La mise en œuvre des normes du GEG 2015 par le Canada

Le Canada aimerait communiquer certaines des pratiques exemplaires qu'il a recensées et des leçons qu'il a apprises au sujet de la mise en œuvre des normes volontaires, non contraignantes et précédemment reconnues pour le comportement responsable des États, qui ont été adoptées par l'Assemblée générale des Nations Unies, pour que cela puisse aider d'autres États membres des Nations Unies à appliquer les 11 normes énoncées dans le rapport du GEG 2015.

Norme 1 : Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États devraient coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des TIC et à prévenir les pratiques informatiques jugées nocives qui peuvent compromettre la paix et la sécurité internationales;

Le Canada a pris certaines mesures pour augmenter la stabilité et la sécurité de l'utilisation des TIC et prévenir les pratiques les plus nocives à cet égard. Ces mesures comprennent :

A) La rédaction et la mise à jour de stratégies nationales globales de cybersécurité

La première Stratégie de cybersécurité du Canada a été publiée en octobre 2010 et fournissait un plan pour se défendre contre les cybermenaces. La Stratégie de 2010 reposait sur trois piliers : I) sécuriser les systèmes du gouvernement du Canada; II) nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral; III) aider les Canadiens à se protéger en ligne. La Stratégie de 2010 et les initiatives nationales qu'elle a lancées par son plan d'action connexe ont renforcé la capacité du gouvernement du Canada à prévenir et à détecter les cyberactivités malveillantes, ainsi qu'à y répondre et à s'en remettre. Parmi les résultats obtenus, nous avons poursuivi notre collaboration avec des partenaires dans des infrastructures essentielles, lancé la campagne d'information publique « Pensez cybersécurité » et renforcé les capacités du Centre canadien de réponse aux incidents cybernétiques. La Stratégie a aussi favorisé la collaboration et l'échange d'information, que le Canada considère comme nos meilleurs moyens de défense dans un environnement où les menaces évoluent rapidement.

Conscient de l'évolution du cyberespace, le gouvernement du Canada, sous la direction de Sécurité publique Canada, a publié sa nouvelle Stratégie nationale de cybersécurité (SNCS) le 12 juin 2018 pour consolider ses partenariats en vue de protéger les cybersystèmes essentiels à l'intérieur et à l'extérieur du gouvernement fédéral, de protéger les Canadiens qui utilisent Internet, et d'améliorer la détection des cybermenaces en évolution constante et la capacité d'y répondre. La nouvelle SNCS est organisée en fonction de trois objectifs de haut niveau :

1) *Des systèmes canadiens sécurisés et résilients*

En collaborant avec les partenaires et en améliorant les capacités en matière de cybersécurité, nous pouvons mieux protéger les Canadiens contre la cybercriminalité, contrer les menaces en évolution et défendre les systèmes essentiels du gouvernement et du secteur privé.

2) *Un écosystème du cyberespace novateur et adaptable*

En appuyant la recherche de pointe, en encourageant l'innovation numérique, en perfectionnant les compétences et les connaissances en matière de cybersécurité, le gouvernement fédéral positionnera le Canada comme un chef de file mondial dans le domaine de la cybersécurité.

3) *Leadership, gouvernance et collaboration*

En étroite collaboration avec les provinces, les territoires et le secteur privé, le gouvernement fédéral jouera un rôle de premier plan pour faire progresser la cybersécurité au Canada.

La nouvelle SNCS a été conçue pour être flexible et demeurer pertinente à mesure que l'environnement de la cybersécurité continue à évoluer. De même, ses activités connexes ne représentent pas un stade final, mais plutôt une étape dans la réalisation par le Canada de sa vision à long terme de sécurité à l'ère numérique, à la fois au pays et à l'échelle internationale.

Dans le cadre de cette stratégie, Affaires mondiales Canada collaborera avec les alliés du Canada, les pays qui partagent notre vision et la communauté internationale pour façonner l'environnement international de la cybersécurité en préconisant un Internet libre, ouvert et sûr, ainsi que le respect du droit international et des normes acceptées pour le comportement des États dans le cyberespace.

B) Le développement de nos cybercapacités à mieux nous défendre et à prévenir les cyberactivités malveillantes d'une manière tout à fait transparente

En déployant sa Stratégie nationale de cybersécurité de 2018, le Canada a créé le Centre canadien pour la cybersécurité (CCC), qui regroupe les unités opérationnelles de cybersécurité du gouvernement du Canada en une seule organisation publique. Le Centre est la source unique et unifiée en matière de conseils, d'orientation, de services et de soutien en cybersécurité pour le gouvernement, les propriétaires et exploitants d'infrastructures essentielles, le secteur privé et le public canadien. Plus particulièrement, le CCC permettra au gouvernement d'intervenir plus rapidement et de manière mieux coordonnée et ciblée face aux cybermenaces. Il permettra de transmettre l'information plus rapidement et efficacement entre le gouvernement et les partenaires du secteur privé, et servira de point de contact national où obtenir des avis et des conseils faisant autorité en matière de cybersécurité. De plus, le CCC permettra de mieux sensibiliser et informer le public au sujet de la cybersécurité, améliorera l'information sur la cybersécurité et l'échange de compétences dans le domaine, et fournira des évaluations périodiques des cybermenaces pour mieux éclairer la prise de décisions et guider la politique fédérale dans le domaine. Ce sera un organisme tourné vers l'extérieur qui développera des collaborations et des projets avec des partenaires du secteur canadien de la cybersécurité.

La politique de défense du Canada, publiée le 7 juin 2017, reconnaît la menace croissante que représentent les personnes malveillantes dans le cyberespace. Pour protéger et défendre le Canada, notre politique de défense veut que les Forces armées canadiennes (FAC) développent la capacité de mener des cyberopérations actives centrées sur les menaces extérieures pour le Canada dans le contexte de missions militaires autorisées par le gouvernement. Toutes nos missions sont assujetties à toutes les lois nationales et internationales applicables. La politique de défense de 2017 a aussi annoncé la création de la profession de cyberopérateur dans l'armée pour augmenter la capacité des FAC dans ce domaine.

En juin 2019, la *Loi sur le Centre de la sécurité des télécommunications (CST)* a reçu la sanction royale. Cette loi a donné au CST, l'agence canadienne de renseignement électromagnétique, le pouvoir de mener des cyberopérations actives et défensives pour la première fois. Ce pouvoir est nécessaire pour permettre au Canada de mieux se défendre contre les cybermenaces étrangères avant qu'elles ne puissent endommager les systèmes ou les banques d'information au pays. La loi comprend aussi des exigences et des restrictions claires concernant l'exercice de ce pouvoir.

D'autres partenaires et alliés ont été également transparents sur leurs capacités et les conditions dans lesquelles elles pourraient être utilisées. Comme d'autres, nous considérons cette transparence comme un moyen important d'éviter les fausses perceptions, de réduire les incertitudes et de favoriser la confiance dans le cyberespace.

C) La promotion, au niveau international, de l'applicabilité de la loi internationale et des normes de comportement responsable pour la conduite des divers acteurs dans le cyberespace

Pour contrer les cybermenaces, le Canada a appuyé la reconnaissance de l'applicabilité de la loi internationale dans le cyberespace, l'adoption de normes volontaires pour le comportement responsable des États et l'élaboration de mesures de renforcement de la confiance. Les rapports du GEG de l'ONU de 2013 et 2015 ont reconnu l'applicabilité de la loi internationale et le rapport de 2015 a exposé des normes pour le comportement responsable des États dans le cyberespace. Ces normes ont par la suite été adoptées dans de nombreux forums internationaux, y compris par l'Assemblée générale de l'ONU, le G20 et diverses organisations régionales. Le Canada a adopté ces normes et travaille activement à promouvoir leur mise en œuvre. L'un des moyens que nous avons pris pour ce faire est d'organiser des ateliers pour aider les pays à mieux comprendre ces normes et ce qu'ils peuvent faire pour les appliquer. Avec le Mexique et l'Organisation des États américains (OEA), nous avons coorganisé le 30 mai 2019 un atelier qui ciblait les pays de l'OEA. Un autre atelier similaire ciblant les pays de la Francophonie a été organisé le 6 septembre 2019.

Dans nos soumissions annuelles à l'ONU, comme celle de 2016, et ailleurs, le Canada a affirmé sa position selon laquelle le droit international actuel s'applique à l'utilisation des TIC par les États et qu'il est essentiel pour maintenir la paix et la sécurité, et pour favoriser un environnement des TIC ouvert, sûr, pacifique et accessible. Le droit international pertinent au cyberespace comprend la charte des Nations Unies, le droit sur la responsabilité des États, y compris les contre-mesures, le droit international en matière de droits de l'homme et le droit international humanitaire, s'il y a lieu.

Le Canada a aussi participé au travail du « Internet & Jurisdiction (I&J) Policy Network ». Fondé en 2012, l'I&J rassemble des acteurs internationaux du milieu universitaire, de l'industrie (entreprises Internet, opérateurs techniques), de gouvernements, d'organisations internationales et de groupes de la société civile. Ses membres comptent plus de 200 organisations clés provenant de plus de 40 pays. Le but du réseau I&J est de développer des approches consensuelles des défis posés par la nature transfrontalière d'Internet, dans trois domaines stratégiques principaux : l'action au niveau des domaines, la gestion du contenu offensant et l'application des lois dans l'accès aux données. Le réseau I&J s'est réuni la dernière fois à Berlin en juin 2019, où les discussions furent centrées sur les approches opérationnelles des normes, des critères et des mécanismes dans les trois domaines. Le réseau I&J a aussi rédigé un rapport de la situation mondiale des champs de compétence sur Internet, en tirant profit de l'expertise de plus d'une centaine de ses membres.

D) Le travail du Canada avec les organisations régionales sur la diffusion des MRC dans le cyberespace

Le Canada croit que les mesures de renforcement de la confiance (MRC) sont un outil important pour promouvoir la stabilité et la sécurité dans le cyberespace et y régler les incidents en prévenant les erreurs de jugement et les conflits. Le Canada collabore étroitement avec des organisations régionales comme le Forum régional de l'ANASE, l'Organisation des États américains (OEA) et l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour diffuser et appliquer les MRC dans le cyberespace. Par exemple, le Canada a contribué aux efforts du Forum régional de l'ANASE pour mettre en place de telles MRC dans les pays de l'ANASE en coorganisant avec Singapour en juin 2019 un atelier sur les stratégies nationales pour la sécurité de l'utilisation des TIC. Le Canada a aussi récemment annoncé qu'il dirigera les efforts pour mettre en œuvre la MRC 4 de l'OSCE : « Les États participants échangeront volontairement des informations sur les mesures qu'ils ont prises pour assurer un Internet ouvert, interexploitable, sécurisé et fiable. » Le Canada informera les autres États participant à l'OSCE comment il applique cette MRC et fournira une orientation et des pratiques exemplaires relatives à sa mise en œuvre.

E) Renforcement des capacités liées à la cybersécurité

Le Programme canadien d'aide au renforcement des capacités de lutte contre la criminalité (PARCLC) soutient les efforts internationaux pour combattre la cybercriminalité et les menaces à la cybersécurité. Les projets de ce programme forment une part essentielle de la stratégie de mobilisation du Canada visant à inciter les pays à partager notre vision d'un Internet ouvert, sûr et gouverné par de multiples intervenants. Le programme améliore aussi les capacités des pouvoirs nationaux à décourager les cybermenaces, à y répondre et à mener des enquêtes à leur sujet, y compris relativement à l'exploitation criminelle des TIC. Depuis 2015, le PARCLC a versé plus de 9 M$ au renforcement des capacités en matière de cybersécurité, essentiellement dans les Amériques. Le Canada met actuellement sur pied des programmes par le biais d'organisations internationales comme l'ONUDC, l'OEA et INTERPOL. Les programmes du PARCLC en matière de cybersécurité aident aussi des pays à développer leurs stratégies nationales dans le domaine, ce qui comprend l'élaboration de normes sur la manière d'augmenter la sécurité des TIC, tout en garantissant les droits de l'homme et la vie privée de tous les citoyens.

Norme 2 : En cas d'incident informatique, les États devraient examiner toutes les informations utiles, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans cet environnement, et la nature et l'ampleur des conséquences de l'incident;

A) La Stratégie nationale de cybersécurité du Canada de 2018 a créé un processus simplifié de réponse aux incidents informatiques : jusqu'à récemment, les capacités opérationnelles du gouvernement du Canada en matière de cybersécurité étaient divisées entre plusieurs ministères et organismes. Même si des mesures existaient pour optimiser la communication et la coordination, l'ambiguïté entourant les rôles et les responsabilités ainsi que la difficulté inhérente à la coordination des multiples décideurs constituaient un

obstacle à la prestation de directives techniques rapides, efficaces, claires et fiables que les Canadiens attendent de leur gouvernement. Pour remédier à cette lacune, le gouvernement a créé en octobre 2018 le nouveau Centre canadien pour la cybersécurité (le Cybercentre) en tant que composante du Centre de la sécurité des télécommunications (CST). Le Cybercentre dirige la réponse du Canada aux incidents liés à la cybersécurité en tant qu'équipe d'intervention en cas d'urgence informatique et équipe d'intervention en cas d'incidents de cybersécurité du gouvernement du Canada. Le Cybercentre offre un point de contact unique aux propriétaires et exploitants d'infrastructures vitales, qui peuvent y trouver des conseils et de l'orientation en cas de cyberincident.

La Stratégie nationale de cybersécurité de 2018 comprend aussi le financement de la nouvelle Unité nationale de coordination de la lutte contre la cybercriminalité (UNCLC). Bien que gérée par la Gendarmerie royale du Canada (GRC), l'UNCLC servira toutes les forces de police canadiennes et collaborera avec les partenaires des secteurs public et privé. L'UNCLC coordonnera les enquêtes sur la cybercriminalité touchant plusieurs champs de compétence au Canada et à l'étranger et résoudra les conflits associés, en plus de mettre en place un nouveau système de signalement public pour que les victimes canadiennes puissent plus facilement signaler les cybercrimes aux forces de l'ordre. L'UNCLC collaborera étroitement avec le Cybercentre pour contrer les cybermenaces. L'UNCLC pourra entrer en activité d'ici avril 2020, et le nouveau système de signalement public est prévu pour 2022.

B) Le Canada a participé à l'attribution publique d'activités qu'il juge être des comportements d'État inacceptables. Dans son processus d'attribution, le Canada considère le contexte plus large de l'événement, les problèmes que pose l'attribution dans le contexte des TIC, le droit international pertinent et les normes volontaires, ainsi que la nature et la portée des conséquences de l'incident.

C) Par le renforcement international des capacités en cybersécurité, le Canada a aidé des pays à mettre sur pied ou à améliorer leur équipe d'intervention en cas d'incident de sécurité informatique (EIISI), ce qui leur permet de diffuser en temps réel l'information sur les cyberincidents, y compris la mauvaise utilisation des TIC. Le Canada collabore aussi avec les forces de police et les systèmes judiciaires de pays étrangers pour augmenter leur capacité en matière d'expertise judiciaire et d'enquête informatique, d'attribution des crimes et de poursuite des personnes qui utilisent les TIC à des fins de crimes ou d'exploitation.

Norme 3 : Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications;

Le Canada considère que les États ont la responsabilité de s'assurer que leur territoire n'est pas utilisé d'une manière qui porte atteinte aux droits des autres États. Si le Canada est informé d'incidents sur son territoire, il prendra les mesures appropriées pour empêcher le comportement nuisible. De plus, pour s'assurer que son territoire n'est pas utilisé pour commettre des faits internationalement illicites, le Canada a :

A) Adopté des lois pour poursuivre les cybercriminels : le *Code criminel* du Canada inclut un certain nombre d'infractions qui peuvent concerner les actions des cybercriminels, et des outils qui peuvent être utiles pour enquêter sur leurs activités. Cela comprend les ordonnances de communication et de conservation, utilisées pour s'assurer que les preuves ne sont pas supprimées avant que les enquêteurs puissent y avoir accès. Une infraction importante à cet égard se trouve à l'article 342.1 Utilisation non autorisée d'ordinateur, qui stipule :

« Est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire, quiconque, frauduleusement et sans apparence de droit :

a) directement ou indirectement, obtient des services d'ordinateur;
b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;
c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue aux alinéas a) ou b) ou à l'article 430 concernant des données informatiques ou un ordinateur;
d) a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas a), b) ou c), ou en fait le trafic ou permet à une autre personne de l'utiliser. »

La possession d'un dispositif permettant l'utilisation non autorisée d'un ordinateur ou la commission d'un méfait est aussi criminalisée à l'article 342.2.

Une autre infraction pertinente dans ce contexte est décrite à l'article 430(1.1) Méfait à l'égard de données informatiques, qui stipule :

« Commet un méfait quiconque volontairement, selon le cas :

a) détruit ou modifie des données informatiques;
b) dépouille des données informatiques de leur sens, les rend inutiles ou inopérantes;
c) empêche, interrompt ou gêne l'emploi légitime des données informatiques;
d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données informatiques ou refuse l'accès aux données informatiques à une personne qui y a droit. »

La peine encourue pour cette infraction est précisée aux paragraphes 430(5) et (5.1), qui stipulent :

« (5) Quiconque commet un méfait à l'égard de données informatiques est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de dix ans;
b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

(5.1) Quiconque volontairement accomplit un acte ou volontairement omet d'accomplir un acte qu'il a le devoir d'accomplir, si cet acte ou cette omission est susceptible de constituer un méfait qui cause un danger réel pour la vie des gens ou de constituer un méfait à l'égard de biens ou de données informatiques est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de cinq ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire. »

B) Poursuivi des cybercriminels : la GRC a enquêté sur plusieurs cybercriminels et les a poursuivis avec succès. Par exemple, une enquête de la GRC sur leakedsource.com a récemment débouché sur un plaidoyer de culpabilité par un Ontarien de 27 ans qui a vendu un grand nombre de mots de passe en ligne au moyen du site leakedsource.com, maintenant fermé.

Autre exemple datant de 2018 : Karim Baratov a été arrêté au Canada en lien avec une atteinte à la sécurité à Yahoo. La GRC et le FBI ont enquêté sur cet individu et il a été condamné aux États-Unis à cinq ans de prison et à une amende de 250 000 $ US. Plusieurs autres cas de cybercriminalité sont actuellement jugés par des tribunaux canadiens.

C) Encouragé la correction de vulnérabilités : le Cybercentre publie régulièrement des alertes et des avis lorsque des cybermenaces, des vulnérabilités ou des incidents possibles, imminents ou réels touchent ou pourraient toucher les infrastructures essentielles du Canada.

D) Renforcé les capacités : par le biais d'organisations internationales comme l'ONUDC, INTERPOL, le Conseil de l'Europe et l'OEA, le Canada aide des pays à développer leur cadre légal portant sur la cybercriminalité et la capacité de leurs institutions judiciaires et policières à combattre la cybercriminalité et à contrer l'abus et l'exploitation de leurs citoyens par les nouvelles technologies de l'information. Cela améliore aussi grandement leur capacité à mener efficacement des enquêtes sur les cybercriminels et à les poursuivre d'une manière qui respecte les normes internationales et les droits de l'homme.

Norme 4 : Les États devraient réfléchir à la meilleure façon de coopérer pour échanger des informations, s'assister mutuellement, engager des poursuites en cas d'utilisation terroriste ou criminelle des technologies de l'information et des communications et appliquer d'autres mesures collectives afin de parer à ces risques; à cet égard, les États peuvent être amenés à déterminer si de nouvelles mesures doivent être élaborées;

Le Canada a élaboré un ensemble de mesures pour augmenter sa coopération avec ses partenaires afin de prévenir l'utilisation criminelle ou terroriste des TIC, comme :

A) L'adoption et la promotion de la Convention de Budapest :
Le principal instrument international qui traite spécifiquement de la cybercriminalité est la Convention sur la cybercriminalité du Conseil de l'Europe, que le Canada a signée en 2001. Aussi nommée Convention de Budapest, elle propose des lignes directrices pour élaborer une législation nationale complète en matière de cybercriminalité, mais aussi un cadre pour la coopération internationale entre les États. Après l'adoption de la *Loi sur la protection des Canadiens contre la cybercriminalité,* le Canada a ratifié la Convention de Budapest le 8 juillet 2015 et elle est entrée en vigueur au Canada le 1er novembre 2015. La Convention aide le Canada et les États parties à combattre les crimes contre l'intégrité, la disponibilité et la confidentialité des systèmes informatiques et des réseaux de télécommunications. Elle aide aussi à lutter contre toute activité criminelle qui laisse des traces électroniques. Depuis que le Canada a ratifié la Convention de Budapest, la GRC répond à un nombre important de demandes venant d'autres États dans le cadre de la Convention. Le Canada appuie fermement la Convention de Budapest, qu'il considère comme le meilleur outil pour lutter contre la cybercriminalité à l'échelle internationale. Le Canada encourage les pays à accroître leurs efforts pour lutter contre la cybercriminalité en devenant parties à la Convention, ou en s'en inspirant pour adopter des lois nationales contre la cybercriminalité.

Le Canada participe activement au travail du Conseil de l'Europe pour rédiger un protocole additionnel à la Convention de Budapest afin d'augmenter la coopération entre les forces de l'ordre et les pouvoirs judiciaires au niveau international, y compris dans le domaine de l'accès aux preuves électroniques. De plus, à la suggestion du Canada, le Quintette des procureurs généraux (qui réunit les procureurs généraux du Canada, des États-Unis, de l'Australie, de la Nouvelle-Zélande et du Royaume-Uni) a publié une déclaration à sa réunion du 31 juillet 2019 pour exprimer son soutien à la Convention de Budapest comme outil mondial efficace de lutte contre la cybercriminalité et au travail fait actuellement par le groupe d'experts intergouvernemental à composition non limitée des Nations Unies sur la cybercriminalité (UNIEG).

B) La promotion de l'adoption d'une résolution provisoire sur la cybercriminalité : lors de la 28e session de la Commission des Nations Unies pour la prévention du crime et la justice pénale en mai 2019, le Canada a présenté, avec le soutien de l'Autriche, un projet de résolution sur la cybercriminalité, en soulignant l'importance de l'aide technique dans ce contexte. La résolution a été adoptée par consensus et renvoyée devant l'Assemblée générale des Nations Unies.

C) Le renforcement des capacités : depuis 2015, le Canada a investi plus de 9,1 M$ dans le renforcement des capacités en matière de cybersécurité, essentiellement dans les Amériques. Les programmes de cette nature relèvent du mandat du PARCLC d'Affaires mondiales. Les programmes internationaux actuels du Canada sur la cybercriminalité sont offerts par l'entremise de plusieurs partenaires internationaux, dont l'OEA, INTERPOL et l'Office des Nations Unies contre la drogue et le crime (ONUDC).

Par son partenariat avec l'OEA sur des projets de renforcement des capacités en matière de cybersécurité, le Canada veut encourager les États à ratifier la Convention de Budapest en les aidant à élaborer leurs propres stratégies nationales de cybersécurité pour respecter les normes de ratification de la Convention. Ces projets aident aussi à former ou à améliorer les équipes d'intervention en cas d'incident de sécurité informatique (EIISI) dans les Amériques. Grâce au financement du Canada, l'OEA a été capable de lancer le site Web CSIRTAmericas.org, qui sert de plateforme centralisée où toutes les EIISI peuvent échanger de l'information et développer des réponses coordonnées à la cybercriminalité et aux menaces à la cybersécurité.

D) Au Sommet du G7 à Charlevoix en juin 2018, les dirigeants ont annoncé la création du **Mécanisme de réponse rapide (MRR)**. Le MRR a pour mandat de coordonner les efforts au sein du G7 afin de cerner les menaces diverses et changeantes qui pèsent sur nos démocraties, et d'y réagir, notamment en échangeant de l'information et des analyses, ainsi qu'en recensant les possibilités de réponse coordonnée. Le MRR vise à contrer un large éventail de menaces pour la démocratie. Les exemples illustratifs cités par les ministres à leur réunion d'avril 2018 à Toronto ont été regroupés sous trois rubriques : 1) institutions et processus, 2) désinformation et médias, et 3) libertés fondamentales et droits de l'homme. Le MRR est composé des points de convergence des membres du G7 et de l'UE chargés de mettre en œuvre la Déclaration d'engagement de Charlevoix. Chaque point de convergence est en mesure de tirer parti de ses propres structures et processus nationaux ou institutionnels. Le Canada coordonne le MRR de façon continue. Afin de rendre le MRR opérationnel et d'assurer son bon fonctionnement, l'Unité de coordination du MRR a été créée à Affaires mondiales Canada. Bien que le MRR soit une entité du G7, il est aussi en relation avec d'autres pays

alliés et partenaires partageant nos intérêts et notre expertise en vue de protéger la démocratie des menaces étrangères. Récemment, l'Australie, la Lituanie, les Pays-Bas et la Nouvelle-Zélande ont été inclus dans le réseau d'échange d'information du MRR. Ce réseau regroupe aussi plus de 100 experts qui représentent des groupes de réflexion, des établissements universitaires et des organisations multilatérales.

E) Le *Code criminel* du Canada contient certaines infractions et certains outils d'enquête qui concernent l'utilisation criminelle d'Internet, y compris à des fins terroristes :

Le *Code criminel* du Canada contient certaines infractions de terrorisme, qui sont conçues essentiellement pour prévenir les activités terroristes. Par exemple, le *Code criminel* contient une infraction consistant à participer sciemment à une activité d'un groupe terroriste, ou à y contribuer, directement ou non, dans le but d'accroître la capacité de tout groupe terroriste de se livrer à une activité terroriste ou de la faciliter (article 83.18).

Les articles 22 et 464 du *Code criminel* sont des infractions générales de conseil qui peuvent concerner le conseil d'infractions de terrorisme et d'autres infractions. Le conseil désigne l'encouragement visant à amener ou à inciter quelqu'un (paragraphe 22(3)). De plus, il y a l'infraction précise de terrorisme à l'article 83.221, qui consiste à conseiller à quelqu'un de perpétrer une infraction de terrorisme en général, sans en préciser une en particulier. Une personne peut être déclarée coupable, qu'une infraction de terrorisme ait été commise ou non par la personne conseillée. Les définitions d'« activité terroriste » et d'« infraction de terrorisme » dans le *Code criminel* incluent expressément le conseil.

Par ailleurs, l'article 320.1 permet à un juge d'ordonner la suppression de propagande haineuse qui est emmagasinée et rendue accessible au public au moyen d'un ordinateur situé dans le ressort du tribunal. En outre, l'article 83.223 permet à un juge d'ordonner la suppression de propagande terroriste qui est emmagasinée et rendue accessible au public au moyen d'un ordinateur situé dans le ressort du tribunal. La « propagande haineuse » et la « propagande terroriste » sont des termes définis dans le *Code criminel* (paragraphes 320(8) et 83.222(8)). Le *Code criminel* accorde des pouvoirs semblables de retirer du contenu offensant de l'Internet, notamment des contenus sexuels prohibés comme la pornographie juvénile et les enregistrements voyeuristes à l'article 164.1 et la propagande haineuse à l'article 320.1, tel que mentionné précédemment.

Le Canada est aussi capable de coopérer avec d'autres États et possède un cadre légal portant précisément sur cette coopération (*Loi sur l'entraide juridique en matière criminelle*).

F) La mise en place de partenariats solides au niveau technique :

Le Cybercentre a noué des partenariats solides avec d'autres organisations dans le gouvernement du Canada, le secteur privé et sur la scène internationale. Au sein du gouvernement du Canada, le Cybercentre fournit une expertise en cybersécurité pour aider les organismes responsables à s'acquitter de leurs fonctions de base, notamment en collaborant avec la GRC pour lutter contre la cybercriminalité. Le Cybercentre a aussi établi des partenariats au niveau technique avec les propriétaires et les exploitants d'infrastructures essentielles au Canada pour échanger une meilleure information sur les cybermenaces et promouvoir l'intégration de la technologie de cyberdéfense. Enfin, le Cybercentre collabore étroitement avec ses équivalents étrangers et d'autres équipes d'intervention en cas d'incidents de cybersécurité et équipes d'intervention en cas d'urgence informatique.

G) Le travail du Canada avec les organisations régionales sur les MRC dans le cyberespace aide aussi à conclure des partenariats au niveau technique. Par exemple, le Canada a participé à plusieurs exercices de l'OSCE qui ont utilisé les MRC pour échanger de l'information entre les points de contact des États participants (aux plans technique et politique) durant des cybercrises simulées. Ces points de contacts pourraient être utilisés pour désamorcer des crises réelles en permettant aux équipes d'intervention en cas d'urgence informatique, aux ministères de l'Intérieur et des Affaires étrangères, et aux points de contact techniques pertinents de communiquer rapidement pendant un vrai cyberincident.

Norme 5 : Les États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression;

A) La position du Canada sur les droits de l'homme et la vie privée en ligne : le Canada croit que la sécurité des TIC doit aller de pair avec le respect des droits de l'homme et des libertés fondamentales. Les mêmes droits que les personnes ont et exercent hors ligne doivent être respectés en ligne, y compris la liberté d'expression et le droit à la protection des renseignements personnels. Tous les États doivent s'acquitter de leurs obligations internationales en matière de droits de l'homme dans le cyberespace. Ils doivent aussi respecter les engagements qu'ils ont pris à cet égard au Conseil des droits de l'homme et à l'Assemblée générale.

B) La protection des droits de l'homme au Canada est fondée sur un système de gouvernement représentatif et responsable, des garanties constitutionnelles, le droit législatif, y compris une législation spécialisée dans les droits de l'homme, la common law et une magistrature indépendante. La protection des droits de l'homme incombe aux organes législatif, exécutif et judiciaire du gouvernement, à tous les ordres du gouvernement au Canada. Les lois pertinentes sont promulguées par le Parlement et les assemblées législatives provinciales et territoriales. De nombreux ministères et organismes œuvrent au sein du pouvoir exécutif à la formulation de politiques et de programmes qui tiennent compte des obligations du Canada en matière de droits de l'homme dans leur travail.

Le Canada a adhéré aux traités des Nations Unies sur les droits de l'homme et aux protocoles facultatifs, dont le Pacte international relatif aux droits civils et politiques (PIDCP) et le Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC).

La Constitution du Canada comprend la *Charte canadienne des droits et libertés*, qui garantit les libertés fondamentales de conscience et de religion, de pensée, de croyance, d'opinion et d'expression (y compris la liberté de la presse et des autres médias), de réunion pacifique et d'association; les droits démocratiques; le droit de circuler librement; le droit à la vie, à la liberté et à la sécurité de la personne, et le droit de ne pas en être privé sauf en conformité avec les principes de justice fondamentale; divers droits relatifs à la procédure judiciaire, y compris le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives; le droit à l'égalité devant la loi et le droit à la même protection et au même bénéfice de la loi, indépendamment de toute discrimination; la reconnaissance du français et de l'anglais comme les deux langues officielles du Canada; et les droits à l'instruction dans la langue de la minorité.

Tous les gouvernements du Canada ont adopté des lois interdisant la discrimination par le gouvernement ou le secteur privé pour divers motifs dans les domaines de l'emploi, de la fourniture de biens, de la prestation de services et de l'accès à des installations et logements généralement accessibles au public. Des lois sur la liberté d'information et la vie privée existent aux niveaux provincial ou territorial et fédéral pour protéger le droit des personnes à la vie privée (la *Loi sur la protection des renseignements personnels* pour le secteur public et la *Loi sur la protection des renseignements personnels et les documents électroniques* pour le secteur privé) et assurer un droit d'accès à l'information qui est confié au gouvernement ou contrôlé par lui.

C) Par des projets de renforcement des capacités en matière de cybersécurité financés par le Canada, les considérations liées aux droits de l'homme sont toujours intégrées de diverses manières, notamment en encourageant les gouvernements bénéficiaires à inclure les groupes de défense des droits de l'homme de la société civile dans les processus qui mènent à l'élaboration des stratégies de cybersécurité; en invitant la Commission interaméricaine des droits de l'homme (CIDH) et son rapporteur spécial sur la liberté d'expression à fournir une expertise pour les activités de projet pertinentes; en invitant des groupes de défense des droits de l'homme de la société civile à participer à des événements régionaux parrainés par des projets et en encourageant les discussions sur les droits de l'homme et la cybersécurité par des activités de sensibilisation.

Norme 6 : Un État ne devrait pas mener ou soutenir sciemment une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement

une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle pour fournir des services au public;

Le gouvernement du Canada a clairement fait savoir que toute cyberopération de sa part sera menée en pleine conformité avec le droit international. Par exemple, la Stratégie de défense du Canada de 2017 précisait que « les cyberopérations seront soumises à toutes les lois nationales applicables, au droit international et aux garde-fous éprouvés tels que les règles d'engagement, le ciblage et les estimations des dommages collatéraux. »

Norme 7 : Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies de l'information et des communications en tenant compte de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions pertinentes;

A) Tel qu'il est précisé dans le plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada, les mesures suivantes ont été prises depuis 2001 pour protéger les infrastructures essentielles du Canada des menaces relatives aux TIC :

Mesure	**Échéancier**	**Produit livrable**	**État**
Élaborer un nouveau processus de coordination de l'intervention à l'échelle nationale en cas d'incident cybernétique majeur.	Début : 2012	Élaborer un Cadre de gestion des incidents cybernétiques.	
Mettre à profit les propriétaires et exploitants des infrastructures essentielles du Canada au moyen des mécanismes établis dans le cadre de la Stratégie nationale et du plan d'action sur les infrastructures essentielles.	Début : 2010	Fournir des séances d'information sur la cybersécurité à tous les réseaux sectoriels.	En cours
	Début : 2013	Élaborer et mettre en œuvre une stratégie visant à mobiliser les premiers dirigeants dans le domaine de la cybersécurité.	
Mobiliser les provinces et les territoires afin qu'ils participent activement à l'amélioration de la cybersécurité de leurs systèmes et des systèmes essentiels qui relèvent de leur compétence.	Début : 2011	Créer un Comité des sous-ministres adjoints fédéraux, provinciaux, territoriaux sur la cybersécurité.	Terminé
		Obtenir des habilitations de sécurité pour le Sous-comité des dirigeants principaux de l'information sur la protection de l'information auquel participent des représentants des provinces et des municipalités, et fournir à ces personnes des séances d'information classifiées.	Terminé

		Élaborer et mettre en œuvre des arrangements et des protocoles d'échange de l'information.	En cours
	Début : 2001	Diriger un Comité de coordination fédéral, provincial, territorial du Groupe de travail des cadres supérieurs sur la cybercriminalité.	En cours
Élaborer un Programme de partenariat en matière de cybersécurité pour les cybersystèmes essentiels à l'extérieur du gouvernement fédéral afin d'offrir un soutien concret à leurs propriétaires et exploitants.	Début : 2010	Organiser des ateliers partout au pays pour accroître la connaissance et la compréhension des menaces contre les systèmes de contrôle industriel.	En cours
		Établir un programme et un environnement de mise à l'essai pour les systèmes de contrôle industriel – le Centre d'essai national sur l'infrastructure énergétique.	Terminé
		Assurer le fonctionnement du programme et de l'environnement de mise à l'essai des systèmes de contrôle industriel.	En cours
		Élaborer et mettre en œuvre un programme de subvention et de contribution.	
		Concevoir et mettre en œuvre d'autres éléments de programme en consultation avec les propriétaires et les exploitants des systèmes essentiels.	En cours

B) La Stratégie nationale de cybersécurité du Canada de 2018 vise à protéger davantage les infrastructures essentielles du pays des menaces relatives aux TIC. Le budget de 2018 a affecté 507,7 M$ sur cinq ans et 108,8 M$ par année par la suite pour la mise en œuvre de la Stratégie, ce qui représente le plus gros investissement du gouvernement du Canada dans la cybersécurité jusqu'à présent. Ces fonds soutiennent 14 initiatives en cours menées par huit ministères fédéraux, qui sont détaillées dans le nouveau Plan d'action national en matière de cybersécurité, publié en août 2019. Le Plan d'action fournit un plan pour la mise en œuvre de la Stratégie et inclut des échéances et des jalons précis, propres à chaque initiative (voir les tableaux ci-dessous).

INITIATIVE	MINISTÈRE	ACTION/JALON	DATE DE FIN CIBLÉE	ÉTAT
Objectif 1 : Des systèmes sécurisés et résilients				
Appui aux propriétaires et exploitants canadiens d'infrastructures essentielles	Sécurité publique Canada (SP)	Acquérir ou créer un outil technique de cyberévaluation	2019	Prévu
		Établir un comité consultatif sur les systèmes de contrôle industriel (SCI)	2019	Terminé
		Accroître le nombre d'exercices de cybersécurité offerts aux intervenants en	2020	Prévu

		infrastructures essentielles		
		Élaborer une solution technique de formation et de sensibilisation à la sécurité des SCI	2020	Prévu
Évaluation intégrée des menaces améliorée	Centre de la sécurité des télécommunications (CST)	Accroître la capacité pour permettre au CST de mieux répondre à la demande croissante d'évaluations des cybermenaces	2024	En cours
		Accroître la capacité pour permettre au CST d'évaluer un plus large éventail de cybermenaces tenant compte de la clientèle croissante du Cybercentre	2024	En cours
Préparer les communications gouvernementales aux progrès de l'informatique quantique	Centre de la sécurité des télécommunications (CST)	Protéger les renseignements classifiés du gouvernement du Canada contre les progrès anticipés de l'informatique quantique	2024	En cours
Étendre la portée des conseils et des directives aux secteurs des finances et de l'énergie	Centre de la sécurité des télécommunications (CST)	Les secteurs des finances et de l'énergie travaillent en collaboration avec le Cybercentre et à l'intérieur de leur secteur respectif pour améliorer leur niveau de cybersécurité	2024	En cours
		Élever le niveau de cybersécurité dans les secteurs des finances et de l'énergie	2024	En cours
Collecte de renseignements cybernétiques et évaluation des cybermenaces	Service canadien du renseignement de sécurité (SCRS)	Accroître la collecte de cyberrenseignements sur la sécurité nationale et l'évaluation des cybermenaces par le SCRS	2023	Prévu
Unité nationale de coordination de la lutte contre la cybercriminalité (UNCLC)	Gendarmerie royale du Canada (GRC)	Atteindre la capacité opérationnelle initiale	2020	En cours
		Créer le groupe consultatif de l'UNCLC	2021	En cours
		Lancer un système national de signalement public de cybercrimes et de cyberfraudes	2022	En cours
		Atteindre la capacité opérationnelle totale	2023	En cours
Capacité d'application de la loi par la police fédérale en matière de cybercriminalité	Gendarmerie royale du Canada (GRC)	Déployer des cyberspécialistes à l'étranger	2020	En cours
		Établir et appuyer des équipes d'enquête sur la cybercriminalité	2021	En cours
		Recruter et former des spécialistes de la cybercapacité	2021	En cours

INITIATIVE	**MINISTÈRE**	**ACTION/JALON**	**DATE DE FIN CIBLÉE**	**ÉTAT**
Objectif 2 : Un écosystème du cyberespace novateur et adaptable				
Programme de stages pratiques en cybersécurité	Emploi et Développement social Canada	Lancement du Programme d'apprentissage intégré en milieu de travail pour étudiants	2018	Terminé

pour étudiants	(EDSC)	Fin et évaluation du Programme d'apprentissage intégré en milieu de travail pour étudiants	2021	Prévu
Évaluation et certification en cybersécurité pour les petites et moyennes entreprises	Innovation, Sciences et Développement économique (ISDE) en collaboration avec le CST et le CCN	Élaboration de contrôles de sécurité en collaboration avec le CST	2019	Terminé
		Lancement d'un outil d'éducation et de sensibilisation à la cybersécurité	2019	En cours
		Lancement d'un programme de cybercertification	2019	En cours
		Lancement d'une norme nationale sur la cybersécurité	2020	Prévu

INITIATIVE	MINISTÈRE	ACTION/JALON	DATE DE FIN CIBLÉE	ÉTAT
Objectif 3 : Leadership, gouvernance et collaboration efficaces				
Capacité en matière de politiques stratégiques sur la cybersécurité et la cybercriminalité	Sécurité publique Canada (SP)	Recruter une équipe de stratèges politiques	2022	En cours
		Procéder à un examen annuel de l'état d'avancement	2021-2024	Prévu
		Procéder à un examen de la gouvernance	2021	Prévu
Programme de coopération en matière de cybersécurité (PCCS)	Sécurité publique Canada (SP)	Procéder au lancement du PCCS renouvelé	2019	Prévu
		Effectuer le marketing du programme	2019	Prévu
		Lancer l'appel de propositions	2019	Prévu
		Décaisser les fonds du projet	2019	Prévu
Centre canadien pour la cybersécurité	Centre de la sécurité des télécommunications (CST)	Procéder au lancement virtuel du Centre canadien pour la cybersécurité (le Cybercentre)	2018	Terminé
		Atteindre la capacité opérationnelle de base	2022	En cours
		Atteindre la capacité opérationnelle totale	2023	En cours
Cadre stratégique international pour le cyberespace	Affaires mondiales Canada (AMC)	Procéder au lancement d'un groupe de travail international sur la cybercollaboration	2018	Terminé
		Créer une unité cybernétique à Affaires mondiales Canada	2019	Terminé
		Élaborer une cyberstratégie internationale	2019	En cours
		Travailler au renforcement des capacités liées à la cybersécurité	2019	En cours
		Élaborer une politique d'attribution	2019	Terminé
		Pourvoir le poste à la mission de Washington	2020	Terminé
		Tenir des réunions pertinentes sur la cybersécurité	2024	En cours
		Soutenir les participants internationaux dans les négociations en cybersécurité	2024	En cours
		Promouvoir les valeurs et les intérêts canadiens en ce qui a trait aux enjeux liés au cyberespace dans les instances internationales	2024	En cours
Collaboration bilatérale sur la cybersécurité et l'énergie	Ressources naturelles Canada (RNCan)	Recruter du personnel de base pour l'équipe de collaboration bilatérale	2019	En cours
		Lancer un premier appel de déclarations d'intérêt et de propositions de projets	2019	Terminé
		Signer des accords de contribution et décaisser des fonds pour les projets de première ronde	2019	En cours
		Lancer un deuxième appel de déclarations d'intérêt et de propositions de projets (le cas échéant)	2020	Prévu
		Signer des accords de contribution et décaisser des fonds pour les projets de deuxième ronde (le cas échéant)	2020	Prévu

		Participer à des activités clés d'échange de renseignements, à des ateliers et à des séances d'information avec le gouvernement des États-Unis	2023	En cours
		Faire progresser des initiatives conjointes avec les partenaires américains sur la cybersécurité et l'énergie (p. ex. exercices de simulation, R. et D., échange de renseignements)	2023	En cours

C) En plus des initiatives financées dans le cadre de la Stratégie, **le budget de 2019 a aussi affecté 144,9 M$ au renforcement de la cybersécurité des infrastructures essentielles du Canada**, dans le but précis de protéger les cybersystèmes essentiels dans les secteurs des finances, des télécommunications, de l'énergie et des transports. Une somme additionnelle de 80 M$ a aussi été accordée pour soutenir la recherche, élargir les partenariats dans le secteur privé et agrandir le bassin de talents en cybersécurité par la création de réseaux affiliés à des universités.

D) Le Canada continue d'offrir des évaluations de cybervulnérabilité aux propriétaires et aux exploitants d'infrastructures essentielles (IE) au Canada grâce au Programme d'évaluation de la résilience régionale (PERR) de Sécurité publique Canada. Les évaluations de cybervulnérabilité du PERR reposent sur le cadre de cybersécurité du NIST et elles évaluent l'état de la cybersécurité d'une organisation dans 10 domaines comme la gestion de la configuration, la gestion de la vulnérabilité et la connaissance de la situation. Les participants reçoivent des notes qui leur permettent de se comparer avec l'industrie et des rapports qui pointent les lacunes de leurs capacités aux fins de correction. Depuis 2013, les évaluations ont aidé le Canada à sensibiliser les exploitants d'IE à la cyberrésilience et leur ont permis d'agir pour améliorer leur cybersécurité dans plus de 80 cas.

Au moyen du Symposium sur la sécurité des systèmes de contrôle industriels (SCI) et des ateliers techniques et concrets sur les SCI, le Canada continue de réunir les experts en SCI dans les 10 secteurs des IE pour offrir de la formation et diffuser des outils et de l'information afin de mieux protéger les SCI des perturbations cybernétiques et d'aider les propriétaires et les exploitants d'IE à mieux protéger leurs SCI et leurs systèmes de TI les plus vitaux. En 2018, le comité consultatif du Symposium sur la sécurité des SCI a été créé en tant que mécanisme pour accroître la collaboration avec la communauté des SCI au Canada et aider à guider la planification stratégique du Symposium sur la sécurité des SCI.

Le Canada travaille aussi à élargir l'offre d'exercices en ligne à la communauté des responsables d'IE. Cela comprendra des exercices plus fréquents et récurrents d'interdépendance des IE, ainsi que le développement d'exercices des cybercapacités pour les propriétaires et exploitants de ces infrastructures. Ces exercices visent à augmenter la résilience de la communauté des responsables d'IE en les aidant à cerner et à réduire leurs cybervulnérabilités.

E) Le renforcement des capacités liées à la cybersécurité aide les pays à améliorer les compétences des responsables des politiques et les connaissances des gouvernements et des exploitants d'IE en vue de détecter et de prévenir les cybermenaces, de répondre aux cyberincidents et de s'en remettre. Cela se fait par des activités comme l'organisation de formations techniques au niveau national, sous-régional ou régional pour les techniciens en sécurité informatique, les exploitants d'IE et les agents des forces de l'ordre. Les sujets à l'étude ont déjà compris la protection des IE et des SCI, les techniques fondamentales et avancées de réponse aux incidents, les techniques d'enquête en ligne et la lutte contre l'utilisation d'Internet à des fins criminelles ou terroristes.

Norme 8 : Les États devraient répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté;

Quand le Canada reçoit une demande d'aide d'un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique, nous répondons et faisons de notre mieux pour aider cet État et contrer toute menace provenant du territoire canadien.

A) Le Canada est actif dans de nombreux forums qui encouragent l'échange d'information et la coopération durant les incidents. Le Canada est aussi un participant actif au sein d'organisations régionales, en particulier l'OSCE, qui ont adopté des MRC pour favoriser l'entraide et l'échange d'information sur les incidents.

B) L'un des buts principaux du **Cybercentre** est de collaborer avec les propriétaires d'IE du Canada et tous les niveaux de gouvernement, les universités et l'industrie privée pour combattre les cybermenaces.

De plus, l'adoption de la *Loi sur le CST* en juin 2019 a donné au Cybercentre le pouvoir de fournir des conseils, de l'orientation et des services concernant les cybermenaces aux propriétaires d'IE. Par exemple, la loi a autorisé le Cybercentre à déployer ses outils uniques de cybersécurité dans les systèmes non gouvernementaux quand ceux-ci ont été désignés par le ministre de la Défense nationale du Canada comme des systèmes d'importance pour le gouvernement du Canada. Ces services pourraient aussi être offerts à la demande des propriétaires de ces systèmes.

C) Les efforts de renforcement des capacités du Canada visent à améliorer continuellement l'échange d'information, la coordination et la coopération dans l'ensemble des Amériques et avec la communauté internationale pour mieux répondre au caractère transnational des cybermenaces. Cela comprend une collaboration technique entre les EIISI, une coopération juridique dans la lutte contre la cybercriminalité et un dialogue politique hémisphérique sur le droit international et les normes volontaires de comportement dans le cyberespace.

Norme 9 : Les États devraient prendre des mesures raisonnables pour garantir l'intégrité de la chaîne logistique, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits informatiques, et devraient s'attacher à prévenir la prolifération des techniques et des outils informatiques malveillants et l'utilisation de fonctionnalités cachées malveillantes.

A) Le Centre canadien pour la cybersécurité collabore étroitement avec des intervenants dans des secteurs essentiels pour fournir des conseils et de l'orientation afin de diminuer les risques pour la chaîne logistique des IE dont les Canadiens dépendent chaque jour. Par exemple, depuis 2013, le Programme d'examen de la sécurité du CST a contribué à réduire les risques pour la chaîne logistique des technologies 3G, 4G et LTE dans le secteur des télécommunications. À ce jour, le CST et ses partenaires gouvernementaux ont travaillé avec des entreprises représentant plus de 99 % du marché des appareils mobiles au Canada pour réduire le risque de cyberespionnage et de perturbation des réseaux. Ce programme a aidé à atténuer les risques en excluant de l'équipement et des services désignés de zones sensibles des réseaux de télécommunication du Canada.

B) Efforts pour améliorer la sécurité de l'Internet des objets afin de réduire les risques et d'inspirer confiance aux consommateurs

À la réunion des ministres des Cinq Nations en 2019, le Canada et ses partenaires aux vues similaires se sont engagés à soutenir la sécurité dès la conception des appareils connectés ou de l'Internet des objets dans leurs industries respectives. Au-delà des Cinq Nations, le Canada s'aligne sur l'UE, le Japon et l'OCDE pour montrer comment la sécurité et la confiance peuvent être soutenues dans le marché de l'Internet des objets. Le Canada a récemment mené à bien une initiative d'un an à plusieurs acteurs avec la Société Internet (ISOC). Le rapport final a été publié pour présenter le travail de ce groupe et indiquer où dans le monde les intervenants canadiens s'engagent dans des questions de sécurité de l'Internet des objets. De façon générale, les gouvernements s'entendent sur les constats suivants :

- Il devrait exister un niveau de base évolutif pour la sécurité des appareils connectés qui peut être mis en œuvre très rapidement par les fabricants. Les organismes de l'industrie nationale et de protection des consommateurs peuvent soutenir la détermination de ce niveau de base.
- De nouveaux règlements ou l'application des cadres actuels du marché (p. ex. la LPRPDE) peuvent faire respecter les exigences de base. Nous ne savons pas exactement quel degré ou quelle cible de l'action gouvernementale seront nécessaires pour assurer la sécurité de l'Internet des objets.

- La coopération internationale dans les forums, plutôt que la compétition, est essentielle. L'échange d'information et la collaboration aideront à atteindre les buts communs (p. ex. sur les normes, etc.).
- Il existe de nombreuses possibilités de sensibiliser les consommateurs à la sécurité de l'Internet des objets. Les gouvernements et les ONG devraient utiliser les efforts en éducation pour venir compléter d'autres travaux sur les normes, les cadres du marché, etc.

Norme 10 : Les États devraient encourager le signalement responsable des failles informatiques et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies de l'information et des communications et pour les infrastructures qui en dépendent;

Le **Cybercentre** publie des alertes et des avis lorsque des cybermenaces, des vulnérabilités ou des incidents possibles, imminents ou réels touchent ou pourraient toucher les infrastructures essentielles du Canada.

Le **Cadre de gestion du partage des nouvelles capacités du CST** est un processus de prise de décisions normalisé utilisé par le CST pour déceler les vulnérabilités des TI. Le Cadre aide le CST à gérer de manière responsable les vulnérabilités découvertes.

Norme 11 : Les États ne devraient pas mener ou soutenir sciemment des activités visant à porter atteinte aux systèmes d'information des équipes d'intervention d'urgence agréées (parfois également appelées équipes d'intervention informatique d'urgence ou équipes d'intervention en cas d'atteinte à la sécurité informatique) d'un autre État; un État ne devrait pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des activités internationales malveillantes;

Le Canada ne réalisera ni ne soutiendra sciemment des activités pouvant nuire aux équipes d'intervention informatique d'urgence des autres États, ni n'utilisera sa propre équipe d'intervention informatique d'urgence pour participer à des activités internationales malveillantes.