Améliorer la fiabilité et la résilience de l'infrastructure numérique du Canada

Recommandations du Forum canadien pour la résilience des infrastructures numériques (FCRIN) au Ministre de l'Innovation, des Sciences et de l'Industrie

Le 1er mai 2023

SOMMAIRE EXÉCUTIF

Les recommandations suivantes ont été élaborées en réponse à une demande du ministre de l'Innovation, des Sciences et de l'Industrie au Forum canadien pour la résilience des infrastructures numériques (FCRIN). Cette demande soulignait l'importance de l'infrastructure numérique dans tous les aspects de l'activité économique et sociale du Canada. Le ministre a également souligné le rôle important des produits, des services et de l'infrastructure fournis par les organisations membres du FCRIN pour la résilience numérique et l'économie du Canada. La lettre du ministre a été envoyée le 1er novembre 2022 avec un délai de six mois.[i]

Le ministre a demandé qu'un ensemble de recommandations soit préparé de manière concertée afin d'améliorer la fiabilité et la résilience de l'infrastructure numérique du Canada. Ces recommandations sont présentées ci-dessous :

- La méthode utilisée pour préparer et présenter nos recommandations.
- Nos recommandations pour améliorer la fiabilité et la résilience de l'infrastructure numérique du Canada vont comme suit :
    - Trois recommandations d'ordre général
    - Douze recommandations pour que le Canada dispose de réseaux et de systèmes robustes à la base de son infrastructure numérique
    - Huit recommandations visant à garantir une planification et une préparation coordonnées pour répondre aux menaces qui pèsent sur notre infrastructure numérique
    - Trois recommandations concernant le renforcement de la responsabilité pour favoriser la résilience des parties prenantes de l'infrastructure numérique

TABLEAU DES RECOMMANDATIONS

Thèmes d'ordre général	**Dirigés vers**	
G 1 : Poste de ministre chargé de veiller à la cohérence et à l'action du gouvernement en matière de politique de cybersécurité et d'objectifs technologiques.	Gouvernement	
G 2 : Compétences, talents et formation	Gouvernement	
G 3 : Maintenir et exploiter le FCRIN	Gouvernement	
Thèmes liés aux réseaux et systèmes robustes	**Dirigés vers**	
RSR 1 : Exigences de résilience pour les programmes de financement de la large bande	Gouvernement	
RSR 2 : Location du réseau de transport des fournisseurs de services Internet titulaires	Gouvernement	
RSR 3 : Améliorer les politiques d'appairage pour une meilleure résilience de l'Internet		Industrie
RSR 4 : Prioriser la concurrence et à la diversité des fournisseurs d'infrastructures	Gouvernement	
RSR 5 : Liste de matériel du fournisseur de réseau Internet en amont	Gouvernement	
RSR 6 : Mise à jour de l'approvisionnement en transit Internet sur la base des normes Internet 2023	Gouvernement	Industrie
RSR 7 : Documenter l'état des solutions de connexions Internet multiples et simultanées		Industrie
RSR 8 : Adoption de normes internationales et de meilleures pratiques	Gouvernement	
RSR 9 : Soutenir la connectivité nationale résiliente	Gouvernement	
RSR 10 : Incitations financières à la résilience	Gouvernement	
RSR 11 : Désignation ou création d'un fournisseur de réseau d'infrastructures essentielles	Gouvernement	
RSR 12 : Interdépendance des systèmes nationaux d'infrastructures numériques	Gouvernement	Industrie
Thèmes de la planification et de la préparation coordonnées	**Dirigés vers**	
PPC 1 : Extension des exercices de planification d'urgence		Industrie
PPC 2 : Personnes-ressources en cas d'urgence	Gouvernement	Industrie
PPC 3 : Mise en place d'un centre de résilience des infrastructures essentielles	Gouvernement	
PPC 4 : Ensemble des règles de gouvernance de la chaîne d'approvisionnement	Gouvernement	Industrie
PPC 5 : Stratégies de défense et ensemble de capacités technologiques	Gouvernement	
PPC 6 : Migration vers la cryptographie post-quantique et l'infrastructure numérique à sécurité quantique	Gouvernement	Industrie
PPC 7 : Sécurité de l'Internet des objets et des réseaux de zombies	Gouvernement	Industrie
PPC 8 : Évaluation nationale des risques liés à l'Internet industriel des objets	Gouvernement	Industrie
Thèmes liés au renforcement de la responsabilité	**Dirigés vers**	
RR 1 : Action de coordination entre le CCCST et le FCRIN	Gouvernement	Industrie
RR 2 : Mise à jour des exigences du programme de sécurité industrielle pour les fournisseurs de technologies de l'information	Gouvernement	
RR 3 : Moderniser la compréhension des mesures de cybersécurité	Gouvernement	Industrie

INTRODUCTION

Le FCRIN est le forum privé-public du Canada par lequel l'industrie et les principaux partenaires fédéraux travaillent ensemble pour améliorer la politique relative à la résilience de l'infrastructure numérique. Le présent document fait un exposé des recommandations des représentants de l'industrie du FCRIN afin d'informer le ministre de l'Innovation, des Sciences et de l'Industrie des mesures à prendre en priorité pour améliorer la résilience de l'infrastructure numérique canadienne.

Au cours de l'été 2022, des millions de Canadiens ont fait l'expérience directe de la difficulté des perturbations technologiques lors de la panne de Rogers ([ii]) et de l'ouragan Fiona. Ces événements – au cours desquels des millions de Canadiens n'ont pas eu accès à des technologies Internet essentielles, des entreprises n'ont pas pu accepter de paiements et accueillir des clients, et des services gouvernementaux ont été rendus inaccessibles – ont démontré l'urgence d'améliorer la résilience.

La résilience de l'infrastructure numérique garantit que les technologies de l'infrastructure numérique de la société canadienne fonctionnent à un niveau acceptable malgré les perturbations dues à des événements tels que des conditions météorologiques extrêmes, des erreurs humaines ou des cyber-attaques. Le paysage technologique étant complexe et en constante évolution, parvenir à la résilience n'est pas une mince affaire. La résilience de l'infrastructure numérique est essentielle pour soutenir une économie et une société numériques fiables et prospères. Qu'il s'agisse des personnes qui interagissent quotidiennement avec la technologie, des entreprises qui développent, déploient, protègent, renforcent, surveillent et vendent la technologie, ou des gouvernements qui élaborent des politiques réglementaires et autres, toutes les parties prenantes ont un rôle actif à jouer pour soutenir la résilience de l'écosystème de l'infrastructure numérique.

Pour parvenir à une résilience généralisée de l'infrastructure numérique, il faut avoir une connaissance approfondie des technologies concernées, de leur fonctionnement et de leur interaction entre elles et avec les différentes parties prenantes. Comme ces technologies, et les normes qu'elles doivent respecter, sont presque entièrement développées par l'industrie des TIC, la voix de l'industrie dans cet effort est essentielle.

MÉTHODOLOGIE

Le Forum canadien sur la résilience des infrastructures numériques est une collaboration public-privé consensuelle et orientée vers l'action qui a été créée pour améliorer la compréhension de la résilience des infrastructures numériques essentielles canadiennes et recommander des améliorations à cet égard. Innovation, Sciences et Développement économique Canada (ISDE) a créé le FCRIN en 2020, en partie pour soutenir la stratégie nationale du Canada pour les infrastructures essentielles (IE). Dans le cadre de cette stratégie, ISDE est le ministère fédéral responsable du secteur des technologies de l'information et des communications (TIC). Le FCRIN rassemble des partenaires fédéraux clés et l'industrie pour améliorer la résilience de l'infrastructure numérique.

Les groupes de travail du FCRIN sont dirigés par l'industrie et comprennent des participants des organisations membres du FCRIN. Les groupes de travail entreprennent des projets convenus d'un commun accord. Les groupes de travail se sont notamment penchés sur les sujets suivants :

- La résilience de l'infonuagique
- L'état de préparation à la quantique
- La fiabilité de la chaîne d'approvisionnement
- La résilience de l'Internet
- L'Internet des objets (IdO)

Les définitions de l'*infrastructure numérique, des services essentiels*, de la *fiabilité* et de la *résilience* peuvent être problématiques si l'on va au-delà du niveau le plus élevé. Quelle est l'infrastructure numérique concernée, et inclut-elle tout ce qui est connecté où que ce soit? Quels services, au-delà du 911, sont considérés comme essentiels? Comment mesurer la fiabilité ou la résilience de cette infrastructure numérique et de ces services essentiels, étant donné que les défaillances peuvent être graves (par exemple, une panne totale) ou légères (par exemple, un temps de réponse lent), généralisées (par exemple, au niveau national) ou localisées (par exemple, au niveau d'un quartier ou d'une tour de téléphonie mobile), durables ou momentanées, et ainsi de suite.

Dans la pratique, le FCRIN considère que les services essentiels sont ceux dont dépendent les Canadiens pour leur subsistance, leur bien-être et leur sécurité. L'infrastructure numérique concernée comprend au moins les actifs qui fournissent ces services. La fiabilité est le degré de protection de notre infrastructure numérique contre les défaillances. La résilience est la mesure dans laquelle notre infrastructure numérique protège les services essentiels aux utilisateurs et est rapidement remise en service en cas de défaillance. Les Canadiens attendent de leur infrastructure numérique qu'elle soit suffisamment fiable et résiliente pour que leurs moyens de subsistance, leur bien-être et leur sécurité ne soient pas menacés par des défaillances de l'infrastructure numérique, quelle qu'en soit la cause.

Bien que la cybersécurité soit un aspect extrêmement important d'une infrastructure numérique résiliente, la plupart des recommandations du FCRIN ne traitent pas spécifiquement de la cybersécurité. La cybersécurité est inhérente à certains sujets, notamment l'état de préparation à la quantique, qui concerne les réponses proactives à une cybermenace imminente pour l'infrastructure numérique. Jusqu'à présent, le FCRIN n'a pas tenté d'aborder de manière exhaustive la cybersécurité de l'infrastructure numérique et s'en remet aux recommandations de Sécurité publique Canada, du Centre de sécurité des télécommunications (CST)/Centre canadien pour la cybersécurité (CCC) et d'autres organismes, qui jouent un rôle de premier plan dans le domaine de la cybersécurité.

Les recommandations contenues dans le présent document ont été fournies par les groupes de travail du FCRIN et rassemblées par une équipe du FCRIN, le Groupe de travail canadien sur la cyber-résilience. Après un processus rigoureux d'examen et d'approbation auquel ont participé tous les membres du FCRIN, nos recommandations sont présentées et discutées ci-dessous sous quatre rubriques – Recommandations générales et les trois catégories du programme de fiabilité des télécommunications d'ISDE – réseaux et systèmes robustes, planification et préparation coordonnées, et renforcement de la responsabilité.[iii]

- Recommandations sur les réseaux et systèmes robustes (RSR)

  Il s'agit de recommandations qui identifieront et traiteront les éléments de l'infrastructure numérique nécessaires pour soutenir la résilience de l'infrastructure numérique canadienne. La résilience de l'infrastructure numérique dépend de la conception et de la construction appropriées des systèmes matériels et logiciels des actifs de communication, de traitement et de stockage sous-jacents. La résilience de l'infrastructure numérique peut être améliorée dans une large mesure par une combinaison de redondance et de diversité dans les interconnexions de réseaux, ce qui réduit le risque de perturbation due à une défaillance du réseau ou à une cyberattaque.

- Recommandations en matière de planification et de préparation coordonnées (PPC)

  Il s'agit de recommandations qui décrivent la manière dont nous nous préparons à des défaillances inévitables et dont nous nous en remettons rapidement. Des réseaux et des systèmes robustes sont nécessaires mais pas suffisants pour garantir la résilience de l'infrastructure numérique. L'infrastructure numérique du XXIe siècle est un système complexe de systèmes dont les composants évoluent rapidement. En outre, les menaces qui pèsent sur l'infrastructure numérique sont diverses et évoluent rapidement. Par conséquent, les défaillances de l'infrastructure numérique sont inévitables. Se préparer à de tels événements peut permettre aux services de se rétablir rapidement malgré la défaillance de certaines parties du système – une mesure clé de la résilience.

- Recommandations sur le renforcement de la responsabilité

  Les recommandations de ce type portent sur des modèles de rapport ou de maturité qui nous permettent d'évaluer nos performances et ce que nous devrions partager au sein ou entre les industries et leurs parties prenantes (par exemple, les utilisateurs, le grand public, le gouvernement, les organismes de réglementation) afin d'éduquer les autres et de garantir que notre infrastructure numérique est résiliente et fiable du point de vue de l'ensemble du cycle de vie.

  Les données et les rapports sont essentiels si nous voulons savoir si les réseaux et les systèmes sont robustes et si notre planification et notre préparation permettent de faire face efficacement aux menaces qui pèsent sur notre infrastructure numérique. La responsabilité commence par la connaissance des performances de l'infrastructure, de l'apparition des problèmes et de la manière dont les défaillances sont traitées en temps opportun.

Dans certains cas, les recommandations peuvent couvrir plusieurs catégories. Nous nous sommes efforcés de regrouper les recommandations en fonction de leur objectif principal, sans essayer de limiter les recommandations fournies par l'industrie.

RECOMMANDATIONS

RECOMMANDATIONS GÉNÉRALES

G 1 : POSTE DE MINISTRE CHARGÉ DE VEILLER À LA COHÉRENCE ET À L'ACTION DU GOUVERNEMENT EN MATIÈRE DE POLITIQUE DE CYBERSÉCURITÉ ET D'OBJECTIFS TECHNOLOGIQUES

Aujourd'hui, les responsabilités en matière de cybersécurité au sein du gouvernement fédéral sont réparties entre au moins 12 ministères et agences[iv]. Pour favoriser la résilience numérique, il est essentiel de créer une cohérence au sein du gouvernement afin de garantir que tous les ministères fonctionnent avec une unité d'effort et d'objectif. Ces efforts coordonnés doivent couvrir l'élaboration des politiques et des programmes, la passation des marchés et l'utilisation des pouvoirs d'approbation et de financement afin de favoriser et de garantir que les actions et les activités aboutissent à des résultats en matière de cybersécurité et de résilience.

Les homologues internationaux du Canada disposent d'organismes similaires qui peuvent servir de cadre de référence. Par exemple, les États-Unis ont nommé en juillet 2021 leur premier directeur national du cyberespace à la Maison Blanche, qui sera le principal conseiller du président en matière de cybersécurité[v]; le Royaume-Uni dispose d'un sous-secrétaire d'État parlementaire pour le numérique et la large bande, chargé de la cybersécurité et des compétences en cybersécurité[vi]; et l'Australie a créé un de poste de ministre autonome de la cybersécurité en juin 2022.[vii]

Recommandation : *Le ministre devrait demander au cabinet d'envisager la création d'un poste de ministre, qui reprendrait les meilleurs aspects de chacun des modèles susmentionnés et enverrait un signal fort indiquant que le Canada prend au sérieux la cybersécurité et la résilience numérique.*

G 2 : COMPÉTENCES, TALENTS ET FORMATION

Le Conseil des technologies de l'information et des communications[viii] et l'Institut CD Howe[ix] font tous deux état de la pénurie de compétences numériques et techniques à laquelle est confronté le marché du travail canadien. On ne saurait trop insister sur l'importance de disposer d'une main-d'œuvre pour l'infrastructure numérique qui soit à la fois suffisante et qualifiée.

La disponibilité et la capacité de cette main-d'œuvre pourraient être améliorées par des actions portant sur les points suivants :

a) À tous les stades de la carrière : Les compétences en matière d'infrastructure numérique sont nécessaires pour les étudiants actuels et futurs de l'enseignement supérieur, ainsi que pour les travailleurs actuels qui ont besoin d'un perfectionnement des compétences.

b) Technique, opérations, secteurs d'activité, juridique, ressources humaines, achats, cadres supérieurs, conseil d'administration, décideurs politiques : Les compétences ou la préparation en matière d'infrastructure numérique vont bien au-delà de la technologie et s'étendent à des organisations entières qui établissent ou renforcent des « cultures numériques » pour leurs opérations. La réduction du temps de mise sur le marché de l'innovation crée une perturbation numérique qui s'étend aux secteurs d'activité, au service juridique, aux ressources humaines, à la direction, etc. Les compétences doivent être acquises dans l'ensemble de l'entreprise pour garantir l'alignement organisationnel.

c) Un programme d'études commun et généralisé : Il n'existe actuellement aucun programme d'études normalisé pour l'infonuagique, la chaîne d'approvisionnement, l'état de préparation quantique et d'autres sujets liés à la résilience de l'infrastructure numérique dans l'ensemble des communautés éducatives canadiennes. Le programme d'études sur l'infrastructure numérique devrait être normalisé dans tout le pays et mettre l'accent sur la sécurité, la protection de la vie privée et la résilience. En outre, il devrait être « intégré » (plutôt que de faire l'objet de cours facultatifs) dans les programmes d'informatique, de génie logiciel, d'électrotechnique, de génie informatique et autres programmes similaires.

d) Immigration et autorisations : Compte tenu du déficit de talents, le Canada devrait améliorer les procédures d'immigration pour les nouveaux arrivants possédant des compétences en matière d'infrastructure numérique. Étant donné que de nombreux postes vacants dans le secteur de l'infrastructure numérique requièrent des habilitations de sécurité, le gouvernement devrait rationaliser et accélérer les processus d'habilitation pour les nouveaux Canadiens possédant ces compétences.

Recommandation : Le *gouvernement, l'industrie et le monde universitaire devraient collaborer en priorité à l'élaboration et à la mise en œuvre d'un plan ambitieux visant à garantir que le Canada dispose de la réserve de talents nécessaire pour construire, installer, mettre à niveau, entretenir et protéger l'infrastructure numérique du pays.*

G 3 : MAINTENIR ET EXPLOITER LE FCRIN

Le FCRIN est un forum qui permet de s'assurer que la résilience est continuellement prise en compte, conçue, mise en œuvre et maintenue dans l'infrastructure numérique du Canada. Il est relativement nouveau, mais il a déjà réuni de nombreuses entreprises de TIC et des leaders d'opinion, et ses groupes de travail œuvrent activement à l'amélioration de la résilience de l'infrastructure numérique du Canada. Le gouvernement devrait éviter de créer d'autres groupes ou forums ayant un mandat similaire et veiller à ce que le rôle du FCRIN soit reconnu au sein de tous les ministères concernés.

Recommandation : *ISDE devrait continuer à soutenir fermement le FCRIN et à tirer parti de son travail autant que possible.*

RECOMMANDATIONS EN FAIT DE RÉSEAUX ET DE SYSTÈMES ROBUSTES

RSR 1 : EXIGENCES DE RÉSILIENCE POUR LES PROGRAMMES DE FINANCEMENT DE LA LARGE BANDE

Recommandation i : *Tous les gouvernements devraient exiger des candidats qui cherchent à obtenir un soutien des programmes de financement de la large bande qu'ils démontrent comment les investissements qu'ils proposent dans l'infrastructure de la large bande amélioreront la résilience des réseaux de la large bande. Cela s'applique aux programmes de financement tels que le programme Brancher pour innover : Collectivités rurales et éloignées d'ISDE, ainsi que les programmes proposés par le CRTC et le ministère des Affaires autochtones.*

Recommandation ii : *Le gouvernement fédéral devrait veiller à ce que les fournisseurs de services Internet régionaux aient accès à des services de transport vers le point d'échange Internet (IXP) le plus proche afin d'accroître leur résilience. Cet objectif peut être atteint en fournissant des services de transport directement aux services d'infrastructures essentielles tels que la résolution des serveurs de noms de domaine (DNS).*

Recommandation iii : *Le gouvernement fédéral, pour le prochain cycle de candidatures au Fonds pour la large bande universelle et pour tout autre programme de financement de la large bande à l'avenir, devrait examiner comment le transport vers les FSI régionaux est soutenu dans le programme de financement ; comment la résilience de la connexion Internet au FSI régional est assurée ; comment garantir qu'il n'y a pas de points de défaillance uniques dans l'accès Internet fourni ; et comment garantir une capacité suffisante en termes de transit Internet et de services de transport.*

RSR 2 : LOCATION DU RÉSEAU DE TRANSPORT DES FOURNISSEURS DE SERVICES INTERNET TITULAIRES

De nombreux fournisseurs de services Internet (FSI) canadiens ne sont interconnectés qu'avec un seul fournisseur en amont, souvent physiquement situé loin de la zone d'activité du FSI. Cette interconnexion unique est un point de défaillance unique potentiel qui rend le FSI vulnérable aux pannes subies par son fournisseur en amont. Parfois, l'absence d'autres options d'interconnexion est due au fait que les fournisseurs de réseau en amont refusent de vendre la connectivité de transport à d'autres fournisseurs ou à des points d'échange Internet desservis par d'autres fournisseurs.

Recommandation : *Le ministre devrait demander au CRTC d'amorcer une procédure publique pour déterminer l'ampleur du refus de certains fournisseurs en amont (notamment les grands FSI titulaires) de vendre des services de transport abordables aux FSI plus petits, et s'il existe des moyens réglementaires ou autres pour remédier à cette situation.*

RSR 3 : AMÉLIORER LES POLITIQUES D'APPAIRAGE POUR UNE MEILLEURE RÉSILIENCE DE L'INTERNET

Les principaux points d'échange Internet ont été établis pour permettre aux fournisseurs de services Internet au Canada d'échanger du trafic Internet (ce que l'on appelle l'« appairage »). Toutefois, la plupart des grands FSI titulaires du Canada ne s'associent pas ouvertement aux IXP existants, au détriment des petits FSI qui ont peut-être déjà établi une présence dans ces IXP. En d'autres termes, les FSI titulaires préfèrent servir les organisations canadiennes en tant que clients plutôt que de s'associer directement avec elles au sein d'un IXP.

En raison des efforts déployés par ces FSI titulaires, qui acheminent la majeure partie du trafic canadien, pour éviter les IXP canadiens, la majeure partie du trafic canadien de consommateur à consommateur et de consommateur à entreprise est acheminée par les fournisseurs titulaires canadiens via les États-Unis (et les IXP américains) plutôt qu'à travers le Canada. La performance de certains services au Canada, tels que les conférences web privées et autres, est entravée par le fait que le trafic est acheminé du nord au sud plutôt que d'est en ouest, ce qui signifie que les consommateurs canadiens ainsi que les petits fournisseurs de services Internet canadiens sont désavantagés.

Recommandation : Le *FCRIN devrait entamer une conversation avec le Comité consultatif canadien pour la sécurité des télécommunications (CCCST) sur la manière d'améliorer les relations entre les IXP canadiens et les fournisseurs de services Internet titulaires, dans le but :*

- *D'encourager une politique d'appairage plus permissive de la part de ces FSI et une transition progressive vers le maintien d'une plus grande partie du trafic au Canada.*
- *D'apparier tous les réseaux d'infrastructures essentielles présents à l'IXP afin qu'ils puissent rapidement commencer à échanger le trafic dans cet IXP avec tous les membres de l'IXP en cas de panne.*

RSR 4 : PRIORITÉ À LA CONCURRENCE ET À LA DIVERSITÉ AU SEIN DES FOURNISSEURS D'INFRASTRUCTURES

L'expansion continue des installations de télécommunications et de réseaux câblés améliore la redondance, et donc la résilience, de l'Internet canadien. La concurrence entre les fournisseurs d'installations, qui se traduit par un éventail diversifié de fournisseurs construisant et exploitant leurs réseaux, FSIt partie intégrante de la redondance et de la résilience de l'Internet canadien.

Recommandation : *Le Conseil de la radiodiffusion et des télécommunications canadiennes et le ministère de l'Innovation, des Sciences et du Développement économique devraient continuer à soutenir et à créer des conditions favorables à la concurrence entre les opérateurs de réseaux pour les installations Internet clés, y compris, mais sans s'y limiter, les liaisons de retour, le transport et le dernier kilomètre*.

RSR 5 : LISTE DE MATÉRIEL DU FOURNISSEUR DE RÉSEAU INTERNET EN AMONT

Tout comme une entreprise de construction peut dresser la liste des matériaux et des composants utilisés pour construire une structure à l'intention du propriétaire de la structure, les fournisseurs de services Internet qui fournissent un accès au réseau au Canada devraient être tenus de mettre à disposition, sur demande, une liste de leurs fournisseurs de réseaux Internet en amont. Cela permettrait aux entreprises et aux consommateurs canadiens de mieux comprendre les éléments qui composent leur accès à Internet, d'identifier et d'atténuer les éventuels points de défaillance uniques, et de déterminer leur propre niveau de résilience en matière d'accès à Internet. Cette exigence accroîtrait la transparence et la connaissance des dépendances de l'accès au réseau Internet, ce qui améliorerait la prise de décision et la gestion des risques pour les consommateurs et les entreprises.

Recommandation : *Les FSI fournissant un accès au réseau au Canada devraient être tenus de mettre à la disposition des clients, sur demande, une liste de leurs fournisseurs de réseau Internet en amont.*

RSR 6 : MISE À JOUR DE L'APPROVISIONNEMENT EN TRANSIT INTERNET SUR LA BASE DES NORMES INTERNET 2023

Selon APNIC Labs, le gouvernement du Canada n'exige pas certaines normes et certains protocoles clés pour ses déploiements d'accès à Internet. APNIC Labs fournit des recherches, des mesures et des rapports techniques sur l'utilisation de certaines normes et protocoles Internet clés, tels que IPv6, DNSSEC et la validation RPKI ROA (le gouvernement canadien exploite ses réseaux en utilisant le numéro autonome AS2675) :

- https://stats.labs.apnic.net/ipv6/AS2675
- https://stats.labs.apnic.net/dnssec/AS2675
- https://stats.labs.apnic.net/roa/AS2675

Recommandation : *Le gouvernement du Canada devrait revoir ses exigences en matière d'achat de transit Internet et veiller à ce que ses propres réseaux et ceux des fournisseurs d'infrastructures essentielles soient conformes aux normes et aux meilleures pratiques les plus récentes.*

Cet examen devrait porter sur des éléments tels que les suivants :

- Prise en charge du transit IPv4 et IPv6 à double empilement pour la redondance des protocoles.
- Faire en sorte que les capacités de transit comprennent des accords d'appairage avec les IXP canadiens concernés qui ont une politique d'appairage suffisamment permissive.
    - Par exemple, l'appairage du trafic avec des fournisseurs d'infrastructures essentielles au Canada.
    - Au minimum, l'appairage avec les fournisseurs DNS tels que .CA, .COM, et les serveurs racine.
- Veiller à ce que les fournisseurs d'accès à Internet :
    - Dressent la liste de leurs fournisseurs de réseau Internet en amont pour aider à comprendre leur niveau de redondance et de résilience.
    - Disposent d'accords de niveau de service couvrant la disponibilité et la qualité du service pour le trafic IPv4 et IPv6.
    - Adoptent les meilleures pratiques, telles que MANRS, BCP38 (Network Ingress Filtering), validations DNSSEC, RPKI.
    - Démontrent un engagement en faveur de la mise en œuvre continue des normes, protocoles, technologies et meilleures pratiques clés d'Internet au fur et à mesure de leur évolution.

RSR 7 : DOCUMENTER L'ÉTAT DES SOLUTIONS DE CONNEXIONS INTERNET MULTIPLES ET SIMULTANÉES

Les parties prenantes devraient collaborer à l'élaboration d'un guide pour les solutions Internet de multiconnexion ou « multi-homing ». Une entreprise ou même une résidence est en mode « multi-homing » lorsqu'elle dispose de connexions Internet simultanées provenant de plus d'un fournisseur d'accès à Internet. Le « multi-homing » est un sujet très complexe et les solutions divergent en fonction des exigences de résilience. Le guide en question pourrait contenir des informations sur les différents types de solutions de « multi-homing » disponibles pour différents types d'utilisateurs (par exemple, particuliers, petites entreprises, entreprises), les avantages et les inconvénients de chaque solution et des recommandations pour choisir la bonne solution en fonction des besoins et des exigences de chacun. Le coût est un facteur important à inclure dans chacun des scénarios. Le guide devrait présenter les différentes options disponibles pour automatiser le passage de la connexion principale à la connexion de secours afin d'éliminer les temps d'arrêt.

L'élaboration du guide impliquerait des experts dans le domaine, tels que des ingénieurs de réseau, des fournisseurs de services Internet et des représentants du gouvernement, afin qu'ils partagent leurs connaissances et leurs expériences. Ces derniers pourraient également mener des enquêtes et des recherches pour mieux comprendre l'état actuel des solutions Internet de « multi-homing » au Canada et identifier les lacunes dans les connaissances ou les domaines dans lesquels des informations supplémentaires sont nécessaires.

Une fois le guide élaboré, il pourrait être diffusé par différents canaux, tels que des ressources en ligne, des programmes de formation et des ateliers, afin de s'assurer que les particuliers et les organisations ont accès aux informations dont ils ont besoin pour prendre des décisions éclairées concernant leurs solutions Internet.

Recommandation : *L'industrie devrait élaborer un guide sur les solutions Internet « multi-homing » et veiller à sa diffusion.*

RSR 8 : ADOPTION DE NORMES INTERNATIONALES ET DE MEILLEURES PRATIQUES

Le Canada accuse un retard dans l'adoption de normes de conformité pour un certain nombre de domaines de l'infrastructure numérique, tels que les services infonuagiques, l'IdO, la chaîne d'approvisionnement et l'informatique quantique. La spécification par le gouvernement fédéral d'exigences sur mesure pour les fournisseurs ne fait pas qu'ajouter des frictions à toute initiative de prestation de services – ces exigences propres au Canada ajoutent également des coûts et une dette technique. Les services financiers, le secteur de l'énergie, les transports et d'autres participants aux infrastructures essentielles réglementées ont adopté des normes internationales telles que ISO, SSE

SOC, Cloud Security Alliance et d'autres pour démontrer des niveaux d'assurance suffisamment élevés pour l'adoption de ces services dans leurs communautés.

Recommandation : Le *gouvernement du Canada devrait adopter des normes internationales et communiquer clairement les normes qu'il soutient lors de l'acquisition de services infonuagiques et d'autres infrastructures numériques. Le gouvernement du Canada devrait prendre en considération les normes existantes des États-Unis et de l'UE. Le gouvernement du Canada devrait également participer activement aux activités d'élaboration de normes internationales pour les normes adoptées*.

RSR 9 : SOUTENIR LA CONNECTIVITÉ NATIONALE RÉSILIENTE

L'infrastructure essentielle du Canada, y compris l'infrastructure numérique, est fortement dépendante de la dynamique nord-sud. Il existe de nombreux points vitaux au Canada où les dommages causés par l'environnement ou d'autres éléments à un endroit précis peuvent avoir un impact significatif sur une variété de services essentiels à une échelle régionale ou plus étendue. Il existe souvent une préférence pour une modalité de communication particulière. Cela peut changer en raison des priorités des fournisseurs de télécommunications locaux et de leurs ambitions en matière d'infrastructure.

Recommandation : *Le gouvernement du Canada devrait chercher à accroître la diversité des routes géographiques d'est en ouest à l'intérieur du Canada pour les infrastructures numériques essentielles, en envisageant un portefeuille de moyens de communication, y compris la fibre, le sans-fil (4G, 5G, Whitespace WiFi) et le satellite LEO pour soutenir la résilience.*

RSR 10 : INCITATIONS FINANCIÈRES À LA RÉSILIENCE

La résilience nécessite souvent des investissements supplémentaires, car des voies et une main-d'œuvre à sécurité intégrée, redondantes et dupliquées sont nécessaires pour assurer le fonctionnement continu des services dans des conditions difficiles.

Recommandation : *Le gouvernement du Canada devrait envisager des mesures incitatives pour encourager les organisations à améliorer leur résilience face aux défaillances du réseau de leur fournisseur principal.*

RSR 11 : DÉSIGNATION OU CRÉATION D'UN FOURNISSEUR DE RÉSEAU D'INFRASTRUCTURES ESSENTIELLES (IE)

De nombreux fournisseurs d'IE du Canada dépendent de l'Internet public fourni par un FSI. En cas de perturbation majeure de l'Internet chez leur FSI, un fournisseur d'IE pourrait compter sur un fournisseur de réseau d'IE désigné pour maintenir la connectivité entre les systèmes d'IE qui sont essentiels à la fourniture de services essentiels.

Recommandation : *Le gouvernement du Canada devrait évaluer la faisabilité et les avantages de la désignation ou de la création d'un fournisseur de réseau d'IE de confiance exploitant un tel réseau de base d'IE d'urgence. Les fournisseurs d'IE désignés doivent se connecter à ce réseau de base d'IE en utilisant une architecture de confiance zéro.*

RSR 12 : INTERDÉPENDANCE DES SYSTÈMES NATIONAUX D'INFRASTRUCTURE NUMÉRIQUE

Les systèmes qui composent l'infrastructure numérique du Canada sont de plus en plus interdépendants. Il est donc difficile de comprendre le fonctionnement normal de notre infrastructure numérique et extrêmement difficile d'anticiper l'impact des défaillances. Ce problème ne doit pas être ignoré.

Recommandation : *Le gouvernement du Canada, avec la collaboration de l'industrie, devrait élaborer un programme complet pour comprendre et gérer le déploiement interdépendant des systèmes technologiques qui constituent l'infrastructure numérique du Canada. Ce programme devrait commencer par les systèmes dont dépendent les secteurs de l'infrastructure numérique du Canada. Ce programme pourrait prendre en compte, entre autres, le besoin de technologies à sécurité cryptographique post-quantique (CPQ) et à sécurité quantique, et devrait inclure une contribution et un soutien significatifs de la part de tous les secteurs d'infrastructures essentielles du Canada*.

RECOMMANDATIONS EN MATIÈRE DE PLANIFICATION ET DE PRÉPARATION COORDONNÉES

PPC 1 : EXTENSION DES EXERCICES DE PLANIFICATION D'URGENCE

Notre infrastructure numérique est sophistiquée et très interdépendante. L'extension des exercices de planification d'urgence à d'autres parties prenantes permettra de mieux refléter la manière dont les situations d'urgence affectent l'ensemble de la société et dont l'infrastructure numérique s'articule avec tous les secteurs. La résilience en cas d'urgence s'en trouvera renforcée.

Ces exercices de planification d'urgence pourraient prendre en compte des scénarios de défaillance « zéro jour », peu probables mais à fort impact, afin de mener une évaluation réfléchie de l'interconnexion de nombreux secteurs et d'équiper le gouvernement et l'industrie pour mieux faire face à des scénarios de défaillance inattendus mais graves. L'objectif serait d'élargir le champ d'application des exercices de planification qui sont déjà réalisés au niveau d'une entreprise individuelle ou d'un fournisseur de services Internet, ou même au niveau du CCCST, et d'inclure une participation plus large de l'industrie et d'autres parties prenantes.

Recommandation : *Le CCCST et le FCRIN devraient élaborer conjointement un plan pour la réalisation d'exercices de planification d'urgence. Ce plan devrait être coordonné avec les programmes appropriés du gouvernement du Canada*.

PPC 2 : PERSONNES-RESSOURCES EN CAS D'URGENCE

L'un des défis de la gestion pendant une panne est que certains canaux de communication ne sont probablement pas disponibles, même pour les techniciens qui s'occupent de la panne. Le CCC devrait collaborer avec le FCRIN pour déterminer les personnes à inclure dans les personnes-ressources d'urgence, le mécanisme permettant de garantir la confidentialité de ces informations (par exemple, TLP AMBER+STRICT), l'obligation pour les parties prenantes (telles que les fournisseurs de réseaux et d'infrastructures essentielles) de tenir leurs informations à jour, et le mécanisme permettant d'utiliser les informations des personnes-ressources dans divers scénarios de défaillance de l'infrastructure numérique.

Recommandation : *Le CCC, avec l'aide du FCRIN et d'autres entités, devrait établir et tenir à jour une liste de personnes-ressources en cas d'urgence comprenant les coordonnées de tous les canaux de communication possibles afin que les parties prenantes puissent être informées des incidents et coordonner leur réponse.*

PPC 3 : MISE EN PLACE D'UN CENTRE DE RÉSILIENCE DES INFRASTRUCTURES ESSENTIELLES (IE)

Le gouvernement du Canada ne dispose pas d'un centre de coordination central pour la résilience des infrastructures essentielles. Il existe de nombreuses interdépendances entre les mandats des ministères fédéraux. Par conséquent, il est difficile de progresser sur les impératifs interministériels visant à mesurer et à améliorer la résilience de l'infrastructure numérique du Canada.

Recommandation : *Le gouvernement du Canada devrait créer un centre de résilience des IE pour combler les lacunes de la résilience des IE du Canada et travailler dans le cadre des mandats ministériels. Le champ d'action du centre de résilience des IE devrait également inclure la cyber-résilience et être lié à l'évaluation de l'infrastructure nationale.*

PPC 4 : ENSEMBLE DE RÈGLES DE GOUVERNANCE DE LA CHAÎNE D'APPROVISIONNEMENT

Le gouvernement du Canada dispose d'un modèle permettant de garantir des résultats stratégiques positifs lorsque plusieurs entités gouvernementales appliquent chacune leurs propres mandats, pouvoirs, ressources et programmes en matière de gestion des risques liés à la chaîne d'approvisionnement. Ce modèle repose sur d'importants facteurs de réussite : 1) Si et dans quelle mesure les agences individuelles opèrent dans le cadre d'une stratégie et d'une vision unifiées, avec un plan d'action défini; 2) Dans quelle mesure chaque agence concernée est consciente et capable de compléter les activités des autres agences de manière coordonnée; et 3) Dans quelle mesure la structure de coordination permet la collaboration avec d'autres partenaires gouvernementaux et non-gouvernementaux.

L'alignement pangouvernemental est essentiel pour garantir que les agences disparates du gouvernement du Canada sont alignées dans leur objectif et leurs actions pour atténuer les risques liés à la chaîne d'approvisionnement numérique, et pour fournir un point de contact centralisé pour la sensibilisation et la collaboration avec les gouvernements provinciaux, territoriaux et municipaux, les propriétaires et exploitants d'infrastructures essentielles et leurs principaux fournisseurs, le monde

universitaire et les efforts internationaux de gestion des risques liés à la chaîne d'approvisionnement numérique.

Recommandation : *Le gouvernement fédéral, par l'entremise d'un ou de plusieurs ministères responsables (ASC, CCC/CST, SPAC, ISDE, CFP, Transports Canada et/ou SCT), devrait fournir les ressources appropriées pour établir un nouveau Centre d'excellence de la chaîne d'approvisionnement du gouvernement du Canada ou un organisme de coordination. Le Centre (ou l'agence de coordination) devrait être conçu pour intégrer les efforts de gestion des risques de la chaîne d'approvisionnement de l'ensemble du gouvernement du Canada avec ceux des provinces, des municipalités, des territoires, des organisations des Premières nations et de l'industrie canadienne. Ce centre devrait être chargé des tâches suivantes :*

1. *Servir de source de connaissances centrale et partagée pour les activités de gestion des risques liés à la chaîne d'approvisionnement menées par les différentes agences et coordonner les activités de gestion des risques liés à la chaîne d'approvisionnement numérique à l'échelle intergouvernementale.*
2. *Élaborer une vision, une stratégie et un plan d'action coordonnés pour les activités de gestion des risques liés à la chaîne d'approvisionnement numérique du Canada, y compris les possibilités de renforcer la collaboration entre les agences fédérales et l'engagement avec les parties prenantes non gouvernementales, ainsi que des orientations pour les parties prenantes non gouvernementales sur les activités clés et les points de contact des agences gouvernementales concernées.*
3. *Examiner les incidents importants liés à la chaîne d'approvisionnement numérique (SolarWinds, Log4j) et élaborer des bilans et des recommandations, y compris l'identification des stratégies de cyberdéfense et des technologies clés qui, ensemble, pourraient contribuer à prévenir ou à atténuer les attaques futures.*
4. *Travailler avec les agences concernées pour examiner les architectures de sécurité et les exigences techniques de référence existantes à l'échelle du gouvernement, et les mettre à jour le cas échéant pour tenir compte des stratégies, des pratiques et des capacités technologiques essentielles en matière de défense des systèmes qui pourraient prévenir, atténuer ou réduire l'impact de futures attaques ou vulnérabilités de la chaîne d'approvisionnement.*
5. *Distribuer les produits de renseignement sur la gestion des risques liés à la chaîne d'approvisionnement du CCC et d'autres organisations aux partenaires des provinces, des municipalités, des territoires, des organisations des Premières nations et de l'industrie canadienne.*
6. *Identifier et/ou concevoir des leviers potentiels de la politique d'approvisionnement du gouvernement du Canada qui pourraient être appliqués pour encourager l'adoption des meilleures pratiques de gestion des risques de la chaîne d'approvisionnement numérique par les fournisseurs de TIC du gouvernement.*

7. *Élaborer un modèle de maturité pour la gestion des risques liés à la chaîne d'approvisionnement propre au Canada afin que les organisations prennent des décisions concernant les ressources de leurs programmes d'assurance de la chaîne d'approvisionnement en fonction de leur profil de risque et afin d'encourager le partage des connaissances. Ce modèle peut intégrer des éléments tirés des modèles de maturité de la chaîne d'approvisionnement existants, par exemple le cadre de cybersécurité du NIST ou le modèle de maturité du Supply Chain Risk Leadership Council (SCRLC).*
8. *Élaborer des recommandations supplémentaires pour impliquer les petites et moyennes entreprises, le cas échéant.*
9. *Identifier les connaissances essentielles en matière de vulnérabilités, déterminer où des recherches et des financements supplémentaires sont nécessaires, et élaborer de nouvelles stratégies pour faire face aux risques existants. Cette organisation intégrerait et coordonnerait les efforts des secteurs public et privé dans le cadre d'une stratégie nationale permanente de gestion des risques liés à la chaîne d'approvisionnement.*
10. *Financer et/ou mener des recherches pour tester la sécurité du courrier électronique, des télécommunications, des centres de données, des appareils et des services technologiques sur le lieu de travail; aider à identifier les vulnérabilités et à développer des mesures d'atténuation; et soutenir les efforts visant à certifier la sécurité des technologies essentielles.*
11. *Élaborer, en collaboration avec l'industrie, un nouveau programme de certification et d'accréditation de l'intégrité de la chaîne d'approvisionnement qui contribuerait à rendre les chaînes d'approvisionnement de l'industrie plus résilientes et plus sûres et, grâce à la certification, offrirait un avantage concurrentiel en démontrant aux consommateurs, par le biais d'une marque de certification, que leurs produits sont résilients et sûrs. Les laboratoires d'essai de l'industrie demanderaient l'accréditation pour offrir ce service d'intégrité de la chaîne d'approvisionnement à l'industrie, lequel pourrait être basé sur la certification de la conformité aux normes d'intégrité de la chaîne d'approvisionnement existante, à savoir : ISO/IEC 27036[x] , ATIS-I-0000090 5G Network Assured Supply Chain.[xi]*

PPC 5 : STRATÉGIES DE DÉFENSE ET ENSEMBLE DE CAPACITÉS TECHNOLOGIQUES

Recommandation : *Le gouvernement du Canada devrait revoir les architectures de sécurité et les exigences techniques de référence existantes à l'échelle du gouvernement et les mettre à jour, le cas échéant, pour tenir compte des stratégies, des pratiques et des capacités technologiques de défense des systèmes essentiels qui pourraient prévenir, atténuer ou réduire l'impact des attaques ou des vulnérabilités de la chaîne d'approvisionnement. Ces architectures et exigences de référence devraient être diffusées auprès de l'industrie en tant que modèles à adopter, dans la mesure du possible et de l'extensibilité. Les actions spécifiques incluraient :*

1. *Adopter des architectures de confiance zéro;*
2. *Aider les ministères et les agences du gouvernement du Canada à mettre en œuvre des mesures d'assurance logicielle et de transparence de la chaîne d'approvisionnement;*
    a. *Maintenir un solide inventaire des fournisseurs qui donne une vue complète de leur situation en matière de sécurité;*
    b. *Mise en place d'un écosystème de collaboration avec les fournisseurs de services de partage d'informations, de réduction des risques et de remédiation, ainsi que de gestion des incidents;*
    c. *Déployer et utiliser la nomenclature des outils de suivi des composants (SBOM pour Software Bill of Materials) dans le cadre des pratiques de gestion des actifs, des pratiques de gestion des vulnérabilités et/ou des pratiques de gestion des licences logicielles d'une organisation;*
    d. *Utiliser une approche sécurisée d'intégration continue et de livraison continue (IC/LC) qui met l'accent sur l'intégration d'outils de sécurité dès le début du cycle de vie de l'ingénierie, par exemple des outils d'analyse statique, dynamique et de composition logicielle.*
3. *Intégrer les technologies de détection et de réponse aux points finaux (EDR pour endpoint detection and response) avec une surveillance basée sur l'intelligence artificielle (IA)/l'apprentissage machine (AM) des plateformes et des produits essentiels pour aider à protéger contre les attaques sophistiquées de la chaîne d'approvisionnement;*
4. *Utiliser des politiques d'assurance fondées sur des principes qui fournissent aux organisations des orientations flexibles fondées sur des objectifs de cybersécurité, par exemple le Règlement général sur la protection des données de l'Union européenne (RGPD UE);*
5. *Maintenir un inventaire solide des actifs et des fournisseurs avec des points de contact explicites pour permettre une action immédiate et coordonnée lors d'un incident afin de sécuriser l'environnement d'une organisation, d'informer les consommateurs en amont et les fournisseurs en aval, et de demander, de collaborer ou d'appliquer des mesures correctives ou d'atténuation dans la propre chaîne d'approvisionnement de l'organisation;*
6. *Maintenir un inventaire précis et actualisé des actifs d'une organisation connectés à Internet et de ceux de sa chaîne d'approvisionnement, afin d'accélérer les mesures correctives et la réponse aux incidents;*
7. *Appliquer des lignes directrices ou des normes largement acceptées pour la gestion du cycle de vie de développement sécurisé (SDLC pour Secure Development Lifecycle), par ex. :*
    a. *NIST SP 800-218 « Secure Software Development Framework »;*
    b. *OWASP « Software Component Verification Standard »;*
    c. *Cloud Native Computing Foundation « Software Supply Chain Best Practices »;*
    d. *Open Source Security Foundation « Supply Chain Levels for Software Artifacts (SLSA) »;*
    e. *ISO/IEC 27034 « Application Security »*

8. *Diffuser à l'industrie les architectures de sécurité et les exigences techniques de référence mises à jour à l'échelle du gouvernement du Canada comme modèles d'adoption, dans la mesure du possible et de l'extensibilité.*

PPC 6 : MIGRATION VERS LA CRYPTOGRAPHIE POST-QUANTIQUE ET L'INFRASTRUCTURE NUMÉRIQUE À SÉCURITÉ QUANTIQUE

Les formes les plus courantes de cryptographie, celles utilisées dans les infrastructures à clé publique, la navigation sur Internet et les appareils IdO, sont également les plus vulnérables aux attaques quantiques. Une grande partie de nos infrastructures essentielles deviendra vulnérable aux actions hostiles en raison de la cryptographie actuelle. En raison de la nature fondamentale de la cryptographie, les défaillances seront systémiques et dévastatrices, et un rétablissement rapide sera probablement impossible.

Les décisions relatives à la sécurité contre les cybermenaces visant des éléments d'infrastructure durables devraient tenir compte de la menace quantique actuelle et future pour la cryptographie et donc la cybersécurité. Le Canada doit se préparer et réagir de manière proactive, en mettant en place des mesures qui favoriseront une transition ordonnée vers l'agilité cryptographique et la cryptographie post-quantique.

Pour améliorer la sécurité et la fiabilité de l'infrastructure numérique du Canada, il est important d'adopter de nouvelles technologies capables de résister aux menaces potentielles de l'informatique quantique. Il s'agit notamment d'utiliser une cryptographie post-quantique normalisée et des produits et services à sécurité quantique qui ont été testés et dont l'efficacité a été prouvée à l'aide de certifications et de méthodes d'essai reconnues au niveau international. En créant une chaîne d'approvisionnement fiable pour ces technologies, le Canada peut protéger ses infrastructures essentielles et même les exporter vers des pays alliés. Chaque secteur d'infrastructures essentielles du Canada devrait évaluer ses vulnérabilités et élaborer un plan pour atténuer la menace quantique à l'aide de solutions de cryptographie post-quantique.

Recommandation : *Le gouvernement canadien et les fournisseurs d'infrastructures essentielles devraient prendre les mesures suivantes, en s'alignant étroitement sur les efforts internationaux de normalisation de cryptographie post-quantique (CPQ) et en reconnaissant la nécessité pour les politiques canadiennes dans ce domaine de s'aligner sur celles de nos principaux alliés – les États-Unis, l'Union européenne et le Royaume-Uni :*

1. *Créer une équipe spéciale ou un groupe de travail pour superviser la mise en œuvre de la CPQ et de l'infrastructure à sécurité quantique. Ce groupe devrait comprendre des experts de l'industrie, des universités et des agences du gouvernement fédéral afin de garantir une approche coordonnée.*
2. *Travailler avec des partenaires de l'industrie pour développer et tester des produits, des services et des solutions de CPQ et à sécurité quantique. Cela pourrait inclure le financement d'initiatives de recherche et de développement, ainsi que des mesures incitatives pour que les entreprises privées investissent dans ces technologies.*
3. *Élaborer un plan visant à créer une chaîne d'approvisionnement fiable en technologies quantiques sûres, y compris celles conçues au Canada, qui peuvent être utilisées au niveau national et exportées vers des pays alliés, en confirmant le respect d'une norme appropriée.*
4. *Procéder à une évaluation complète des risques dans tous les secteurs d'infrastructures essentielles du Canada afin d'identifier les systèmes vulnérables et de hiérarchiser les mesures correctives.*
5. *Sensibiliser et former les fonctionnaires fédéraux, les partenaires industriels et le public à l'importance de la CPQ et de l'infrastructure à sécurité quantique, ainsi qu'aux risques potentiels associés à l'absence de mise en œuvre de ces solutions.*
6. *Élaborer des politiques et des réglementations exigeant l'utilisation de la CPQ et d'infrastructures à sécurité quantique dans les secteurs d'infrastructures essentielles.*
7. *Contrôler et évaluer l'efficacité de la CPQ et de l'infrastructure à sécurité quantique au fil du temps et procéder aux ajustements nécessaires pour garantir la sécurité et la fiabilité constantes de l'infrastructure numérique du Canada.*

Les dix secteurs d'infrastructures essentielles du Canada devraient tous participer activement à cet effort, et toutes les entreprises du secteur des infrastructures essentielles devraient réaliser une évaluation des risques quantiques d'ici à la fin de l'année 2024 et préparer un plan de correction complet d'ici à la fin de l'année 2025.

PPC 7 : SÉCURITÉ DE L'INTERNET DES OBJETS ET DES RÉSEAUX DE ZOMBIES

Les réseaux de zombies IdO à grande échelle comme MIRAI représentent une menace importante pour les réseaux d'infrastructures essentielles. Ces zombies sont constitués d'appareils IdO compromis, tels que des routeurs et des caméras, qui peuvent être contrôlés à distance par des cybercriminels pour lancer des attaques par déni de service distribué (DDoS). Ces attaques peuvent surcharger un réseau de trafic, entraînant son ralentissement, voire sa panne, ce qui peut avoir de graves conséquences pour des secteurs d'infrastructures essentielles tels que la santé, la finance et l'énergie. Les attaques de zombies IdO peuvent également compromettre la sécurité et l'intégrité des données transmises sur ces réseaux, rendant les informations sensibles vulnérables au vol ou à la manipulation.

La taille et la complexité de ces réseaux de zombies, combinées au nombre croissant d'appareils IdO non sécurisés, en font une menace particulièrement difficile à traiter. En l'absence de mesures efficaces pour sécuriser ces appareils et ces réseaux, le risque d'attaques DDoS à grande échelle par des zombies basés sur l'IdO continuera de croître, ce qui pourrait causer des dommages importants aux infrastructures essentielles et à l'économie dans son ensemble.

Recommandation : *Le gouvernement canadien et les fournisseurs d'infrastructures essentielles, afin d'atténuer la menace des zombies IdO à grande échelle comme MIRAI, devraient envisager les actions suivantes axées sur les attaques provenant du Canada :*

1. *Accroître la sensibilisation : Le gouvernement devrait sensibiliser davantage aux risques associés aux dispositifs IoT et aux attaques de botnets par le biais de campagnes de sensibilisation du public et d'initiatives d'éducation. Cela contribuera à promouvoir les meilleures pratiques pour sécuriser les dispositifs et les réseaux IoT.*
2. *Élaborer des réglementations : Le gouvernement devrait élaborer des réglementations qui exigent l'utilisation d'appareils et de réseaux IdO sécurisés dans les secteurs d'infrastructures essentielles. Il peut s'agir d'exigences relatives à la mise à jour régulière des micrologiciels, à la mise en œuvre de contrôles d'accès solides et à d'autres mesures de sécurité.*
3. *Collaborer avec l'industrie : Le gouvernement devrait collaborer avec des partenaires industriels afin de développer les meilleures pratiques et normes pour sécuriser les appareils et les réseaux IdO. Il peut s'agir de travailler avec les fabricants d'appareils pour s'assurer que les appareils sont conçus en tenant compte de la sécurité.*
4. *Investir dans la recherche : Le gouvernement devrait investir dans la recherche afin de mieux comprendre la menace que représentent les réseaux de zombies de l'IdO et d'élaborer des stratégies d'atténuation efficaces. Cela pourrait inclure le financement d'initiatives de recherche axées sur le développement de nouvelles technologies et techniques de sécurité.*
5. *Renforcer les capacités : Le gouvernement devrait renforcer les capacités au sein de ses propres organisations et avec les secteurs d'infrastructures essentielles pour s'assurer qu'ils ont les compétences et les connaissances nécessaires pour gérer efficacement les risques associés aux zombies de l'IdO.*
6. *Élaborer des plans d'intervention : Le gouvernement devrait élaborer des plans d'intervention qui décrivent comment il réagira à d'éventuelles attaques DDoS par des zombies basés sur l'IdO contre des réseaux d'infrastructures essentielles. Il peut s'agir de mesures de détection précoce et d'atténuation pour empêcher les attaques de se propager et de causer des dommages importants.*
7. *Favoriser la coopération internationale : Le gouvernement doit encourager la coopération internationale pour faire face à la menace mondiale des réseaux de zombies de l'IdO. Il peut s'agir de collaborer avec d'autres pays pour élaborer des normes communes et des bonnes pratiques afin de sécuriser les appareils et les réseaux IdO.*

PPC 8 : ÉVALUATION NATIONALE DES RISQUES LIÉS À L'INTERNET INDUSTRIEL DES OBJETS

Il existe très peu d'informations ou d'inventaire sur la quantité et la sécurité des dispositifs connectés déjà déployés dans les secteurs des infrastructures essentielles. Bon nombre des dispositifs connectés actuels ont été déployés avec des technologies non sécurisées et avec les services de surveillance, d'assistance et de maintenance qui y sont associés. On pense que beaucoup de ces dispositifs ont des logiciels obsolètes et qu'il n'est peut-être même pas possible de les mettre à jour. Ces dispositifs n'ont probablement pas de pratiques de confiance zéro appropriées ni de cryptographie adéquate.

Pourtant, nous déployons activement des dispositifs connectés dans tous les secteurs des IE au Canada, notamment l'eau, la sécurité, la santé, la finance, les transports, l'énergie et les services publics, l'alimentation, la fabrication, le gouvernement et les technologies de l'information et des communications. Ces dispositifs comprennent des capteurs, des équipements de réseau, des SCADA, des systèmes de contrôle industriels (SCI), des villes intelligentes, des paiements et bien plus encore.

Le nombre d'appareils IdO augmente considérablement, tout comme la vitesse des processeurs et des réseaux. Ils utilisent également de plus en plus de composants open-source dans leur déploiement, ce qui peut entraîner des risques supplémentaires pour la chaîne d'approvisionnement en logiciels, avec pour conséquence des vulnérabilités à grande échelle.

Les meilleures pratiques exigent que la cybersécurité soit intégrée dans l'architecture, le déploiement et le fonctionnement de ces dispositifs. On estime que les outils et mécanismes de prévention, de détection et d'intervention en matière de cybersécurité en place aujourd'hui sont peu nombreux et qu'une analyse approfondie des risques aiderait le gouvernement canadien et le secteur privé à élaborer des politiques, des normes, des procédures et des lignes directrices solides et fondées sur des données probantes afin de mieux protéger l'infrastructure IdO canadienne dans tous les secteurs de l'infrastructure d'information géographique. Dans le cadre de cet exercice, il serait important d'examiner l'ensemble des technologies de l'information et des technologies opérationnelles (TO) associées pour comprendre les vulnérabilités de ces systèmes.

Recommandation : *Le gouvernement du Canada devrait procéder à une évaluation nationale des risques liés à l'Internet industriel des objets, dans tous les secteurs des infrastructures essentielles canadiennes, dans un délai de deux ans, afin d'aider à identifier les principaux risques liés à l'IdO dans les secteurs des infrastructures essentielles.*

L'achèvement de l'évaluation des risques permettra, dans un deuxième temps, d'identifier et de mettre en œuvre des stratégies et des mesures d'atténuation des risques, afin de contribuer à réduire les

menaces pour les principaux domaines de risque de l'Internet industriel des objets identifiés. Une partie des meilleures pratiques émergentes devrait inclure le partage des meilleures pratiques et des renseignements exceptionnels sur les menaces afin d'améliorer la résilience dans les domaines présentant des vulnérabilités à haut risque / à fort impact.

RECOMMANDATIONS EN FAIT DE RENFORCEMENT DE LA RESPONSABILITÉ

RR 1 : ACTION DE COORDINATION ENTRE LE CCCST ET LE FCRIN

Au Canada, l'Internet ne se résume pas aux fournisseurs de services Internet. Il comprend également les éléments d'infrastructure numérique essentielle tels que les serveurs de noms de domaine, les fournisseurs de contenu, les réseaux d'entreprise, les fournisseurs de services à grande échelle, les fournisseurs de services infonuagique et bien d'autres encore. Le Comité consultatif canadien de la sécurité des télécommunications a déjà fait des recommandations au ministre pour améliorer la résilience de l'infrastructure numérique canadienne. Le FCRIN présente ses recommandations dans le présent document.

Recommandation : *Les présidents du FCRIN et du CCCST devraient se rencontrer pour discuter des domaines dans lesquels il serait bénéfique de collaborer sur les mesures prises sur la base des deux séries de recommandations adressées au ministre.*

RR 2 : MISE À JOUR DES EXIGENCES DU PROGRAMME DE SÉCURITÉ INDUSTRIELLE POUR LES FOURNISSEURS DE TECHNOLOGIES DE L'INFORMATION

Recommandation : *Le gouvernement devrait moderniser le Programme de sécurité industrielle géré par Services publics et Approvisionnement Canada (SPAC) en tenant compte des contrôles de sécurité, de confidentialité et de résilience utilisés dans la prestation de services infonuagique.*

RR 3 : MODERNISER LA COMPRÉHENSION DES MESURES DE CYBERSÉCURITÉ

Alors que les auteurs des menaces de cybersécurité ont progressé dans leurs méthodes d'exploitation des réseaux d'entreprise, de nombreuses entreprises n'ont pas mis en œuvre les contrôles de sécurité fondamentaux préconisés depuis plus de 40 ans. Les marchés publics du gouvernement fédéral et du secteur privé continuent d'utiliser des exigences qui s'alignent sur des approches de la prestation de services informatiques vieilles de plusieurs décennies. Il est clair qu'une approche différente doit être adoptée au-delà des centaines de pages de contrôles et des régimes de conformité et d'audit associés.

Recommandation : *Le gouvernement du Canada devrait examiner les orientations existantes en matière de cyber-résilience et de sécurité des TI pour y déceler des approches dépassées et les réviser en y intégrant des principes modernes afin de répondre aux besoins actuels en matière de menaces et de résilience.*

.

RÉFLEXIONS FINALES

Le FCRIN reste concentré sur les activités visant à améliorer la résilience de l'infrastructure numérique du Canada et est heureux de présenter les recommandations des représentants de l'industrie du FCRIN au ministre de l'Innovation, des Sciences et de l'Industrie. Les technologies, les architectures, les infrastructures, les produits, les services et les solutions, les marchés verticaux, les modèles d'affaires et les processus représentés au sein des membres du FCRIN sont extrêmement variés. Cette diversité reflète la profondeur et l'étendue de l'infrastructure numérique du Canada.

Peu de temps après sa création au début de 2020, le FCRIN a rassemblé de nombreuses entreprises de TIC et des leaders d'opinion. Les groupes de travail du FCRIN ont contribué de manière significative aux efforts visant à identifier et à comprendre les lacunes et les faiblesses auxquelles il faut remédier pour accroître la résilience de l'infrastructure numérique du Canada. On encourage ISDE à poursuivre son soutien de premier ordre qui est très apprécié au sein de ce forum.

Le paysage des technologies et des risques liés à l'infrastructure numérique est très dynamique. Le FCRIN étudie la possibilité de créer deux nouveaux groupes de travail : l'un qui pourrait se concentrer sur l'intelligence artificielle/l'apprentissage machine, et un autre qui pourrait coordonner la réponse du secteur des TIC aux cybermenaces et aux cyberévénements. Le FCRIN examinera également s'il convient de maintenir le groupe de travail canadien sur la cyber-résilience au-delà de son mandat du 1er mai, 2023, et de quelle manière. Nous prévoyons que les activités de ce groupe de travail permettront d'approfondir la question de la résilience de l'infrastructure numérique canadienne.

Le FCRIN continuera à travailler sur les défis les plus urgents auxquels est confrontée la résilience de l'infrastructure numérique du Canada. Il existe de nombreux domaines technologiques *horizontaux* au-delà de ceux qui sont actuellement traités par les groupes de travail du FCRIN, tels que l'intelligence artificielle ou le développement de logiciels sécurisés. Il existe également des technologies plus spécifiques aux marchés *verticaux*, comme les véhicules connectés et les transports. Ces sujets pourront être abordés par les groupes de travail du FCRIN à l'avenir. Pour l'instant, nous sommes prêts à discuter de nos recommandations actuelles afin d'en faciliter la compréhension et la mise en œuvre.

Le FCRIN souhaite remercier le ministre de l'Innovation, des sciences et de l'industrie de lui avoir donné l'occasion de formuler des recommandations visant à améliorer la résilience de l'infrastructure numérique du Canada. Nous sommes impatients de travailler avec l'équipe du ministre sur les actions et le suivi de ces recommandations.

ACRONYMES ET ABRÉVIATIONS

4G	Quatrième génération (sans fil cellulaire)
5G	Cinquième génération (sans fil cellulaire)
APNIC Labs	Asia Pacific Network Information Centre Labs
CCCST	Comité consultatif canadien de la sécurité des télécommunications
CPQ	Cryptographie post-quantique
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes
DDOS	Distributed Denial Of Service (déni de service distribué) (attaque)
DNS	Domain Name System (système de noms de domaine)
DNSSEC	Extensions de sécurité du système de noms de domaine
EDR	Endpoint Detection and Response (détection et réponse au niveau des points finaux)
FCRIN	Forum canadien pour la résilience des infrastructures numériques
IA/AM	Intelligence artificielle/Apprentissage machine
IC/LC	Intégration continue/Livraison continue (processus de développement de logiciels)
IdO	Internet des objets
IE	Infrastructures essentielles
IPv4	Protocole Internet version 4
IPv6	Protocole Internet version 6
ISO	International Organization for Standardization (organisation internationale de normalisation)
ISP	Internet Service Provider (fournisseur de services Internet)
IXP	Internet eXchange Point (point d'échange Internet)
LEO	Low Earth Orbit (orbite terrestre basse) (satellite)
MANRS	Mutually Agreed Norms for Routing Security
MIRAI	Mot japonais signifiant « futur » (zombie)
PPC	Planification et préparation coordonnées
ROA	Route Origin Authorization
RPKI	Resource Public Key Infrastructure
RR	Renforcement de la responsabilité
RSR	Réseaux et systèmes robustes
SBOM	Software Bill Of Materials (outils de suivi des composants)
SCADA	Supervisory Control And Data Acquisition
SCI	Système de contrôle industriel
SCRLC	Supply Chain Risk Leadership Council
SDLC	Secure Development Lifecycle (cycle de vie de développement sécurisé)
SSE SOC	Security Service Edge
TIC	Technologies de l'information et des communications (secteur)
TO	Technologies opérationnelles
ZOMBIE	Réseau de zombies (attaque)

[i] https://ised-isde.canada.ca/site/services-mobiles/fr/lettre-envoyee-ministre-champagne-forum-canadien-pour-resilience-infrastructures-numeriques

[ii] Global News, Rogers Outage July 8, https://globalnews.ca/tag/rogers-outage-july-8-2022/

[iii] Innovation, Sciences et Développement économique Canada, (7 septembre 2022), Programme de fiabilité des réseaux de télécommunications, https://ised-isde.canada.ca/site/services-mobiles/fr/programme-fiabilite-reseaux-telecommunications

[iv] https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-fr.aspx

[v] https://thehill.com/policy/cybersecurity/562601-chris-inglis-formally-sworn-in-as-national-cyber-director/

[vi] https://www.gov.uk/government/ministers /parliamentary-under-secretary-of-state--109

[vii] https://www.arnnet.com.au/article/698646/labor-creates-standalone-cyber-minister-new-cabinet-line-up/

[viii] Paul Stasny, (August 26, 2021), ICTC Labour Market Outlook: Additional Demand for Digital Talent to Reach 250,000 By 2025, Information and Communications Technology Council, https://www.ictc-ctic.ca/news-events/ictc-labour-market-outlook-additional-demand-for-digital-talent-to-reach-250000-by-2025.

[ix] Institut CD Howe, (23 août 2022), *The Knowledge Gap : Canada Faces a Shortage in Digital and STEM Skills,* https://www.cdhowe.org/public-policy-research/knowledge-gap-canada-faces-shortage-digital-and-stem-skills-0

[x] https://www.iso.org/ standard/82905.html

[xi] https://access.atis.org/apps/group_public/download.php/66150/ATIS-I-0000090.pdf