cybersécurité :

- mène des recherches visant à évaluer les composants cryptographiques de remplacement;
- participe activement à l'élaboration de nouvelles normes en matière de cryptographie;
- travaille avec le GC pour mettre à jour la cryptographie servant à protéger ses renseignements les plus sensibles;
- collabore avec l'industrie et le milieu universitaire pour créer un plan visant à assurer la cyberprotection du Canada.

Partenariat collaboratif avec la Société indépendante d'exploitation du réseau d'électricité (SIERE)

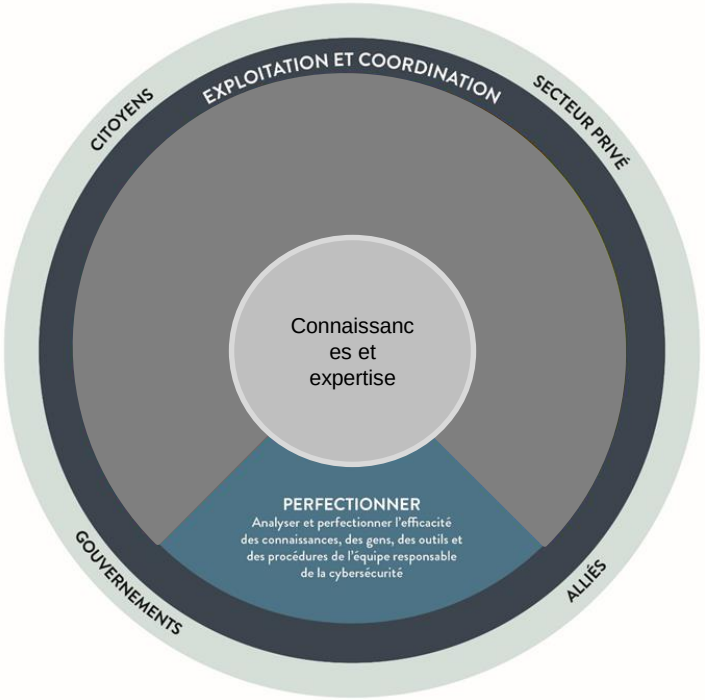
- En plus des échanges en matière d'information et de technologie, le Centre pour la cybersécurité appuiera, au besoin, les activités de prévention, d'établissement et d'intervention en ce qui a trait aux menaces, et il fournira des conseils sur l'évaluation et le signalement des menaces.

- Ce partenariat reflète l'importance de gérer les risques liés à la cybersécurité et d'encourager la collaboration au sein de l'industrie.

- Ce partenariat aidera également la SIERE à gérer les risques liés aux cybermenaces

Perfectionner

- Carrefour de l’apprentissage et de l’innovation
- Événement de collaboration : GeekWeek
- Relations avec le milieu universitaire
- Recherche et développement



Carrefour de l'apprentissage

- Source fiable d'activités et de programmes de pointe en matière d'apprentissage pour les professionnels de la cybersécurité et de la COMSEC qui travaillent
  au sein du gouvernement, de l'industrie et du milieu universitaire.
  - Il propre des services, des avis et des conseils sur la formation et l'éducation en cybersécurité.
- Plus de 30 cours divisés en deux volets :
  - COMSEC
  - Cybersécurité

GeekWeek

- GeekWeek est un événement unique en son genre dans le cadre duquel le gouvernement, l'industrie, le milieu universitaire et les partenaires internationaux en cybersécurité se réunissent en vue d'améliorer et de protéger le cyberespace.
- Cet événement collaboratif souligne l'importance de l'échange d'information entre partenaires pour assurer la réussite des innovations.

- En 2018, plus de 200 personnes ont participé à GeekWeek.
  - GeekWeek a produit plus de 80 nouveaux outils de source ouverte et innovations majeures dans différents domaines
    tels que l'analyse des journaux et du trafic réseau, la détection des maliciels et l'analyse automatisée des maliciels

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

ÉVALUATION DES CYBERMENACES NATIONALES 2018

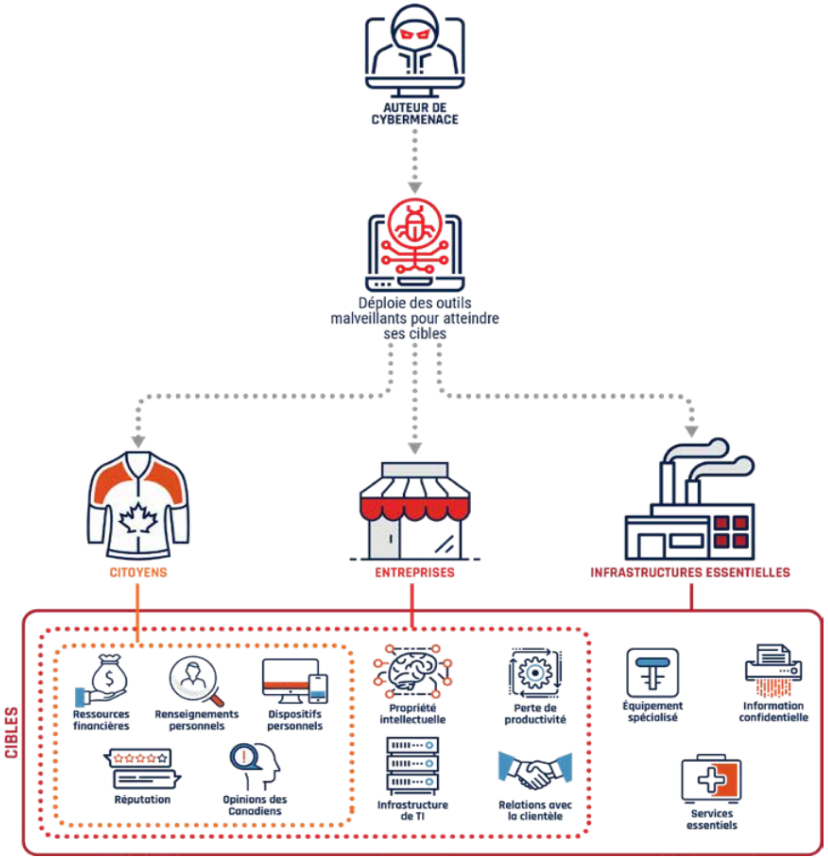
Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Quels risques pèsent sur les réseaux canadiens?

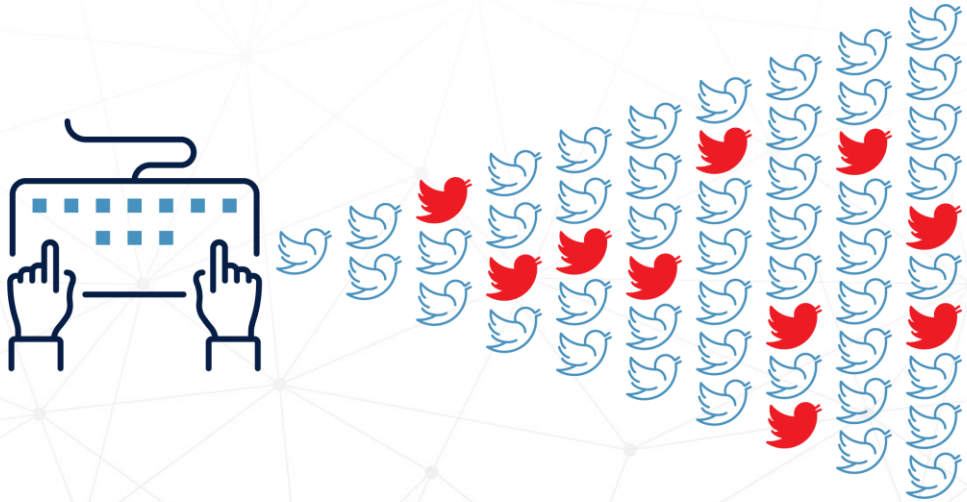
- Les cybermenaces, y compris celles qui proviennent d'hacktivistes, de criminels, de terroristes et d'États étrangers, mettent continuellement à l'épreuve les systèmes pour y déceler des vulnérabilités qui permettront d'accéder aux ordinateurs.

Une fois l'accès obtenu, les auteurs de menace peuvent voler ou altérer l'information, corrompre les opérations ou programmer les ordinateurs pour exploiter d'autres ordinateurs ou systèmes auxquels ils sont connectés.



Cybermenaces contre les Canadiens

Faits saillants



La cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens et les entreprises canadiennes en 2019.

Il est fort probable que les Canadiens fassent l'objet d'activités malveillantes d'influence en ligne en 2019.

Cybermenaces contre les entreprises canadiennes

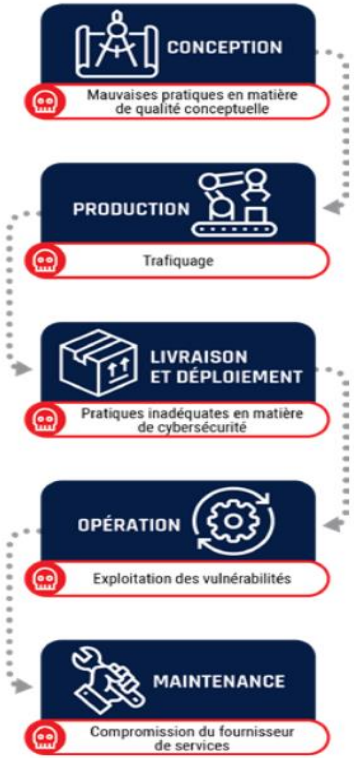
Faits saillants

Les auteurs de cybermenace sophistiqués continueront probablement de tirer parti des relations de confiance entre les entreprises et leurs fournisseurs de services.

Les auteurs de cybermenace – quel que soit leur degré de sophistication – accroîtront l'étendue de leurs activités en vue de voler de grandes quantités de données personnelles et commerciales.

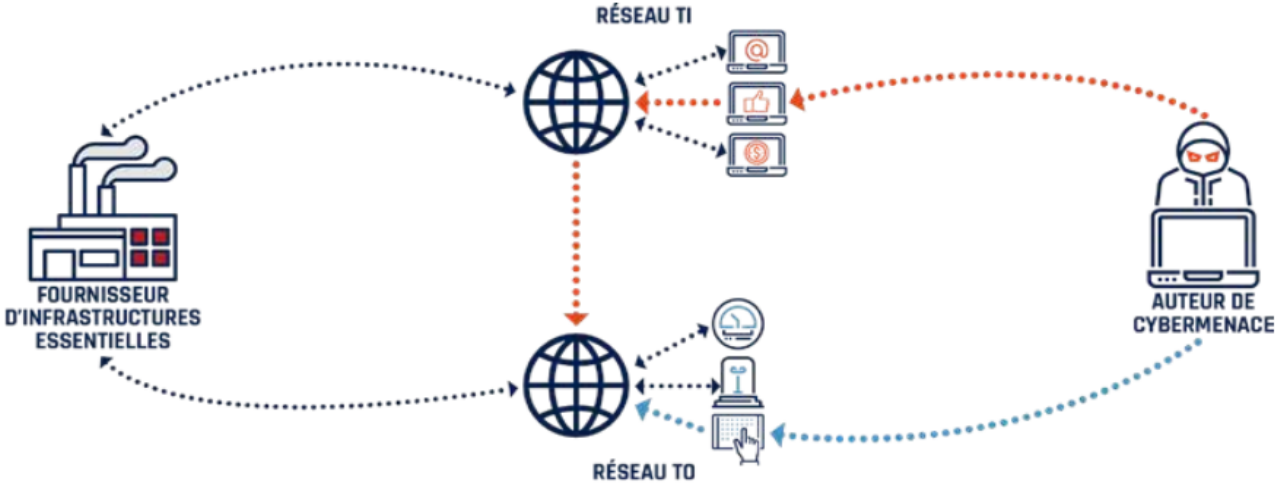
À mesure que la cybersécurité s'améliore, les auteurs de cybermenace adoptent des méthodes plus avancées, comme la compromission des chaînes d'approvisionnement du matériel et des logiciels, ce qui rend le processus de détection et d'attribution plus difficile pour les responsables de la sécurité.

Processus de la chaîne d'approvisionnement



Cybermenaces contre les infrastructures essentielles du Canada

Faits saillants



Il est fort improbable que des auteurs de cybermenace parrainés par des États perturbent volontairement les infrastructures essentielles du Canada s'il n'y a aucun climat d'hostilité à l'échelle internationale.

Les auteurs de cybermenace parrainés par des États continueront de se livrer à des activités de cyberespionnage contre les entreprises et les infrastructures essentielles du Canada s'ils estiment que ces activités profiteront à leurs objectifs stratégiques nationaux.

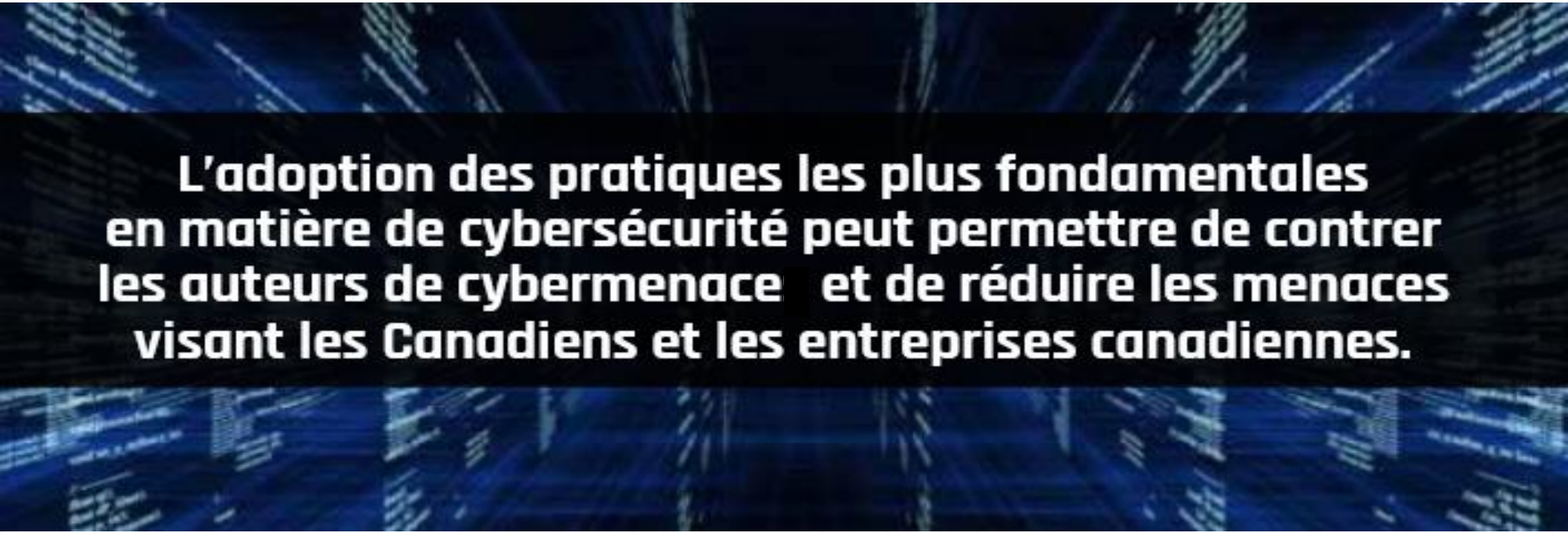
Compromission du secteur de l’énergie

Étude de cas

- En 2017, le Centre de la sécurité des télécommunications a informé ses partenaires des États-Unis de la cybercompromission d’un SCI du secteur de l’énergie.
- Selon les représentants du département de la Sécurité intérieure, les auteurs de cybermenaces russes avaient réussi à atteindre les systèmes sécurisés et les réseaux isolés, s’introduisant à un point tel qu’ils auraient pu interrompre le transit d’énergie en Amérique du Nord.
- Pour compromettre les tierces parties, les auteurs de cybermenaces ont fait appel à des techniques relativement simples, comme des courriels de harponnage.

Principales occasions de protéger votre organisation

- Gouvernance interne
  - La cybersécurité est-elle une priorité continue?
- Investissement
  - Dans quelle mesure consacrez-vous des ressources à la cybersécurité?
- Résilience
  - Dans quelle mesure êtes-vous prêt à faire face à une cyberattaque?
- Chaîne d'approvisionnement
  - Toutes les composantes de votre chaîne d'approvisionnement sont-elles protégées adéquatement contre les cyberattaques?
- Collaboration
  - Travailler avec les spécialistes en cybersécurité commerciale, et tirer parti des avis et des conseils du GC


L'adoption des pratiques les plus fondamentales
en matière de cybersécurité peut permettre de contrer
les auteurs de cybermenace et de réduire les menaces
visant les Canadiens et les entreprises canadiennes.

Gardez un lien avec nous

@cse_cst

contact@cyber.gc.ca

www.cyber.gc.ca

@centrecyber_ca