Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Décision de Conformité et Enquêtes et de Télécom CRTC 2022-170

Version PDF

Références : 2021-9, 2021-9-1

Ottawa, le 23 juin 2022

Dossier public : 1011-NOC2021-0009

Développement d'un cadre de blocage à l'échelle des réseaux pour limiter le trafic des réseaux de zombies et renforcer la sécurité en ligne des Canadiens

Le Conseil conclut que des mesures réglementaires sont nécessaires afin de faire en sorte que les entreprises canadiennes qui bloquent les réseaux de zombies le fassent d'une manière qui assure un niveau de protection de base aux Canadiens.

Le Conseil établit les principes directeurs fondamentaux pour un futur cadre de blocage des réseaux de zombies et demande au Comité directeur du CRTC sur l'interconnexion (CDCI) d'examiner un certain nombre de questions afin d'aider à l'élaboration des paramètres techniques qui sont conformes à ces principes directeurs, et de produire un rapport détaillant ses recommandations dans les **neuf mois** suivant la date de publication de la présente décision. Après réception du rapport du CDCI et des observations des intéressés, le Conseil a l'intention d'établir les normes minimales pour le blocage des réseaux de zombies.

Contexte

1. Le 13 janvier 2021, le Conseil a publié l'avis de consultation de Conformité et Enquêtes et de Télécom 2021-9 (avis de consultation), dans lequel il a sollicité des observations sur l'élaboration d'un cadre de blocage à l'échelle des réseaux afin de limiter le trafic des réseaux de zombies[1] et de renforcer la sécurité en ligne des Canadiens.
2. Les réseaux de zombies font partie intégrante de l'infrastructure de communication utilisée par les acteurs de cybermenace. Ils facilitent un large éventail d'activités en ligne nuisibles, y compris les violations les plus flagrantes de la Loi canadienne anti-

[1] Un réseau de zombies est un réseau d'appareils infectés par des logiciels malveillants et contrôlé en groupe à l'insu et sans le consentement de leurs propriétaires, dans un but malveillant. Le trafic des réseaux de zombies est le trafic Internet qui circule entre les appareils infectés, appelés zombies, et leurs points de contrôle, appelés serveurs de commande et de contrôle. L'utilisation du terme « réseaux de zombies » dans la présente décision et dans l'avis de consultation fait uniquement référence aux réseaux de zombies malveillants qui causent des préjudices aux Canadiens et n'inclut pas les systèmes de traitement distribués ou les prétendus bons zombies programmés pour effectuer des tâches utiles (p. ex. les robots commerciaux et les robots d'exploration du Web).

pourriel (LCAP)[2]. Ils ont des répercussions sur tout le monde, des grandes, moyennes et petites entreprises aux écoles, hôpitaux et citoyens. Ils permettent le pourriel, les attaques par déni de service distribué, le déploiement de logiciels malveillants et le vol de renseignements, tout en donnant aux attaquants un accès illimité aux réseaux au moyen des systèmes infectés.

3. Les Canadiens sont particulièrement préoccupés par les fréquentes attaques par logiciel de rançon qui ont causé d'importantes interruptions de service et des préjudices financiers. La communication des réseaux de zombies passe par les réseaux des fournisseurs de services de télécommunication (FST)[3]. Les FST sont donc particulièrement bien placés afin de mettre en œuvre le blocage à l'échelle des réseaux afin de perturber les activités nuisibles des réseaux de zombies.

4. Le Conseil a reçu des interventions de particuliers et d'Allarco Entertainment 2008 Inc.; l'Autorité canadienne pour les enregistrements Internet (CIRA); Bell Canada; Bragg Communications Incorporated, exerçant ses activités sous le nom d'Eastlink (Eastlink); un mémoire conjoint de la CIBC [Banque Canadienne Impériale de Commerce] et de plusieurs grandes banques, dont BMO Banque de Montréal, Banque Manuvie, Banque Scotia, Canada Vie, Desjardins, RBC [Banque Royale du Canada], et TD Canada Trust (ci-après, la CIBC et autres); le Centre de la sécurité des télécommunications (CST)[4]; le Centre pour la défense de l'intérêt public (CDIP); la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC); la coalition manitobaine (composée de l'Aboriginal Council of Winnipeg, de la section manitobaine de l'Association des consommateurs du Canada, et de Harvest Manitoba[5]; Cogeco Communications Inc. au nom de sa filiale Cogeco Connexion Inc. (Cogeco); le Conseil canadien de l'identification et d'authentification numériques; Distributel Communications Limited (Distributel); Électricité Canada[6]; le Groupe national de coordination contre la cybercriminalité de la Gendarmerie royale du Canada (GRC); l'Independent Telecommunications Providers Association et la Canadian Communication Systems Alliance (ITPA/CCSA); un mémoire

---

[2] La *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, L.C. 2010, ch. 23, est habituellement appelée la Loi canadienne anti-pourriel (LCAP).

[3] Le terme « FST », défini dans la *Loi sur les télécommunications* comme étant la personne qui fournit des services de télécommunication de base, désigne à la fois les fournisseurs dotés d'installations et les revendeurs, et inclut les fournisseurs de services Internet.

[4] Le CST est l'autorité technique en matière de cybersécurité au Canada et l'opérateur du Centre canadien pour la cybersécurité (CCC).

[5] La coalition manitobaine a tenu deux séances de discussion avec les consommateurs dans le contexte de l'avis de consultation et a fait état des points de vue de diverses personnes dans son mémoire.

[6] Électricité Canada était auparavant appelée l'Association canadienne de l'électricité. Son intervention dans le cadre de la présente instance a été faite sous ce nom. Au début de l'année 2022, elle a changé son nom pour Électricité Canada. Par souci de commodité, Électricité Canada est utilisée dans la présente décision.

conjoint de Crypto Québec, Hackfest Communication et INFOSECSW (collectivement INFOSECSW); l'Internet Society; Lumen Technologies, Inc.; le Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG); Nokia Canada Inc. (Nokia); Open-Xchange AG; Québecor Média inc. au nom de Vidéotron ltée (Vidéotron); Rogers Communications Canada Inc. (RCCI); Saskatchewan Telecommunications (SaskTel); Shaw Communications Inc. (Shaw); Stealth Network Services; TekSavvy Solutions Inc. (TekSavvy); TELUS Communications Inc. (TCI); Vaxination Informatique; et Xplornet Communications Inc. et sa filiale Xplore Mobile Inc. (Xplornet).

Demandes de renseignements

5. Le personnel du Conseil a envoyé des demandes de renseignements aux FST qui sont intervenus dans l'avis de consultation, à savoir Bell Canada, Cogeco, Distributel, Eastlink, RCCI, SaskTel, Shaw, TCI, TekSavvy, Vidéotron et Xplornet.

6. Étant donné que les interventions que le Conseil a reçues des FST suggèrent qu'ils ont déjà mis en place des mesures pour réduire le trafic des réseaux de zombies et, dans certains cas, remédier aux infections par des logiciels malveillants associés, le but des demandes de renseignements était de comprendre la portée des activités existantes de lutte contre les réseaux de zombies effectuées par les FST. Elles visaient également à faire en sorte que des renseignements supplémentaires sur la nature, la portée et les conditions du blocage des réseaux de zombies effectué à ce jour par les FST soient inclus par ces derniers dans le dossier public.

7. Tous les FST énumérés au paragraphe 5 ont déposé des réponses aux demandes de renseignements.

8. Le Conseil a reçu des réponses à la demande de renseignements de six parties soit : Marc Nanni, Bell Canada, RCCI, TCI, TekSavvy et Vaxination Informatique.

9. Le processus public a été clôturé à la fin de la période de réponse à la demande de renseignements, le 12 août 2021.

Questions

10. Le Conseil a déterminé qu'il devait examiner les principales questions suivantes dans la présente décision :

    - Le problème du trafic des réseaux de zombies nécessite-t-il des mesures réglementaires?

    - Si le problème du trafic des réseaux de zombies nécessite des mesures réglementaires, quel type de mesure réglementaire serait approprié?

    - Quels sont les paramètres techniques d'un cadre de blocage?

Le problème du trafic des réseaux de zombies nécessite-t-il des mesures réglementaires?

Ampleur du problème posé par le trafic des réseaux de zombies

Position du Conseil dans l'avis de consultation

11. Dans l'avis de consultation, le Conseil a souligné pourquoi les réseaux de zombies et leur trafic constituent un problème. La cyberactivité malveillante vise les consommateurs et les entreprises du Canada, ainsi que les organisations qui fournissent des services essentiels comme les hôpitaux, les écoles et les organismes gouvernementaux. Cette activité malveillante compromet la vie privée et porte atteinte à l'intégrité et à la disponibilité des réseaux. Elle impose également des coûts aux victimes et mine la confiance des Canadiens dans l'utilisation des communications électroniques pour mener leurs activités en ligne.

12. Cette activité malveillante s'appuie généralement sur des réseaux de zombies afin de permettre à un attaquant d'accéder à des réseaux privés tout en préservant son anonymat. Les Canadiens sont particulièrement préoccupés par les fréquentes attaques de logiciels de rançon, qui ont causé d'importantes interruptions de service et des préjudices financiers.

Positions des parties

13. La majorité des parties s'accordent à dire que les réseaux de zombies continuent de représenter un problème important de cybersécurité[7], tant en termes de volume de trafic que de gravité des préjudices. La CIBC et autres ainsi que SaskTel ont indiqué qu'elles estiment que les comptes de zombies malveillants représentent de 20 à 30 % de l'ensemble du trafic Internet, et ont ajouté que ces zombies ont déjà causé des préjudices importants à l'économie et à la sécurité nationale. SaskTel a ajouté que le trafic des réseaux de zombies est indésirable pour ceux qui gèrent les réseaux.

14. Distributel a indiqué que les réseaux de zombies continuent d'être un problème mondial malgré les ressources importantes allouées pour y remédier.

15. L'Internet Society a fait valoir que les Canadiens ont de plus en plus besoin de solutions pour faire face à l'activité des réseaux de zombies et aux tendances plus générales des cyberattaques, notamment pendant la pandémie de COVID-19, car une grande partie des activités quotidiennes se déroulent en ligne.

---

[7] La cybersécurité désigne l'ensemble des technologies, processus, pratiques et mesures d'intervention et d'atténuation conçus afin de se protéger contre les cyberattaques et garantir la confidentialité, l'intégrité et la disponibilité des renseignements électroniques. Une cyberattaque est l'utilisation de moyens électroniques pour interrompre, manipuler, détruire ou obtenir un accès non autorisé à un système, un réseau ou un appareil informatique.

16. Le CDIP a indiqué que les réseaux de zombies portent atteinte au droit fondamental des Canadiens à la vie privée, menacent les emplois et ébranlent la confiance du public dans les services en ligne.

17. Malgré les changements de comportement en ligne entraînés par la pandémie, Nokia a fait valoir que les réseaux de cinquième génération et la prolifération des appareils en matière de l'Internet des objets signifient que les attaques de réseaux de zombies sont susceptibles d'être beaucoup plus importantes et plus puissantes si elles ne sont pas contrôlées.

18. Bell Canada, RCCI et TCI s'entendent pour dire que les réseaux de zombies malveillants causent des préjudices aux Canadiens, mais remettent en question leur prévalence.

19. Bien que Bell Canada, RCCI et TCI aient indiqué, dans leurs réponses aux demandes de renseignements, qu'elles estiment la cybersécurité comme une priorité, elles ont ajouté que le pourcentage du trafic de leurs réseaux qu'elles ont attribué à des réseaux de zombies ou à des logiciels malveillants au cours des cinq dernières années n'est pas disponible. Bell Canada, RCCI et TCI ont fait référence au très faible pourcentage de Xplornet, soit 0,0002 %, pour appuyer leur argument selon lequel il n'y a aucun élément de preuve d'un problème qui justifie une intervention réglementaire.

Résultats de l'analyse du Conseil

20. Le Conseil fait remarquer que la majorité des parties ont estimé que les réseaux de zombies constituent un problème de cybersécurité important. Ce point de vue est soutenu par les universitaires et les spécialistes en matière de cybersécurité qui sont intervenus dans la présente instance, et s'harmonise avec la position stratégique adoptée par les régulateurs et les gouvernements de pays du monde entier, notamment l'Allemagne, l'Australie, la Corée du Sud, les États-Unis, la Finlande, le Japon, la Norvège, les Pays-Bas et le Royaume-Uni.

21. Alors que quelques parties ont fait valoir que les réseaux de zombies ne constituent pas un problème important, les facteurs suivants suggèrent le contraire :

    - Les statistiques fournies par Nokia donnent une vue d'ensemble des infections des appareils. Le Conseil estime que rien ne permet de déterminer que les chiffres au Canada seraient sensiblement inférieurs ou supérieurs aux chiffres mondiaux. Les statistiques mondiales de Nokia peuvent donc donner un aperçu supplémentaire de l'ampleur du problème au sein des abonnements canadiens aux appareils mobiles et à large bande. Nokia a mesuré un taux d'infection mensuel des appareils mobiles compris entre 0,2 % et 0,5 % entre 2017 et 2020. Si l'on ajoute à cela les données sur l'utilisation des téléphones intelligents au Canada, on peut en déduire qu'il pourrait y avoir entre 61 000 et 153 000 appareils mobiles infectés au Canada au cours de quelconque mois donné. Nokia a démontré que le nombre de foyers connectés à Internet possédant un appareil infecté a baissé entre 2017 et 2020. Les taux d'infection

des réseaux résidentiels fixes de 6 % à 3,2 % pour la période de 36 mois entre 2017 et 2020 identifiés par Nokia se traduisent par un nombre total de foyers canadiens possédant au moins un appareil infecté par un logiciel malveillant compris entre 910 000 et 485 000 au cours de cette période.

- Les estimations auxquelles font référence la CIBC et autres ainsi que SaskTel suggèrent que le trafic des réseaux de zombies représente 20 à 30 % du trafic Internet total.

- Les projections basées sur les parts de marché de huit des onze FST canadiens participants (Bell Canada, Cogeco, Eastlink, RCCI, SaskTel, Shaw, TCI et Vidéotron) pour le premier trimestre de 2021 suggèrent que les Canadiens ou les appareils au Canada tentent d'accéder à des domaines malveillants à un rythme d'environ sept millions de tentatives par jour.

22. Le Conseil reconnaît que les sites Web malveillants consultés par les Canadiens, en pourcentage du total des sites Web visités, peuvent être faibles en termes absolus. Toutefois, étant donné que la visite d'un seul domaine malveillant suffit à faire progresser l'infection d'un appareil ou à entraîner un vol d'identifiants, le Conseil estime que même le ratio relativement faible détecté par les FST est important.

23. Compte tenu de ce qui précède, le Conseil conclut que le trafic des réseaux de zombies constitue un problème important en matière de cybersécurité, tant en termes de volume que de gravité des préjudices.

Des mesures réglementaires sont-elles nécessaires?

Position du Conseil dans l'avis de consultation

24. Dans son avis de consultation, le Conseil a invité les intéressés à lui faire part de leurs observations sur la pertinence et l'efficacité des mécanismes de réglementation actuels qui seraient utilisés pour remédier au préjudice causé par les réseaux de zombies.

Positions des parties

Parties en faveur d'une intervention réglementaire

25. Bien que leurs points de vue particuliers aient une portée différente, un nombre de particuliers ainsi que le CDIP, la CIBC et autres, la CIRA, la coalition manitobaine, le CST, Électricité Canada, la GRC, Open-Xchange AG, SaskTel, Shaw, TekSavvy et Vidéotron ont tous appuyé l'intervention réglementaire du Conseil. Le soutien de ces parties découle de la reconnaissance de la nature persistante et criminelle des réseaux de zombies, ainsi que de la prévalence croissante et des répercussions négatives des réseaux de zombies sur l'économie canadienne.

26. Le CST, Électricité Canada et la GRC ont tous convenu que le blocage par les FST contribuerait à lutter contre les cybermenaces auxquelles les Canadiens sont confrontés et à diminuer l'exposition des Canadiens aux risques associés. La CIBC et autres ont indiqué que ce sont les consommateurs canadiens qui sont les plus exposés aux risques lorsqu'il s'agit de pertes dues à la fraude, y compris la fraude perpétrée par des réseaux de zombies. Les grandes entreprises disposent des compétences et des ressources nécessaires pour réagir aux réseaux de zombies et aux cyberattaques, ce qui n'est souvent pas le cas des citoyens. Benoit Dupont, la coalition manitobaine et Open-Xchange AG ont caractérisé les défis auxquels sont confrontés les citoyens en arguant que la sophistication des réseaux de zombies les rend résistants aux antivirus classiques et aux autres outils de suppression disponibles pour les utilisateurs finals, et que ces derniers n'ont souvent pas les compétences nécessaires pour comprendre les risques présentés par les réseaux de zombies.

27. TekSavvy était initialement opposée à une intervention réglementaire et affirmait que le blocage à l'échelle des réseaux serait inefficace et inapproprié, et qu'il briserait l'Internet. Elle est ensuite revenue sur sa position en se fondant sur les interventions déposées par d'autres FST, qui indiquaient que la plupart d'entre eux bloquaient déjà les réseaux de zombies et autres cybermenaces depuis de nombreuses années. Dans sa réponse définitive, TekSavvy a indiqué que les réponses à la demande de renseignements ont confirmé et amplifié le besoin évident d'une surveillance indépendante et fondée sur des principes des activités de blocage largement entreprises par les FST. TekSavvy a demandé au Conseil d'établir un cadre minimal basé sur des incitations.

28. Le CDIP, la CIRA et TekSavvy ont plaidé en faveur d'une intervention réglementaire étant donné que les FST bloquent déjà le trafic malveillant, mais, selon eux, ils le font sans l'autorisation requise du Conseil en vertu de l'article 36 de la *Loi sur les télécommunications* (*Loi*). La CIRA a défendu les activités de blocage des FST en arguant que l'écosystème de l'Internet comprend un trafic malveillant qui empêcherait l'Internet de fonctionner s'il n'était pas traité. Elle a conclu que le Conseil devrait accorder aux FST une autorisation limitée pour bloquer le trafic malveillant.

29. Les parties en faveur d'une intervention réglementaire et les parties neutres ont souligné le manque de renseignements concernant les pratiques actuelles des FST. Par exemple, la CIPPIC s'est abstenue de tout commentaire sur la nécessité d'une intervention réglementaire, en partie parce que les pratiques de blocage actuelles des FST sont largement inconnues. La coalition manitobaine a indiqué que certains participants au groupe de discussion qu'elle a dirigé, en particulier les personnes âgées, semblaient croire que le blocage du trafic des réseaux de zombies était déjà systématiquement mis en œuvre par les FST.

30. Bien que le CDIP ait indiqué qu'un certain niveau d'intervention du Conseil pourrait être approprié, il a fait remarquer qu'une telle intervention présente des préjudices potentiels pour la neutralité du réseau. La coalition manitobaine a

suggéré qu'une exception à la neutralité du réseau peut seulement être acceptable si elle est étroitement limitée à son but prévu, peu intrusive, très réactive et est efficace.

Parties opposées à une intervention réglementaire

31. Des particuliers, Bell Canada, Eastlink, INFOSECSW, l'Internet Society, l'ITPA/CCSA, RCCI, TCI et Xplornet ont argué que l'intervention réglementaire n'est pas nécessaire. En particulier, Bell Canada, RCCI et TCI ont rejeté l'idée d'un régime de blocage obligatoire. Les parties opposées à une intervention réglementaire ont soutenu que la flexibilité actuelle offerte par la collaboration est plus adaptable que la réglementation, qu'il existe déjà une autorité réglementaire pour bloquer les réseaux de zombies, que les efforts de blocage actuels suivent déjà les meilleures pratiques de l'industrie et que d'autres parties peuvent contribuer aux stratégies d'affaiblissement des réseaux de zombies plus que les FST ne le peuvent.

32. Selon Bell Canada et RCCI, plusieurs FST (Bell Canada, RCCI, SaskTel, Shaw, TCI et Vidéotron) partagent déjà les indicateurs de compromission (IC)[8] des réseaux de zombies et des logiciels malveillants au moyen des sous-groupes de travail et d'autres forums du Comité consultatif canadien pour la sécurité des télécommunications (CCCST)[9].

33. Fenwick McKelvey et Reza Rajabiun (dans une intervention conjointe), Bell Canada et RCCI ont indiqué que le statu quo (c.-à-d. que les FST s'occupent des réseaux de zombies et des logiciels malveillants en assurant la liaison entre eux, avec les ministères et avec les responsables de l'application de la loi) fonctionne bien et qu'il n'est pas nécessaire de d'améliorer le mécanisme actuel. L'Internet Society et TCI étaient d'accord pour dire que la coopération est la bonne façon de s'attaquer aux réseaux de zombies, mais elles ajoutent que le problème des réseaux de zombies bénéficierait d'une collaboration plus large.

34. Les parties opposées à une intervention réglementaire obligatoire ont également argué qu'un cadre formel n'est pas nécessaire puisque l'environnement

---

[8] Un IC est un élément de données criminalistiques, également appelé artefact, observé sur un réseau ou dans un système informatique qui indique, avec un haut degré de confiance, une intrusion dans ce système et, plus largement, qu'une activité malveillante est en cours. En d'autres termes, les IC sont des identifiants associés aux cyberattaques. Les IC typiques sont les signatures de virus et les adresses IP, les hachages MD5 [Message Digest 5] des fichiers malveillants et les adresses Internet ou les noms de domaine des serveurs de commande et de contrôle des réseaux de zombies. Les chercheurs en matière de sécurité utilisent les IC afin de mieux analyser les techniques et les comportements d'un logiciel malveillant particulier. Les IC fournissent également de l'information exploitable concernant les menaces, qui peuvent être partagés au sein de la communauté afin d'améliorer encore plus les stratégies de réponse aux incidents et de remédiation.

[9] Le CCCST est un comité consultatif qui permet aux secteurs privé et public d'échanger des renseignements et de collaborer stratégiquement sur les questions actuelles et en évolution qui peuvent avoir une incidence sur l'infrastructure des télécommunications, y compris les menaces en matière de cybersécurité. Le CCCST comprend le Groupe de travail sur la protection cybernétique des télécommunications canadiennes, qui a élaboré des pratiques exemplaires pour les FST canadiens.

réglementaire actuel permet de bloquer à l'échelle des réseaux les menaces en matière de sécurité telles que les réseaux de zombies. Cependant, les parties se sont appuyées sur différents mécanismes réglementaires pour soutenir le blocage. La plupart des parties, tant celles qui s'opposent à des mesures réglementaires obligatoires (p. ex. RCCI et TCI) que celles qui y sont favorables (p. ex. la CIBC et autres et Shaw), étaient d'avis que dans la politique réglementaire de télécom 2009-657, le Conseil a permis aux FST de bloquer le trafic des réseaux de zombies à l'échelle des réseaux.

35. Bell Canada a affirmé qu'il n'est pas clair si le Conseil a l'autorité requise, que ce soit en vertu de la LCAP ou de la *Loi*, pour mettre en œuvre un régime de blocage obligatoire des réseaux de zombies. En outre, elle a fait valoir que la LCAP autorise expressément les FST à modifier les données de transmission et à, ainsi, bloquer le trafic à des fins de gestion du réseau.

36. Un autre facteur mis de l'avant par les parties opposées à une intervention réglementaire est l'utilisation actuelle des meilleures pratiques de l'industrie des télécommunications, telles que celles du Broadband Internet Technical Advisory Group (BITAG), du CCCST et de l'Internet Engineering Task Force. Les parties ont affirmé que ces meilleures pratiques fournissent déjà les recommandations nécessaires afin de mettre en œuvre le blocage des réseaux de zombies.

37. Xplornet s'est dite préoccupée par le fait qu'un cadre de blocage des réseaux de zombies cultiverait un faux sentiment de confiance chez les Canadiens et d'autres parties prenantes qui n'étaient pas des FST, les amenant à croire que les Canadiens sont entièrement protégés contre les activités malveillantes en ligne et qu'ils n'ont pas besoin d'exercer une bonne cyberhygiène. Des préoccupations semblables exprimées par d'autres parties opposées à une intervention réglementaire ont suggéré que d'autres entités peuvent mieux contribuer à une stratégie d'affaiblissement des réseaux de zombies, notamment :

    i. les utilisateurs finals, qui peuvent utiliser les solutions existantes afin de sécuriser leurs appareils et leur connexion Internet (mises à jour de sécurité, solutions payantes d'antivirus et de pare-feu fournies par les FST et les fournisseurs de sécurité, le programme Bouclier canadien de la CIRA[10], etc.);

    ii. d'autres fournisseurs de l'écosystème Internet, tels que les fabricants d'appareils (p. ex. les fabricants d'appareils de l'Internet des objets) et les fournisseurs de logiciels, qui peuvent s'assurer qu'ils ne vendent pas de produits dotés de logiciels obsolètes ou vulnérables;

---

[10] Le Bouclier canadien de la CIRA est un mécanisme de blocage à l'échelle des réseaux fourni en collaboration entre Akamai Technologies, le CCC et la CIRA. Il s'agit d'un service de blocage basé sur le domaine, offert gratuitement à tous les Canadiens, sur la base d'une approche à option d'adhésion. Les utilisateurs choisissent d'y adhérer en configurant leur routeur pour qu'il envoie les recherches de domaines au résolveur de la CIRA.

iii. le gouvernement fédéral, qui peut réglementer les autres fournisseurs mentionnés au paragraphe 37ii. et soutenir la sensibilisation des utilisateurs afin d'empêcher les infections de zombies de se produire en premier lieu;

iv. les organismes responsables de l'application de la loi, qui peuvent développer des réseaux de coopération internationale pour s'attaquer aux réseaux de zombies à leur source.

38. Les parties opposées à une intervention réglementaire, dont Samuel Harper, Karine Leduc, Marc Nanni et INFOSECSW, ont argué que ce projet nuira, ou ira clairement à l'encontre, de la liberté d'expression et du principe de neutralité du réseau reconnu par le Conseil.

Réponses aux demandes de renseignements

39. Tout au long de leurs observations dans le cadre de la présente instance, la plupart des FST ont répondu, implicitement ou explicitement, qu'ils collaborent les uns avec les autres et qu'ils ont mis en place des systèmes de blocage particuliers afin de lutter contre les logiciels malveillants et le pourriel.

40. Outre les renseignements déposés à titre confidentiel par les FST, Shaw et Xplornet ont indiqué qu'elles utilisent également des méthodes automatisées pour partager les IC des réseaux de zombies. Shaw a ajouté qu'elle partage les IC avec le CCCST et le Centre canadien pour la cybersécurité (CCC), mais Xplornet a indiqué qu'elle ne partage que les IC avec des FST interconnectés non identifiés qu'une fois par jour. Vidéotron a fait valoir qu'elle prévoit d'automatiser son partage, mais n'a pas fourni d'échéancier. Cogeco, Distributel et TekSavvy ont signalé qu'elles ne partagent pas les IC des réseaux de zombies. Cogeco a précisé que, en cas de détection, elle partage parfois les IC associés à l'hameçonnage, aux domaines malveillants ou à d'autres cybermenaces avec toute partie prenante concernée, y compris les développeurs de logiciels ou de matériel, sur une base manuelle ou *ad hoc*.

41. Tous les FST, à l'exception de Cogeco, Distributel et SaskTel, ont fourni des réponses indiquant qu'elles bloquent actuellement le trafic des réseaux de zombies. Shaw a précisé que ses options de blocage ne sont pas mises à la disposition des abonnés de sa marque complémentaire Freedom.

42. Eastlink a indiqué qu'elle utilise une liste de blocage d'une tierce partie afin de détecter et bloquer le trafic des réseaux de zombies sur son infrastructure de serveurs de noms de domaine. RCCI a indiqué qu'elle utilise un système de blocage exclusif, mais n'a pas précisé quelles méthodes elle utilise. Shaw a présenté ses trois différents systèmes de blocage soit i) un service gratuit de blocage de domaine avec option d'adhésion, qui s'appuie sur une liste de blocage d'une tierce partie; ii) une solution payante pour les utilisateurs finals, vendue comme un complément afin de bloquer les tentatives d'accès non autorisés; et iii) une solution de sécurité payante pour ses petites et moyennes entreprises clientes, qui comprend le filtrage de domaine et une solution antivirus.

43. Les FST ont également identifié un nombre de tiers différents qu'ils utilisent pour surveiller le trafic et faciliter le blocage ou les notifications aux clients. Les listes de blocage de tiers identifiées par les FST variaient, mais toutes comprenaient un éventail plus large d'IC qui ne se limitaient pas aux réseaux de zombies. Le coût de l'abonnement à ces listes de blocage variait également.

44. En réplique aux réponses à la demande de renseignements, Jonathan Curtis a déclaré que les FST ont un long historique de filtrage et de blocage du pourriel, qui remonte à 1996. Marc Nanni s'est dit préoccupé par l'utilisation de listes de blocage de tiers et a ajouté que RCCI, Shaw et Vidéotron utilisent toutes trois Comcast X1/Xfinity, basé aux États-Unis, pour le blocage de tiers. Marc Nanni a également fait référence à des publications montrant l'utilisation de Zvelo par Shaw et l'utilisation par Bell Canada d'une solution de blocage appelée Bell-Environics.

Résultats de l'analyse du Conseil

45. Le Conseil estime que des mesures réglementaires sont nécessaires, car :

- Les pratiques actuelles des FST sont diverses et ne sont pas transparentes et nécessitent un mécanisme pratique et conforme pour partager les IC des réseaux de zombies;
- Les FST sont particulièrement bien placés pour s'attaquer à l'activité des réseaux de zombies;
- Le blocage à l'échelle des réseaux est efficace et approprié;
- Il existe une confusion entre les parties concernant la base réglementaire du blocage actuel des réseaux de zombies par les FST.

Les pratiques actuelles des FST sont diverses et ne sont pas transparentes et nécessitent un mécanisme pratique et conforme pour partager les IC de réseaux de zombies

46. Alors que les parties opposées à une intervention réglementaire se sont largement appuyées sur les pratiques existantes de partage volontaire et de collaboration, les réponses des FST à la demande de renseignements n'ont fourni aucun élément de preuve de l'existence d'un mécanisme pratique ou conforme de partage des IC des réseaux de zombies au sein de la communauté des FST. Seuls quelques FST partagent les IC des réseaux de zombies. Dans ces cas limités, le partage se fait généralement de manière manuelle et *ad hoc*.

47. Le Conseil reconnaît la nécessité d'une collaboration au moyen de groupes de travail comme le CCCST ou le Groupe de travail sur la protection cybernétique des télécommunications canadiennes du CCCST. Ce sont des forums essentiels afin de partager l'information sur les tendances et discuter d'une stratégie générale, de l'architecture et de questions opérationnelles ou politiques particulières. Toutefois, le Conseil estime que ce type de coopération est insuffisant pour le partage des IC de réseaux de zombies ou de logiciels malveillants. Les IC sont très dynamiques et

le transfert informel des IC sur une base *ad hoc* n'est ni efficace ni efficient. Un IC peut même devenir obsolète avant la fin de la séance du groupe de travail. Les techniques comme le *fast flux*[11] employées par les réseaux de zombies peuvent faire correspondre un domaine à des milliers d'adresses du protocole Internet (IP) qui changent de seconde en seconde. Les réseaux de zombies modernes peuvent également utiliser des algorithmes de génération de domaines afin de générer des listes quasi infinies de domaines de commande et de contrôle possibles. Grâce à ces techniques et à d'autres, un haut degré d'automatisation est nécessaire pour que les listes d'IC soient mises à jour et appliquées de manière cohérente et en temps réel par l'ensemble de la communauté des FST.

48. En outre, presque tous les aspects des activités de blocage des FST diffèrent dans l'industrie. Les différents FST bloquent différentes menaces, en utilisant différentes méthodes et listes de blocage. Conformément à la recommandation du CST, on s'appuie beaucoup sur des listes qui détectent un spectre plus large des IC (c.-à-d. non seulement les réseaux de zombies, mais aussi les pourriels et les logiciels malveillants, qu'ils soient distribués par des réseaux de zombies ou non). Il existe également des exemples, comme le BlueCurve de Shaw, où les abonnés qui optent pour le blocage doivent consentir à certaines formes de blocage de contenu, tels que les sites Web estimés comme violant les droits d'auteur, comme condition au blocage à des fins de sécurité. Les FST bloquent le trafic des réseaux de zombies à l'aide de listes de blocage exclusives ou de listes de blocage d'une tierce partie différentes, mais ils se fient à des tiers choisis à leur propre discrétion. Les organisations en matière d'information concernant les menaces chargées d'élaborer et de tenir à jour les listes de blocage de tiers sont exclusivement non nationales et principalement basées aux États-Unis. Les FST n'ont pas précisé si les listes de blocage sont accréditées afin de garantir leur robustesse ou vérifiées en vue d'évaluer leur efficacité avec le temps. Il n'est pas certain que les listes de blocage utilisées sont efficaces pour empêcher l'accès aux appareils infectés situés au Canada.

49. Bien que le Conseil reconnaisse que la variabilité présente des avantages, il estime également que les abonnés canadiens aux services Internet bénéficieraient d'une solution qui assure un degré de sécurité de base et bloque les menaces visant la population canadienne. La solution la plus notable, basée au Canada, est le Bouclier canadien de la CIRA. Les FST canadiens n'ont pas identifié le Bouclier canadien de la CIRA comme l'une des solutions qu'ils utilisent.

50. Les FST ont argué que leurs méthodes de blocage suivent les meilleures pratiques, mais le Conseil fait remarquer un certain nombre d'incohérences. L'écart le plus notable par rapport aux meilleures pratiques concerne la manière dont les FST suivent et classent les événements bloqués. Les meilleures pratiques du CCCST recommandent de suivre les événements bloqués et de classer les types d'infections associés, et l'article 4 du document Internet Engineering Task Force

---

[11] Le *fast flux* consiste à échanger des adresses IP dans et hors des enregistrements dans un système des noms de domaine (DNS) à une fréquence extrêmement élevée.

Recommendations for the Remediation of Bots in ISP Networks, RFC 6561 (en anglais seulement) souligne les raisons pour lesquelles ces activités sont essentielles afin de lutter contre les réseaux de zombies[12]. Cependant, les réponses à la demande de renseignements ont montré que la plupart des FST qui ont répondu ne suivent pas les événements bloqués. Parmi les FST qui ont indiqué qu'ils suivent les infections, seul un FST a indiqué les classer.

51. Bien que les politiques en matière des meilleures pratiques du CCCST fournissent une direction importante et précieuse concernant la sécurisation des infrastructures de communication critiques, le Conseil constate des lacunes importantes, par exemple :

- les meilleures pratiques du CCCST ne précisent pas les normes qui doivent être respectées afin d'atteindre les buts, mais suggèrent plutôt des capacités que le FST doit développer;
- bien qu'il existe une distinction entre la protection des réseaux des FST et la protection des utilisateurs finals contre les menaces en matière de cybersécurité, il semble dans l'ensemble des documents du CCCST que la protection des utilisateurs finals est vue comme une caractéristique facultative[13];
- les meilleures pratiques du CCCST n'abordent pas certaines approches communément reconnues afin de prévenir le trafic nuisible (p. ex. le pourriel transitant par les réseaux des FST), comme le blocage du trafic sortant du protocole SMTP (Simple Mail Transport Protocol).

52. Le Conseil a également examiné d'autres meilleures pratiques auxquelles les parties ont fait référence, notamment le rapport du BITAG publié en 2013 (en anglais seulement), qui a démontré que certains ports font couramment fonctionner des services qui sont vulnérables aux mauvaises utilisations relatives à Internet[14].

---

[12] Ces raisons sont les suivantes : i) confirmer et corroborer les infections par des zombies à l'aide de plusieurs points de données, ii) réduire au minimum la possibilité d'une identification de faux positifs des hôtes, iii) confirmer l'intention ou la nature malveillante de l'infection, iv) estimer la gravité de la menace que représente l'infection, v) déterminer les méthodes potentielles de remédiation future, et vi) permettre une surveillance continue pour tenir compte de la nature dynamique typique des réseaux de zombies.

[13] Par exemple, le rapport indique que « ces politiques ou normes ne limitent en rien la capacité d'un FSTC [fournisseur de services de télécommunication canadien] de restreindre les fonctionnalités qui sont disponibles à un tel niveau de service ou d'exiger des frais pour ces fonctionnalités. »

[14] L'expression « blocage de port », utilisé dans le rapport du BITAG, fait référence à la pratique d'un FST consistant à identifier le trafic Internet par un protocole de transport particulier et un numéro de port (un nombre entier qui indique de manière unique un service particulier à l'extrémité d'un flux de communication), et à le bloquer entièrement. Les communications par protocole SMTP sur le port 25 sont un exemple de protocole de transport et de port qui sont bloqués par certains FST afin d'éviter les mauvaises utilisations du réseau, comme le pourriel.

53. En réponse aux demandes de renseignements, un seul FST a affirmé bloquer certains ports à des fins de sécurité, conformément au rapport du BITAG. Cependant, l'examen du mémoire de TCI et des divulgations (en anglais seulement) de Bell MTS et TekSavvy, ainsi que les forums de soutien technique de plusieurs autres FST canadiens qui comprennent des commentaires d'abonnés, suggèrent que cette pratique est plus fréquente. Parallèlement, au moyen de leurs politiques d'utilisation acceptable, les FST cherchent à limiter les communications sur certains ports généralement associés à des mauvaises utilisations du réseau.

54. Enfin, étant donné l'absence de paramètres de base pour classer les résultats des activités de blocage des FST, le Conseil n'est pas en mesure de pleinement étudier l'efficacité des mécanismes actuels de blocage des réseaux de zombies.

Les FST sont particulièrement bien placés pour s'attaquer à l'activité des réseaux de zombies

55. Bien que le Conseil reconnaisse que d'autres parties prenantes ont un rôle à jouer dans l'affaiblissement des réseaux de zombies, la présente instance se limite au blocage des réseaux de zombies par les FST, car c'est cette activité qui relève du champ d'application de la *Loi*. Le Conseil estime qu'une obligation pour les FST engagés dans le blocage des réseaux de zombies de fournir un niveau de protection de base compléterait, sans les remplacer ni les limiter, d'autres initiatives en vue de lutter contre les réseaux de zombies, telles que la collaboration, la sensibilisation, l'élaboration de politiques et la notification aux utilisateurs finals.

56. Dans le même ordre d'idées, le Conseil estime qu'aucune entité du paysage de la cybersécurité, y compris les FST, ne peut résoudre seule le problème des réseaux de zombies. Les réponses aux réseaux de zombies, compte tenu de leur complexité, de leur persistance et de leurs répercussions, sont généralement estimées comme nécessitant une approche de « défense en profondeur »[15]. Dans le cadre de cette approche, plusieurs couches de contrôles en matière de sécurité sont combinées pour se protéger contre les points de défaillance uniques.

57. Jusqu'à présent, la majeure partie du fardeau de la sécurisation des appareils contre les menaces de logiciels malveillants incombait aux utilisateurs finals. Bien qu'il soit vrai que les utilisateurs finals sont les mieux placés afin de lutter contre les infections par des logiciels malveillants à la source, ils ont une liste impressionnante de responsabilités à assumer s'ils veulent y parvenir. Par exemple, ils doivent installer et mettre à jour des solutions antivirus, effectuer des mises à jour logicielles régulières, installer et gérer un pare-feu, utiliser des mots de passe robustes, activer l'authentification à deux facteurs et sécuriser leur connexion sans

---

[15] Le guide d'étude officiel du Certified Information Systems Security Professional (en anglais seulement) indique que « la défense en profondeur, également connue sous le nom de superposition, est l'utilisation de plusieurs contrôles dans une série. Aucun contrôle ne peut protéger contre toutes les menaces possibles. L'utilisation d'une solution multicouche permet de mettre en place de nombreux contrôles différents afin de se protéger contre toute menace qui se présente. » [traduction]

fil, tout en maintenant une vigilance constante contre les menaces en ligne dans un environnement de menaces en constante évolution.

58. En réalité, la plupart des utilisateurs finals dont l'appareil est infecté par un logiciel malveillant n'ont pas conscience de l'infection. Même lorsqu'ils en sont informés, ils n'ont souvent pas les compétences techniques nécessaires pour remédier au problème et prévenir de futurs incidents, ou ne réagissent pas à l'infection parce qu'ils ne sont pas conscients des risques associés aux réseaux de zombies. Un autre élément à prendre en compte est que de nombreux utilisateurs finals possèdent plusieurs appareils et ne peuvent pas se permettre le coût supplémentaire d'un logiciel antivirus ou d'un pare-feu basé sur l'hôte sur chaque machine de leur réseau domestique. Même si ce n'était pas le cas, les appareils de l'Internet des objets dotés de faibles capacités informatiques et d'une capacité limitée, voire nulle, pour les mises à jour ou les solutions antivirus pourraient empêcher les utilisateurs finals, même les plus diligents, d'adopter des contrôles de sécurité appropriés.

59. Bien que les FST ne puissent pas traiter les infections de zombies à la source, leur position en tant que fournisseurs d'accès Internet signifie qu'ils constituent un point de contrôle critique pour les communications des réseaux de zombies. Ils ont une vision beaucoup plus large du problème et, par conséquent, ont plus de possibilités de perturber les canaux de communication des réseaux de zombies à leur échelle. De plus, contrairement à de nombreux utilisateurs finals, ils ont les compétences, l'expertise et la capacité de comprendre la menace des réseaux de zombies et de réagir de manière proportionnée.

60. En outre, l'article 4.1 des meilleures pratiques du CCCST reconnaît qu'il y a des cas où un FST peut détecter une infection qu'un utilisateur final ne peut pas détecter parce que les auteurs de logiciels malveillants prennent des mesures pour éviter la détection par les contrôles de sécurité de l'utilisateur final.

Le blocage à l'échelle des réseaux est efficace et approprié

61. Le Conseil estime que le blocage à l'échelle des réseaux devrait être mis en place en plus, et non à la place, d'autres initiatives (p. ex. la sensibilisation et la collaboration des consommateurs et des parties prenantes) afin d'obtenir les meilleurs résultats.

62. Le Conseil estime en outre qu'aucun contrôle de sécurité unique n'est entièrement efficace. Cela s'applique aux réseaux de zombies, car certaines techniques peuvent échapper au blocage à l'échelle des réseaux (p. ex. le *fast flux*, les algorithmes de génération de domaines et les architectures de réseaux de zombies de type poste à poste).

63. Néanmoins, le Conseil estime que le blocage à l'échelle des réseaux est un mécanisme efficace et approprié pour les raisons suivantes :

- La plupart des entreprises canadiennes ont investi des ressources dans le blocage à l'échelle des réseaux de leur propre initiative depuis de nombreuses années.

- Le Bouclier canadien de la CIRA est un succès. Malgré son faible taux d'adoption par le grand public[16], la solution a bloqué plus de 20 millions de demandes de domaines malveillants pour ses 100 000 utilisateurs au cours de ses sept premiers mois de fonctionnement. En outre, selon le site Web de la CIRA, elle a récemment conclu un partenariat avec Mozilla Firefox, en vertu duquel le service est activé par défaut pour les utilisateurs du navigateur Web. Dans le cadre de ce partenariat, le trafic Web des utilisateurs canadiens de Mozilla Firefox est filtré par défaut par l'infrastructure de blocage du Bouclier canadien de la CIRA. Cette initiative a été déployée au cours de la présente instance. Elle a commencé en juillet 2021 et elle a atteint l'ensemble des utilisateurs canadiens de Mozilla Firefox à la fin septembre 2021. Selon son site Web, la CIRA bloque depuis lors environ un domaine malveillant par utilisateur par jour.

- Le gouvernement fédéral a mis en place un blocage à l'échelle des réseaux pour son propre réseau. Le CST, qui est l'autorité technique en matière de cybersécurité au Canada et le gestionnaire de la liste de blocage du réseau du gouvernement fédéral, estime qu'un nouveau cadre de blocage à l'échelle des réseaux améliorerait le degré moyen de cybersécurité des Canadiens.

- D'autres pays ont mis en œuvre de telles solutions.

- Un mécanisme de blocage étroitement limité aurait des répercussions nettes minimes, voire inexistantes, sur la neutralité du réseau[17]. Bien que certains puissent estimer que le blocage des réseaux de zombies soit incompatible avec la neutralité du réseau dans la mesure où il bloque la fourniture de services de télécommunication, il a également un rôle à jouer dans la préservation de la neutralité du réseau. Non seulement un tel mécanisme permet de protéger l'accessibilité des services Internet, une condition nécessaire à la neutralité du réseau, mais il corrige également la distorsion créée par les réseaux de zombies dans la bande passante globale de l'Internet résultant de l'avantage significatif et injuste en faveur du trafic généré par les machines des acteurs de

---

[16] Afin d'opter pour le Bouclier canadien de la CIRA, les utilisateurs doivent configurer manuellement leur routeur pour qu'il envoie les recherches de domaine au résolveur de la CIRA, ce qui nécessite une certaine compétence technique. De nombreux Canadiens ne savent peut-être pas non plus que la CIRA offre ce service. Ces facteurs peuvent expliquer le faible taux d'adoption.

[17] La neutralité du Net est le concept selon lequel tout le trafic sur l'Internet devrait être traité de manière égale par les FST, avec peu de manipulation ou même sans manipulation, interférence, priorité, discrimination ou préférence.

cybermenace. Par conséquent, le Conseil estime que les avantages du blocage des réseaux de zombies pour les Canadiens et pour les réseaux des entreprises l'emportent sur les répercussions nettes minimes, voire inexistantes, sur la neutralité du réseau, à condition que le blocage des réseaux de zombies soit soumis à des contraintes appropriées.

Il existe une confusion entre les parties concernant la base réglementaire du blocage actuel des réseaux de zombies par les FST

64. Dans la politique réglementaire de télécom 2009-657, le Conseil a fourni aux FST des conseils sur l'utilisation des pratiques de gestion du trafic Internet (PGTI) afin de réduire ou prévenir la congestion sur leurs réseaux.

65. D'après les paragraphes 44 et 45 de la politique réglementaire de télécom 2009-657, le blocage à des fins de sécurité du réseau, y compris le blocage du trafic des réseaux de zombies, n'a pas été explicitement traité dans le cadre des PGTI. En effet, la principale justification du cadre des PGTI était de gérer la congestion du réseau plutôt que de répondre à des préoccupations en matière de sécurité. Toutefois, le Conseil a fait remarquer au paragraphe 44 que certaines PGTI étaient employées afin de protéger les utilisateurs contre les menaces pesant sur le réseau. Le Conseil était donc d'avis que ces activités étaient peu susceptibles de déclencher des plaintes ou des préoccupations en vertu de la *Loi*. Sur la base du dossier de la présente instance, le Conseil fait remarquer que les parties ont interprété le libellé du paragraphe 44 de diverses manières et qu'il existe une certaine confusion quant à l'autorité des FST à s'engager dans le blocage des réseaux de zombies conformément à la *Loi*. Le Conseil estime que les parties prenantes bénéficieraient d'une clarté supplémentaire et d'une approche cohérente du blocage des réseaux de zombies en vertu de la *Loi*.

66. Conformément à l'article 36 de la *Loi*, les entreprises canadiennes doivent obtenir l'approbation préalable du Conseil pour contrôler le contenu ou influencer le sens ou l'objet des télécommunications qu'elles acheminent pour le public. Le blocage de la transmission des réseaux de zombies peut empêcher la livraison des télécommunications à leur destinataire. Le but et l'effet ultimes du blocage de ces télécommunications par des réseaux de zombies sont d'empêcher la diffusion de contenus malveillants aux utilisateurs finals. Ainsi, en bloquant ces télécommunications de réseaux de zombies, une entreprise canadienne exerce un contrôle sur le contenu de ces télécommunications qu'elle transporte pour le public, ou influence leur but. Par conséquent, une telle activité relève de l'article 36 de la *Loi*. En ce qui concerne l'argument de Bell Canada selon lequel les entreprises sont autorisées à bloquer les réseaux zombies en vertu de la LCAP, le Conseil estime que ses pouvoirs en vertu de l'article 36 ne sont pas touchés par le paragraphe 7(2) de la LCAP[18]. Le paragraphe 7(2) ne sert qu'à exclure certaines activités menées

[18] Le paragraphe 7(2) énonce que « le paragraphe (1) ne s'applique pas si la modification est effectuée par un télécommunicateur pour la gestion d'un réseau. »

par les FST de l'interdiction énoncée au paragraphe 7(1) de la LCAP, qui concerne la modification des données de transmission d'un message électronique.

Conclusion

67. Compte tenu de ce qui précède, le Conseil conclut que des mesures réglementaires sont nécessaires, car i) les pratiques actuelles des FST sont diverses et ne sont pas transparentes et dépendent de communications manuelles et *ad hoc* inefficaces pour le partage de renseignements; ii) les FST ont un rôle important à jouer dans le blocage des réseaux de zombies, conformément à une stratégie de défense en profondeur en matière de cybersécurité; iii) les programmes de blocage à l'échelle des réseaux sont efficaces et appropriés; et iv) il existe une confusion entre les parties concernant la base réglementaire du blocage actuel des réseaux de zombies par les FST.

Si le problème du trafic des réseaux de zombies nécessite des mesures réglementaires, quel type de mesure réglementaire serait approprié?

Position du Conseil dans l'avis de consultation

68. Dans l'avis de consultation, le Conseil a sollicité des observations sur la pertinence et l'efficacité des mécanismes de réglementation énumérés.

Positions des parties

69. Jonathan Curtis; Kristin Surette; le CDIP; la CIRA; Cogeco; Eastlink; l'Internet Society; Lumen Technologies Inc.; le M3AAWG; Nokia; Open-Xchange AG; SaskTel; Shaw; TekSavvy; et Vaxination Informatique se sont prononcés contre une solution unique ou une option réglementaire descendante qui imposerait à tous les FST une solution technique rigide en vue de bloquer le trafic des réseaux de zombies. En général, cette catégorie d'interventions s'appuyait fortement sur une coopération et une sensibilisation continues. Les parties prenantes sont favorables à l'utilisation d'un code de conduite volontaire ou de principes directeurs établis par le Conseil qui accorderaient aux FST la flexibilité nécessaire afin de mettre en œuvre et adapter leurs mesures de cybersécurité comme ils l'entendent. À quelques exceptions près, ces interventions n'ont généralement pas fourni d'exemples d'engagements ou de solutions concrètes qui pourraient être mis en œuvre pour détecter et bloquer le trafic des réseaux de zombies dans le cadre de telles initiatives volontaires. Par exemple, Eastlink a suggéré que le Conseil encourage l'élaboration d'un code de conduite volontaire pour les FST, et qu'Eastlink continue de travailler avec des experts en cybersécurité et d'expérimenter différentes approches pour déterminer laquelle est la plus efficace.

70. Graeme Smith, la CIBC et autres, la coalition manitobaine, Électricité Canada et Vidéotron ont appuyé un cadre détaillé obligatoire, mais à des degrés différents. La CIBC et autres ont argué que le blocage volontaire est déjà effectué en vertu du paragraphe 44 de la politique réglementaire de télécom 2009-657 et que les

entreprises devraient déjà avoir la capacité de bloquer le trafic puisque cette capacité est comprise dans les meilleures pratiques du CCCST.

71. Shaw a indiqué que le Conseil devrait créer un cadre volontaire simple, comprenant une organisation de blocage centralisée afin de gérer une liste de blocage. Shaw a ajouté qu'étant donné les avantages universels associés au blocage des réseaux de zombies et le coût très faible de la participation à l'approche qu'elle propose, elle s'attendrait à ce que chaque FST canadien veuille profiter de la liste de blocage de la Botnet Blocking Organization proposée par Shaw afin de protéger ses clients et elle-même des préjudices.

72. Benoit Dupont a préparé une étude pour Sécurité publique Canada en 2013, et l'a déposée dans le cadre de la présente instance. L'étude, *An International Comparison of Anti-Botnet Partnerships* (en anglais seulement), présente en détail les avantages et les inconvénients du blocage volontaire par rapport au blocage obligatoire. Benoit Dupont a argué qu'une approche volontaire offre aux FST la flexibilité nécessaire pour s'adapter aux changements technologiques ou tactiques des acteurs de menaces, ce qui permet d'améliorer les performances. Le point de vue contraire est que les approches obligatoires offrent une plus grande cohérence de mise en œuvre. Benoit Dupont a indiqué que l'un des inconvénients des programmes volontaires est le manque d'uniformité ressenti par les utilisateurs finals. Benoit Dupont a ajouté que le fait que les FST participants conservent un certain degré d'indépendance quant à la manière dont les infections sont traitées rend plus difficile l'évaluation du programme dans son ensemble. Cela ne protège pas non plus contre les problèmes de parasitisme des FST qui choisissent de ne pas partager des renseignements qui pourraient être utiles à d'autres FST dans leurs efforts de lutte contre les réseaux de zombies. Benoit Dupont a argué que, malgré cela, le Conseil devrait commencer par une approche basée sur le volontariat.

73. De même, le CDIP a indiqué que toute directive volontaire devrait être réexaminée ultérieurement afin de confirmer son efficacité et de déterminer s'il existe de nouveaux éléments de preuve du préjudice que les réseaux de zombies causent aux consommateurs, qui justifieraient la conversion des directives volontaires en exigences réglementaires obligatoires.

74. Certains FST et d'autres parties ont indiqué qu'un cadre obligatoire entraînerait le transfert des coûts aux consommateurs. Bell Canada et RCCI ont argué qu'il devrait y avoir une compensation pour les coûts de mise en œuvre associés. SaskTel a indiqué que la solution devrait permettre une certaine flexibilité dans son intégration, être non bureaucratique dans son fonctionnement et son entretien, et être aussi rentable que possible afin d'éviter une augmentation des tarifs pour l'utilisateur final. La coalition manitobaine a indiqué qu'un cadre mandaté permettrait au Conseil de faire en sorte que le cadre de blocage des réseaux de zombies soit financé par l'industrie, selon l'approche de la Commission des plaintes relatives aux services de télécom-télévision.

75. Benoit Dupont a indiqué que les FST avaient peu d'intérêt à payer pour une meilleure protection contre les réseaux de zombies parce que leurs revenus ne sont pas touchés par les activités des réseaux de zombies qui ciblent les consommateurs, les institutions financières et les réseaux de publicité en ligne, alors que les coûts techniques et de service à la clientèle associés aux programmes de lutte contre les réseaux de zombies sont élevés. En outre, il y a également très peu d'éléments de preuve qui indiquent que les utilisateurs finals seraient prêts à payer plus pour une meilleure sécurité, car ils ne disposent pas de renseignements détaillés concernant le problème.

76. En ce qui concerne la portée des mesures réglementaires potentielles, un certain nombre de parties ont présenté des arguments relatifs à la question de savoir si un cadre obligatoire devrait être étendu ou non aux entreprises autres qu'un FST. Des entreprises, dont Eastlink et Vidéotron, ont indiqué que tous les FST devraient partager les coûts et le fardeau d'un programme de blocage obligatoire. Toutefois, le CDIP a indiqué qu'un cadre obligatoire pourrait injustement imposer un fardeau réglementaire aux petits FST qui n'ont peut-être pas les ressources nécessaires pour se conformer au cadre. L'ITPA/CCSA se sont également opposé à l'application de tout nouveau cadre aux petits FST, car cela augmenterait les coûts sous-jacents des services. Les préoccupations entourant la concurrence, en particulier celles des petites entreprises, empêchent toute augmentation des tarifs pour compenser ces coûts supplémentaires. Ainsi, un nouveau cadre obligatoire aurait des répercussions disproportionnées sur les petits fournisseurs de services ruraux par rapport aux grands concurrents qui sont en mesure de subventionner les coûts de ces services à partir de leurs territoires d'exploitation urbains vastes et denses.

77. Benoit Dupont a indiqué que les caractéristiques locales de l'écosystème numérique canadien doivent également être prises en considération lors de l'élaboration des politiques. Plus précisément, le mémoire de Benoit Dupont fait état d'une étude de 2010 dont les auteurs ont fait remarquer que les FST canadiens ne représentent que 42 % des sources uniques de pourriel, soit un indicateur fiable des ordinateurs infectés par les réseaux de zombies. Cette situation contraste avec les autres pays de l'Organisation de coopération et de développement économiques, dont les FST représentent en moyenne près de 80 % du pourriel. Benoit Dupont a conclu que la différence suggère qu'un partenariat canadien de lutte contre les réseaux de zombies ne devrait pas se limiter aux FST, mais devrait également inclure l'industrie des fournisseurs d'hébergement Web.

Résultats de l'analyse du Conseil

78. Après avoir examiné les observations concernant les avantages et les inconvénients liés au blocage volontaire et obligatoire, le Conseil estime que l'approche la plus appropriée dans les circonstances actuelles est de faire en sorte que, lorsque les FST fournissent un blocage des réseaux de zombies à l'échelle des réseaux, ce blocage soit assujetti à certaines normes minimales. Selon le Conseil, cette approche offrira aux FST la flexibilité d'une approche volontaire tout en faisant en sorte qu'un

niveau de protection de base soit fourni, servant l’intérêt public et en faisant avancer les objectifs de la politique de télécommunication établis dans la *Loi*.

79. Dans la section suivante, le Conseil établit les principes directeurs pour régir tout mécanisme de blocage des réseaux de zombies. Suivant des processus supplémentaires, le Conseil imposera ces normes minimales, y compris certains paramètres de base, comme conditions de son approbation de tout blocage des réseaux de zombies à l’échelle des réseaux, en vertu de l’article 36 de la *Loi*.

80. Bien que ce cadre ne s’applique qu’aux entreprises canadiennes, le Conseil encourage les entreprises autres qu’un FST à adopter une approche semblable. Si les entreprises autres qu’un FST s’engagent dans le blocage des réseaux de zombies d’une manière qui n’est pas conforme aux normes minimales établies par le Conseil, le Conseil peut examiner s’il est nécessaire et approprié d’imposer de telles normes comme conditions de service conformément à l’article 24.1 de la *Loi*.

Quels sont les paramètres techniques d’un cadre de blocage?

Techniques de blocage

Position du Conseil dans l’avis de consultation

81. Dans l’avis de consultation, le Conseil a sollicité des observations concernant les aspects techniques d’un cadre de blocage des réseaux, notamment les techniques de blocage, la sélection des résolveurs de domaines et l’adaptation aux changements technologiques.

Positions des parties

82. Fenwick McKelvey et Reza Rajabiun, Marc Nanni, Bell Canada, la CIBC et autres, le CDIP, la CIRA, le CST, Eastlink, Électricité Canada, l’Internet Society, l’ITPA/CCSA, Lumen Technologies Inc., le M3AAWG, Nokia, RCCI et SaskTel ont indiqué que le cadre doit être technologiquement neutre et offrir aux FST la flexibilité nécessaire afin de choisir une technique de blocage appropriée à l’échelle des réseaux dans une situation donnée, car aucune technique unique n’est efficace pour arrêter les réseaux de zombies. Par exemple, le CDIP et la CIRA ont suggéré que le cadre fixe des principes directeurs, tels que des principes relatifs à la transparence, à la non-discrimination, à la nécessité, à la proportionnalité, à la responsabilité, à l’exactitude et à la vie privée, plutôt que des normes de blocage technique.

83. RCCI a ajouté que si le Conseil estimait nécessaire d’imposer le blocage par les FST, il faudrait laisser ces derniers concevoir et mettre en œuvre une solution de leur choix, car ils connaissent les limites de leurs réseaux. La CIBC et autres étaient d’accord et ont suggéré que le cadre intègre un langage large afin d’assurer une flexibilité appropriée aux FST.

84. D’autres parties prenantes ont indiqué que l’intervention réglementaire du Conseil pourrait être plus précise et ont fourni des observations concernant certaines formes de blocage.

85. En résumé, les parties ont indiqué que le blocage basé sur le domaine offre une combinaison de faibles coûts de mise en œuvre et un faible risque de blocage excessif (observations de Cogeco, Nokia et Vidéotron), mais que son efficacité est limitée (observations de Jonathan Curtis, du CCC, de Cogeco, d’Eastlink, de M3AAWG et de Nokia) parce que de nombreuses familles de logiciels malveillants n’utilisent pas le système de noms de domaine (DNS) et, même lorsqu’elles l’utilisent, le blocage basé sur le domaine est facilement contourné[19]. Une autre technique de blocage est le blocage basé sur les adresses IP, dont les parties ont généralement estimé comme plus efficace, même s’il peut encore être contourné par certaines techniques utilisées par les acteurs de menaces (p. ex. le *fast flux*). Bell Canada, Cogeco, Nokia et Vidéotron ont toutefois indiqué que les inconvénients du blocage basé sur les adresses IP sont les risques plus élevés de blocage excessif et les coûts d’entretien plus élevés en raison de la nature dynamique des adresses IP. Bell Canada a également fait remarquer que le blocage de protocole (protocole de communication ou port de service) est généralement effectué en combinaison avec une adresse IP, une méthode qui est parfois appelée blocage de prise réseau.

Résultats de l’analyse du Conseil

86. Le Conseil a examiné les différentes techniques de blocage mentionnées par les parties, notamment les méthodes de blocage basées sur le domaine, l’URL [Uniform Resource Locator], l’IP, la signature et le protocole de communication ou le port de service, ainsi que d’autres méthodes. Le Conseil conclut que chacune de ces techniques présente des avantages et des inconvénients différents en matière d’efficacité, de précision, de coûts de mise en œuvre et d’entretien, et de performance du réseau.

87. Le Conseil estime que le dossier ne démontre pas qu’une méthode l’emporte clairement sur les autres, mais suggère plutôt que ces méthodes sont complémentaires et que les entreprises peuvent souhaiter en mettre en œuvre plus d’une, et ce, afin d’obtenir le meilleur résultat dans une situation donnée.

88. Le Conseil est d’avis que tout cadre pour le blocage des réseaux de zombies à l’échelle des réseaux doit être technologiquement neutre et ne doit pas se limiter à

---

[19] Les protocoles tels que DNS-over-HTTPS (DoH) et DNS-over-TLS (DoT) chiffrent les requêtes DNS d’une manière qui contourne les résolveurs de domaine d’un FST et contourne donc les blocs de domaine mis en œuvre par le FST. En outre, les créateurs de réseaux de zombies peuvent utiliser des algorithmes de génération de domaines afin de s’assurer que les zombies s’inscrivent avec une liste quasi infinie de domaines de sauvegarde dérivés. Parmi les autres tactiques qui nuisent à l’efficacité du blocage basé sur le domaine, citons les architectures poste à poste et la mise en œuvre au sein de réseaux décentralisés non basés sur le DNS, tels que Tor (*The Onion Router*).

un type de blocage particulier. Cela permettra aux FST de s'adapter aux changements technologiques et aux techniques employées par les créateurs de réseaux de zombies, car la nature des menaces posées par les réseaux de zombies est telle qu'elles dépasseront continuellement toute tentative de réglementer les solutions de manière prescriptive.

Gestion centralisée ou décentralisée

Position du Conseil dans l'avis de consultation

89. Le Conseil a cherché à savoir quelles parties sont les mieux placées pour déterminer ce qui est bloqué. Les déterminations relatives au blocage ne doivent pas être prises à la légère et doivent tenir compte de facteurs tels que le degré de préjudice potentiel pour les utilisateurs d'Internet et d'autres effets non désirés inhérents au blocage.

90. Dans l'avis de consultation, le Conseil a établi son avis préliminaire selon lequel une partie indépendante ayant des compétences en matière de cybersécurité serait la mieux placée pour évaluer les répercussions du blocage d'un domaine ou d'une adresse IP en particulier en vue de protéger l'intérêt public et pour décider si le blocage est justifié. Le Conseil a également affirmé qu'à son avis, les entreprises et les FST devraient être tenus de demander l'approbation de l'évaluateur indépendant avant d'ajouter de nouveaux indicateurs à la liste de blocage, mais il a reconnu que les FST pourraient avoir besoin de la flexibilité nécessaire pour retirer de la liste de blocage les indicateurs qui donnent lieu à de faux positifs, afin de protéger l'intégrité du cadre.

Positions des parties

91. Bell Canada, Eastlink, RCCI, SaskTel et TCI ont indiqué qu'on devrait laisser à chaque FST le soin de concevoir et de mettre en œuvre la solution la mieux adaptée aux capacités de leurs réseaux actuels respectifs. Le M3AAWG était également favorable à un régime de filtrage décentralisé par fournisseur, sur une base volontaire, plutôt qu'à l'adoption d'une partie indépendante unique afin d'arriver à des déterminations en matière de blocage ou de filtrage à l'échelle du secteur. La CIRA a indiqué qu'il est essentiel que tout cadre évite un point de défaillance unique. En ce qui concerne la mise en œuvre d'une approche décentralisée, la CIRA a suggéré que les fournisseurs de listes de blocage se conforment à certaines normes et exigences de service (p. ex. des normes de rapidité d'exécution pour assurer un redressement de base) pour être accrédités.

92. Shaw était en faveur d'une liste centralisée de blocage des réseaux de zombies qui serait utilisée par tous les FST canadiens. Le rôle du Conseil se limiterait à la détermination des principes en matière de blocage et à la désignation d'une organisation chargée du blocage des réseaux de zombies qui gérerait la liste de blocage et le mécanisme d'appel en cas de faux positifs. Cogeco et Vidéotron ont également soutenu un type de blocage ciblé (basé sur le domaine), par lequel un tiers indépendant ayant une expertise en matière de cybersécurité serait chargé de fournir à tous les FST une liste de blocage. Vidéotron a indiqué qu'une organisation

de blocage indépendante renforcerait la légitimité du cadre de blocage pour les consommateurs. Vidéotron a ajouté qu'un système flexible, où chaque FST pourrait choisir sa propre méthode de blocage, comme le préconisent Bell Canada, RCCI et TCI, entraînerait des incohérences et de la confusion pour les consommateurs. Bien que le CDIP n'ait pas précisé s'il préférait une liste de blocage gérée de manière centralisée, il a indiqué que le Conseil devrait encourager les FST à partager l'information concernant l'activité des réseaux de zombies sur leurs réseaux afin de favoriser une intervention plus coordonnée concernant la sécurité des réseaux.

93. Une majorité de parties, qu'elles se soient opposées à un cadre en général ou en faveur d'une approche obligatoire ou volontaire, ont préféré impliquer une partie indépendante ayant de l'expérience en matière de cybersécurité plutôt que d'avoir une approche entièrement décentralisée. Par exemple, Vaxination Informatique a affirmé que ce système ne devait en aucun cas être laissé à un seul FST ou à une seule association de FST. Open-Xchange AG s'est fait l'écho de cette position et a indiqué que le Conseil devrait veiller à ce que l'équilibre approprié entre les besoins en matière de sécurité et de protection des données ne soit pas laissé à la discrétion de chaque opérateur.

94. Les tierces parties suivantes, expertes en matière de cybersécurité, ont été suggérées comme des parties indépendantes qui pourraient être impliquées dans le développement d'un mécanisme de blocage :

    - le Canadian Cyber Threat Exchange (CCTX)[20];
    - le CCC;
    - le CCCST;
    - la CIRA;
    - la Coalition canadienne contre l'exploitation des enfants sur Internet;
    - le Conseil;
    - une organisation indépendante nouvellement créée.

95. Benoit Dupont a indiqué que le Conseil pourrait être un bon candidat pour superviser le cadre de blocage, étant donné sa longue expérience en tant que régulateur des télécommunications, et a avancé qu'un cadre serait plus légitime s'il était supervisé par le Conseil. Vaxination Informatique a proposé un système informel afin de réduire les coûts indirects tout en assurant une surveillance, où un organisme central tel que le CCC ou le CST validerait les menaces, et le Conseil diffuserait ces rapports de menaces à tous les FST avec l'autorité de bloquer les

---

[20] Le CCTX est le forum de collaboration concernant les cybermenaces et la source d'information sur les cybermenaces au Canada, où les organisations privées et publiques collaborent afin de réduire les risques liés à la cybersécurité. Le CCTX gère à la fois le CCTX Data Exchange et le CCTX Collaboration Centre. Le CCTX Data Exchange est l'endroit où CCTX recueille, analyse et partage l'information sur les cybermenaces entre les entreprises, les gouvernements et les centres internationaux de partage de menaces.

menaces. Le Conseil fixerait également une date d'expiration pour les menaces afin que les blocages soient temporaires. Les FST seraient alors libres de mettre en œuvre ou d'ignorer un rapport de menaces.

96. Certaines parties ont indiqué que le fait de demander l'autorisation de bloquer les menaces serait contre-productif, car de nombreux FST bloquent déjà systématiquement le trafic malveillant, et les dommages causés par les fraudeurs auraient déjà été faits.

97. Le CST a indiqué qu'il peut fournir un flux d'IC au Conseil et à tout intéressé, mais ne s'est pas engagé à gérer une liste de blocage pour les FST. Le CST a ajouté que, n'étant pas un organisme de réglementation, il ne devrait pas avoir de pouvoir décisionnel dans quelconque cadre proposé. Le CST a en outre indiqué qu'il n'est pas la seule source d'IC à haut degré de confiance et a suggéré au Conseil d'envisager d'autres sources d'information concernant les menaces. Le CST a conclu que le Bouclier canadien de la CIRA pouvait également être utilisé.

98. Vaxination Informatique s'est dite préoccupée par le fait que certains tiers aient le pouvoir discrétionnaire de bloquer les menaces et a indiqué que le Conseil devrait assurer un certain degré de responsabilité par la divulgation publique.

99. Le M3AAWG a argué que le fait d'autoriser les FST à utiliser des listes de blocage de tiers dans leur mise en œuvre du cadre de blocage, comme autre solution aux déterminations de blocage centralisées, n'est pas sans inconvénient. Le M3AAWG a indiqué que lorsqu'il s'agit de données provenant de sources tierces, comme les listes de blocage de serveurs de noms de domaine, les données sont généralement offertes sur la base du « à prendre ou à laisser ». Lorsque les fournisseurs de listes de blocage d'une tierce partie reportent les risques liés à l'utilisation de leur liste de blocage sur l'utilisateur de la liste de blocage, le M3AAWG a ajouté que les FST et les opérateurs mobiles peuvent atténuer ces risques en définissant et en mettant en œuvre des critères pour la sélection des fournisseurs de listes de blocage de domaine qu'ils utilisent. Les critères définis par l'Internet Corporation for Assigned Names and Numbers dans la méthodologie de son système de signalement des cas d'utilisation malveillante des noms de domaine en sont un exemple.

Résultats de l'analyse du Conseil

100. Le Conseil a examiné i) les avantages et les inconvénients généraux d'une certaine forme de centralisation, et ii) les candidats potentiels proposés par les intervenants qui pourraient servir d'autorité centrale d'un cadre de blocage, y compris leur expertise et leur indépendance, ainsi que la facilité de mise en œuvre.

Avantages et inconvénients généraux d'une certaine forme de centralisation

101. Le partage d'IC entre les FST dépend actuellement de communications *ad hoc*. Le Conseil reconnaît qu'il peut y avoir des limites commerciales à la capacité d'un FST de partager des renseignements provenant d'une liste de blocage fournie par un tiers. Le Conseil estime qu'un certain degré de centralisation permettrait de combler cette

lacune en faisant en sorte que tous les FST disposent d'un niveau de renseignements de base, ce qui garantirait à son tour un degré de protection de base pour tous les clients. Le Conseil estime que l'existence d'une liste de blocage gérée de manière centralisée augmenterait nécessairement la visibilité des faux positifs et diminuerait le risque de blocage excessif.

102. Le Conseil est donc d'avis qu'une liste de blocage centralisée est l'option la plus efficace et efficiente. Néanmoins, un cadre minimal pour le blocage des réseaux de zombies à l'échelle des réseaux doit permettre aux FST de mettre en œuvre des initiatives complémentaires. Ces initiatives, par exemple, peuvent comprendre des systèmes exclusifs et des listes de blocage de tiers afin de protéger leurs réseaux et leurs clients contre les cybermenaces.

103. Le Conseil reconnaît que l'existence d'une variété de listes ou de systèmes de blocage est généralement moins transparente pour le public et rend plus complexe l'obtention de mesures regroupées (p. ex. ce qui est bloqué par quel système). Cependant, et plus important encore, le fait de disposer d'une variété de solutions rend plus difficile pour les opérateurs de réseaux de zombies de s'introduire largement dans les réseaux et les systèmes des clients. Le Conseil estime également que les améliorations apportées à une liste de blocage de base avec d'autres systèmes exclusifs ou tiers pourraient favoriser l'innovation et la concurrence entre les FST et les tiers. Toutefois, l'utilisation de listes de blocage supplémentaires soulève la question de savoir si elles seront évaluées et accréditées, et si oui, comment et par qui.

104. Le Conseil estime que l'accréditation de listes de blocage supplémentaires présente plusieurs avantages. L'accréditation ferait en sorte que les FST mettent en œuvre le blocage des réseaux à l'échelle des réseaux conformément au cadre minimal établi par le Conseil. Elle permettrait également de faire en sorte que les fournisseurs de listes de blocage disposent d'une expertise technique suffisante.

Candidats potentiels proposés par les intervenants qui pourraient servir d'autorité centrale concernant un cadre de blocage

105. Le CCC est l'autorité technique du Canada en matière de cybersécurité. Le CCC réunit en une seule organisation l'expertise opérationnelle existante en matière de cybersécurité du CST, de Sécurité publique Canada et de Services partagés Canada. En plus de son expertise en matière de cybersécurité et de sa neutralité, le CCC a également l'avantage d'être membre du CCCST et travaille déjà en collaboration avec les FST et la GRC. En outre, elle gère déjà une liste de blocage pour le gouvernement du Canada et fournit une alimentation en données au CCTX.

106. En ce qui concerne le CCTX et le CCCST, il ne fait aucun doute que les deux organisations possèdent l'expertise nécessaire en matière de cybersécurité. Cependant, étant donné que Bell Canada est l'un des fondateurs du CCTX et l'actuel président du conseil d'administration du CCTX, et que RCCI est le coprésident de l'industrie du CCCST, certaines parties prenantes pourraient ne pas estimer ces organisations comme des tiers neutres. En outre, les frais d'adhésion au

CCTX varient de 500 à 50 000 dollars. L'adhésion au CCCST est limitée à 12 FST et ne représente donc pas les intérêts de tous les FST. Ces facteurs limitent encore plus la pertinence pour ces organisations de servir de gestionnaires de listes de blocage.

107. Une autre option, telle que suggérée par le CCC, consiste à tirer parti du Bouclier canadien de la CIRA. La CIRA possède l'expertise et est relativement indépendante des FST[21]. Comme indiqué précédemment, la CIRA a bloqué 20 millions de domaines en 12 mois, et 50 000 d'entre eux sont basés sur la liste de blocage du CCC. Cela signifie que la liste de blocage de la CIRA est beaucoup plus étendue que celle créée par le CCC. Cependant, la CIRA mentionne qu'elle sert actuellement plus de 500 millions de requêtes chaque jour au moyen du Bouclier canadien de la CIRA. Cela signifie que l'utilisation du Bouclier canadien de la CIRA ne serait possible que si la CIRA était en mesure de faire évoluer ses systèmes pour gérer un trafic beaucoup plus important. Si la CIRA n'est pas en mesure de faire évoluer ses systèmes dans la mesure requise, cette option ne sera pas réalisable. D'autres problèmes qui peuvent survenir en utilisant l'infrastructure DNS de la CIRA plutôt que celle des entreprises comprennent le risque d'un point de défaillance unique, les complications pour le soutien à la clientèle et l'augmentation de la latence moyenne de réponse DNS.

108. Le Conseil rejette également la suggestion en faveur de sa propre participation, étant donné son manque actuel d'expertise et de ressources pour soutenir la gestion, la conservation ou la distribution d'une liste de blocage de réseau centralisée. En outre, le Conseil estime qu'il ne devrait pas être impliqué dans le traitement des plaintes de faux positif qui nécessitent une résolution en quelques heures.

109. La dernière option consiste à créer une nouvelle organisation autonome. Cela prendrait du temps et serait coûteux. En outre, selon le Conseil, elle pourrait être indûment fastidieuse.

110. Compte tenu de ce qui précède, le Conseil estime qu'il n'existe actuellement aucune organisation unique prête à gérer une liste de blocage centralisée à l'usage des FST canadiens. Toutefois, comme indiqué ci-dessus, une centralisation complète n'est pas nécessairement requise.

111. Le Conseil demande donc au Comité directeur du CRTC sur l'interconnexion (CDCI) d'examiner si une organisation indépendante (comme le CCC ou la CIRA) serait capable et désireux de maintenir une liste de blocage de base à l'usage des FST au Canada. Le Conseil demande que le CDCI examine également si et comment des systèmes complémentaires ou autres (c.-à-d. des listes de blocage de tiers, des systèmes exclusifs et des pratiques telles que le blocage des ports de service normalisés ou d'autres pratiques exemplaires recommandées) peuvent être

---

[21] La CIRA est une organisation privée, à but non lucratif. Quelques membres du conseil d'administration de la CIRA occupent également des postes de direction dans la communauté des FST.

accrédités ou soumis à des exigences techniques. Ces systèmes pourraient être utilisés en complément d'une liste de blocage centralisée, ou à la place d'une liste de blocage centralisée si celle-ci n'est pas une option viable. Les questions détaillées destinées au CDCI figurent à l'annexe 2 de la présente décision.

112. Le Conseil demande au CDCI de déposer un rapport **dans les neuf mois** suivant la date de publication de la présente décision. Les intéressés auront la possibilité de commenter le rapport avant que le Conseil ne tire d'autres conclusions concernant le cadre à appliquer au blocage des réseaux de zombies à l'échelle des réseaux.

113. Bien que le Conseil renvoie ces questions au CDCI, il fait remarquer l'existence de groupes de travail tels que le CCCST, où les parties prenantes peuvent avoir des délibérations plus approfondies et privées sur des questions en matière de sécurité sensibles, au besoin.

Approches de blocage par défaut, à option d'adhésion et à option de retrait

Position du Conseil dans l'avis de consultation

114. Dans l'avis de consultation, le Conseil a affirmé que les appareils infectés connectés à Internet et fonctionnant comme des zombies le font généralement à l'insu de leur propriétaire ou sans son consentement. Le Conseil reconnaît également que les abonnés aux services Internet peuvent ne pas voir l'intérêt de participer à un programme de blocage à l'échelle des réseaux, même si leur appareil est infecté par un logiciel malveillant. Considérant ces facteurs, le Conseil a indiqué sa préférence préliminaire pour une approche de blocage par défaut, mais a invité les parties à évaluer les avantages et les inconvénients relativement à l'efficacité des approches de blocage par défaut, à option d'adhésion et à option de retrait pour traiter les communications des réseaux de zombies.

Positions des parties

115. Plusieurs parties, particulièrement les FST, ont préféré une approche de blocage par défaut plutôt que les approches à option d'adhésion et à option de retrait.

116. Eastlink, RCCI, SaskTel et Shaw, par exemple, ont soutenu une approche de blocage par défaut et ont adopté la position selon laquelle il ne devrait pas y avoir de processus à option d'adhésion ou de retrait, puisque la protection du réseau est avantageuse et applicable pour tous. Elles ont fait valoir que les approches à option d'adhésion et de retrait imposent toutes deux un fardeau administratif accru sur les TSP. Shaw a utilisé Cleanfeed[22] comme exemple d'approche de blocage par défaut qu'elle considérait être utile et applicable pour bloquer les réseaux de zombies.

---

[22] Dans le cadre du projet Cleanfeed, les FST les plus grands au Canada, y compris Bell Canada, MTS Allstream, RCCI, Shaw, SaskTel, TCI et Vidéotron, ont bloqué l'accès aux sites Web affichant du matériel d'exploitation d'enfants depuis 2006 et 2007.

117. Bell Canada était aussi en faveur d'une approche de blocage par défaut et a argué qu'elle n'a actuellement pas la capacité de mettre en œuvre les approches à option d'adhésion ou de retrait dans le cadre du blocage de réseaux de zombies. Bell Canada a expliqué que le blocage à l'échelle des réseaux, où la fonctionnalité de blocage est toujours activée, ne fait pas de distinction entre chaque utilisateur d'Internet. Il est plutôt généralement appliqué uniformément sur l'ensemble des réseaux des FST sans pouvoir être personnalisé par le chaque utilisateur.
Bell Canada a indiqué que l'avantage de la fonctionnalité du blocage permanent est qu'il offre une protection contre les réseaux de zombies tout en évitant les coûts supplémentaires relatifs à la mise en place de nouveaux mécanismes de suivi dynamiques des adresses IP liés aux renseignements sur les comptes des clients. Ces coûts seraient inévitablement transmis aux clients des services Internet.
Bell Canada a également affirmé que l'approche de blocage par défaut permet d'éviter la collecte et l'utilisation accrues des renseignements personnels des clients.

118. Nokia, du point de vue d'un fournisseur d'information sur les menaces, a soutenu l'argument des FST selon lequel les approches à option d'adhésion ou de retrait peuvent être peu pratiques à mettre en œuvre et à gérer pour eux. Nokia a indiqué que si la technologie est précise et fiable, il pourrait être possible d'utiliser l'approche de blocage par défaut et de fournir une fonctionnalité de retrait. Elle a ajouté que la flexibilité offerte par les approches à option d'adhésion ou de retrait augmente les coûts pour les entreprises et, en fin de compte, pour les utilisateurs.

119. La CIBC et autres ont indiqué que le fait de se retirer de la protection n'a pas seulement des répercussions sur l'utilisateur qui se retire, mais aussi sur les autres utilisateurs du réseau des FST. Permettre aux utilisateurs qui ont choisi de se retirer de rester dans le réseau de confiance d'un FST constitué d'appareils protégés contre des réseaux de zombies aurait des répercussions négatives tangibles. La CIBC et autres ont conclu en recommandant l'approche du blocage par défaut.

120. J. Clarke, Fenwick McKelvey et Reza Rajabiun, l'Internet Society, TCI et TekSavvy se sont prononcés en faveur d'une approche à option d'adhésion, mais ont présenté des arguments différents pour justifier leur soutien.

121. J. Clarke et TCI ont indiqué que le secteur privé offre déjà des services de blocage auxquels les clients peuvent adhérer, et que ces fournisseurs de services disposent des ressources nécessaires pour générer et maintenir des listes de blocage. L'Internet Society, dans son soutien à une approche à option d'adhésion, a recommandé que les utilisateurs potentiels soient informés des implications potentielles de participation et du consentement à la participation sur une base périodique.
Fenwick McKelvey et Reza Rajabiun ont indiqué que le blocage des ressources Internet en dehors du réseau d'un FST ne devrait être abordé qu'au moyen d'une approche à option d'adhésion, et que si les FST veulent offrir des protections supplémentaires à leurs clients, ils devraient le faire sur une base à option d'adhésion dans le cadre d'une offre groupée disponible gratuitement.

122. Les parties en faveur d’une approche à option de retrait étaient principalement des organisations à but non lucratif ou des particuliers. Open-Xchange AG a estimé que le blocage des contenus potentiellement dommageables est un bien collectif et a recommandé que le blocage soit activé par défaut. Elle a toutefois suggéré qu’un mécanisme à option de retrait soit mis à la disposition de certains individus, tels que les chercheurs en logiciels malveillants. Le M3AAWG s’est prononcé en faveur d’une approche à option de retrait, car l’approche à option d’adhésion peut être peu adoptée. La CIRA s’est prononcée en faveur d’une approche à option de retrait, car elle a estimé important que les abonnés puissent exercer leur droit de choisir. Les participants au groupe de discussion du sondage mené par la coalition manitobaine ont préféré une approche à option de retrait par laquelle les clients recevraient des notifications d’événements bloqués et pourraient signaler les cas de faux positifs. Kristin Surette a estimé que la méthode à option de retrait appropriée, car les réseaux de zombies fonctionnent généralement à partir d’ordinateurs personnels, à l’insu de leurs propriétaires.

Résultats de l’analyse du Conseil

123. Le Conseil fait remarquer le faible taux historique d’utilisation des approches à option d’adhésion. Bien qu’il s’agisse d’un service gratuit disponible pour tous les Canadiens, le Bouclier canadien de la CIRA n’est utilisé que par 1 % des ménages. Ce chiffre très bas suggère que les approches à option d’adhésion entraînent une sous-utilisation. Le Conseil estime toutefois que le fait que les utilisateurs ne prennent peut-être pas des mesures positives pour adhérer à un service de blocage des réseaux de zombies ne signifie pas qu’ils préféreraient que leurs appareils et leurs réseaux soient exposés à des réseaux de zombies malveillants.

124. Bien qu’une approche à option de retrait ne pose pas le problème de la sous-utilisation, le Conseil estime que cette approche présente d’autres inconvénients. Tant l’approche à option d’adhésion que celle à option de retrait portent atteinte à la sécurité, notamment celle des autres utilisateurs. Puisque la protection du réseau est avantageuse à tous les utilisateurs, elle devrait s’appliquer à tous.

125. Le Conseil estime également que les approches à option d’adhésion ou de retrait augmentent considérablement le fardeau de mise en œuvre et les coûts supportés par les FST, peuvent retarder la mise en œuvre du mécanisme de blocage et peuvent être excessivement lourdes à gérer.

126. Le Conseil conclut que ni les approches à option d’adhésion ou de retrait ne sont appropriées et que, lorsque le blocage à l’échelle des réseaux est offert, il devrait s’appliquer par défaut. Cette approche ferait en sorte que tous les clients du FST bénéficient du blocage de la manière la plus efficace et efficiente possible. Le Conseil fait remarquer que l’approche de blocage par défaut est compatible avec l’approche de blocage de Cleanfeed et avec l’approche de blocage actuel de la CIRA résultant de son partenariat avec Mozilla Firefox.

127. Le Conseil fait remarquer que le cadre ne serait pas totalement dépourvu de mécanismes à option de retrait, car les utilisateurs et les chercheurs peuvent i) utiliser des services VPN [Virtual Private Network] auxquels le blocage ne s'appliquerait pas, i) utiliser les renseignements sur les pratiques de blocage des FST pour éclairer leur choix de fournisseur de services, ou iii) diriger les demandes de domaine vers des résolveurs qui contournent le blocage effectué par certains FST.

Champ d'application technique (types d'IC)

Positions des parties

128. Certaines parties ont soutenu un cadre plus large concernant la cybersécurité, qu'il soit lié ou non aux réseaux de zombies. Par exemple, le Conseil d'identification et d'authentification numériques du Canada a indiqué que le renforcement d'un cadre en matière de cybersécurité qui aborde des menaces de cybersécurité plus diverses et qui adopte une approche de l'ensemble de la sécurité sur Internet servirait mieux le Conseil, les Canadiens et les entreprises canadiennes.

129. De même, le CST a indiqué que, sur la base de son expérience de la défense des réseaux du gouvernement du Canada, il estime que l'expression « réseaux de zombies » a une portée trop étroite. Le CST a ajouté qu'il recommande d'élargir le champ d'application pour permettre le blocage des IC généraux, de la même manière qu'il bloque de tels IC pour le gouvernement du Canada.

130. En revanche, Samuel Harper, la CIRA, INFOSECSW, l'Internet Society et Vaxination Informatique ont exprimé de sérieuses préoccupations quant au fait qu'un nouveau cadre pourrait être une pente glissante vers le blocage de contenu et la surveillance des citoyens. Par exemple, la CIRA a indiqué qu'elle était profondément préoccupée par le fait qu'un tel cadre volontaire pourrait être détourné à des fins qui s'éloignent de l'intégrité et de la sécurité du réseau de quelque manière que ce soit. Elle a argué que le résultat définitif de la présente instance ou les activités du Conseil dans ce domaine ne doivent pas être le développement d'un commutateur principal plus accessible qui pousse les entreprises publiques à jouer le rôle d'éditeurs, de filtres ou de shérifs de l'Internet. Vaxination Informatique a également indiqué que ce projet doit être extrêmement bien circonscrit, avec un mandat très précis et balisé qui ne permet aucun élargissement progressif.

Résultats de l'analyse du Conseil

131. Le Conseil fait remarquer que les réseaux de zombies, les logiciels malveillants et les intrusions informatiques sont interconnectés, ce qui rend peu pratique et inefficace le fait de bloquer uniquement le trafic des réseaux de zombies et de ne pas bloquer les autres types d'IC. En fait, les FST filtrent actuellement les IC sur la base de listes de blocage, quelle que soit leur source (réseaux de zombies ou non). De plus, la justification stratégique du blocage du trafic des réseaux de zombies (c.-à-d. le préjudice causé aux Canadiens par les cybermenaces) s'applique également aux autres IC. Par conséquent, sur le plan stratégique, la recommandation du CST en

faveur d'une approche axée sur l'ensemble des IC plutôt que sur le trafic des réseaux de zombies, qui, en pratique, n'est pas isolé d'un IC particulier, peut être appropriée. Une approche centrée sur les IC devrait être extrêmement bien circonscrite pour faire en sorte qu'elle se limite à la cybersécurité et exclue tout élargissement progressif de son champ d'application.

132. En outre, le Conseil estime, à titre préliminaire, que le blocage d'autres IC devrait être soumis aux mêmes principes directeurs que le blocage du trafic des réseaux de zombies. Le Conseil demande au CDCI de confirmer certaines considérations techniques relatives aux IC, telles que détaillées à l'annexe 2 de la présente décision. Le Conseil publiera le rapport du CDCI sur son site Web, où les intéressés auront l'occasion de formuler des observations.

Mesures concernant la protection de la vie privée

Position du Conseil dans l'avis de consultation

133. Dans l'avis de consultation, le Conseil a affirmé que les réseaux de zombies constituent une menace importante pour la vie privée des consommateurs lorsqu'ils accèdent à des renseignements personnels, et que le blocage des communications des réseaux de zombies peut contribuer à protéger les consommateurs. Toutefois, cette protection est assurée par la surveillance du trafic Internet. Les conséquences pour la vie privée des consommateurs que la surveillance entraîne sont des questions importantes que tout cadre de blocage potentiel doit aborder. Le Conseil a invité les parties à présenter leurs observations sur les conditions qui peuvent contribuer à protéger la vie privée des consommateurs.

Positions des parties

134. Vidéotron a indiqué que les conditions de protection de la vie privée des consommateurs sont déjà énoncées dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et la jurisprudence connexe. Dans ce contexte, des exceptions s'appliquent à l'accès aux renseignements personnels à des fins d'application de la loi.

135. Bell Canada et SaskTel ont argué que, d'après leur expérience, le blocage à l'échelle des réseaux ne soulève pas de problèmes de protection de la vie privée parce qu'il ne repose pas sur des indicateurs de contenu et ne révèle pas de renseignements propres au client qui permettent son identification.

136. Comme indiqué ci-dessous, un certain nombre de parties ont indiqué que des mesures de protection particulières devraient être mises en place concernant la manière dont les renseignements personnels sont recueillis, utilisés, conservés et divulgués. Plus précisément, la CIRA a indiqué que le Conseil devrait établir une norme de protection de la vie privée plus élevée que celle qui serait disponible en vertu de la LPRPDE, comme l'a reconnu le Conseil dans la décision de télécom 86-7 et d'autres décisions connexes concernant les mesures concernant la protection de la confidentialité des consommateurs des services téléphoniques.

137. La coalition manitobaine a indiqué que le respect de la vie privée est une priorité pour les consommateurs. Elle a suggéré la création d'un organe décisionnel indépendant et l'imposition de restrictions strictes quant aux renseignements recueillis et contrôlés et à ce qui est fait en définitive de ces renseignements. Benoit Dupont a également fait remarquer que le respect de la vie privée et la responsabilité devraient être maintenus au plus haut niveau afin d'éviter toute controverse et l'élargissement progressif de la surveillance.

138. Fenwick McKelvey et Reza Rajabiun ont indiqué que tous les types de renseignements recueillis dans le but de lutter contre les réseaux de zombies devraient être inclus dans la conclusion du Conseil, et que les données recueillies ne peuvent être vendues à des tiers.

139. Shaw a argué que les renseignements bloqués devaient être limités, et que le mécanisme de blocage devait respecter ces principes :

- But limité de collecte, d'utilisation et de conservation : Les FST et l'organisation de blocage ne doivent recueillir, utiliser, divulguer et conserver que les données nécessaires au blocage des réseaux de zombies.

- Transparence : Les politiques en matière de confidentialité des FST doivent indiquer clairement que des renseignements limités seront recueillis et utilisés pour bloquer les réseaux de zombies.

- Processus défini : Les FST devraient disposer d'un processus afin de documenter les données recueillies et traitées dans le cadre de la gestion de leur système de blocage des réseaux de zombies.

- Mécanisme approprié pour la suppression des données : Les FST devraient disposer d'un processus permettant de gérer et d'éliminer efficacement les données recueillies dans le cadre de ce traitement des données, notamment en les conservant de façon distincte des autres données.

140. Open-Xchange AG a également mentionné que tout renseignement personnel recueilli ne doit pas être utilisé à d'autres fins. Les destinations bloquées devraient être recueillies aux fins de la notification de l'infection à l'utilisateur final, mais sous réserve d'une limite de temps (p. ex. 30 jours), après laquelle les données recueillies sont détruites. La CIPPIC a indiqué que les règles concernant la suppression appropriée doivent être incluses dans tout type de cadre pour les entreprises.

Résultats de l'analyse du Conseil

141. Le Conseil reconnaît le point de vue de certains FST selon lequel le blocage des réseaux de zombies à l'échelle des réseaux ne révèle généralement pas de renseignements propres aux clients qui permettent son identification. Néanmoins, le Conseil estime que lorsque des renseignements personnels concernant les clients sont recueillis, utilisés ou divulgués, les mesures concernant la protection de ces

renseignements sont d'une importance capitale. Les FST sont déjà tenus de se conformer aux obligations légales existantes concernant la collecte, l'utilisation et la divulgation des renseignements personnels des clients[23]. En outre, le Conseil s'attendrait à ce que les FST mettent en œuvre les meilleures pratiques qui renforcent ces obligations afin de tenir compte des spécificités d'un cadre de blocage et de faire en sorte que les renseignements confidentiels concernant les clients recueillis, utilisés ou divulgués aux fins du mécanisme de blocage soient limités à ce qui est essentiel à cette fin, et uniquement pendant la durée nécessaire à cette fin, et que les renseignements recueillis ne soient pas utilisés ou divulgués à d'autres fins. Le principe correspondant est indiqué à l'annexe 1 de la présente décision.

142. Le Conseil fait remarquer que la CIRA a effectué une vérification (en anglais seulement) de ses processus en matière de protection de la vie privée dans le contexte du Bouclier canadien de la CIRA. Bien qu'à ce stade, le Conseil n'estime pas qu'une obligation de vérification soit nécessaire, le rapport de la CIRA contient des renseignements utiles concernant les mesures opérationnelles concernant la protection de la vie privée pour tenir compte des spécificités d'une solution de blocage de la cybersécurité.

Transparence et exigences de divulgation des FST

Position du Conseil dans l'avis de consultation

143. Dans l'avis de consultation, le Conseil a demandé aux parties de commenter les exigences en matière de divulgation nécessaires pour les FST. En particulier, le Conseil a invité les intéressés à faire part de leurs observations sur les dispositions qui assureront la transparence des programmes de blocage, par exemple en informant les clients de la portée du mécanisme de filtrage ou en créant un portail où les abonnés peuvent vérifier si un domaine particulier est bloqué.

Positions des parties

144. En général, les parties ont indiqué que tout cadre de blocage devrait être transparent pour les utilisateurs afin qu'ils puissent être en mesure de donner leur consentement en connaissance de cause. Les renseignements accessibles au public devraient au moins expliquer aux clients comment le blocage fonctionne, qui est impliqué et quels renseignements sont conservés. De plus, SaskTel, Shaw et Vaxination Informatique ont avancé que ces renseignements accessibles au public devraient fournir un lien vers un site Web qui indique avec qui communiquer afin d'obtenir de

---

[23] En plus de la LPRPDE, les FST sont tenus de se conformer aux mesures de protection de la confidentialité des consommateurs imposées par le Conseil, qui interdisent aux FST de divulguer des renseignements sur les clients autres que le nom, l'adresse et le numéro de téléphone inscrit à toute personne sans le consentement exprès du client, sauf dans certaines circonstances précises (voir par exemple les décisions de télécom 2003-33 et 2005-14 les politiques réglementaires de télécom 2009-723 et 2017-11).

plus amples renseignements ou qui consiste en une page plus détaillée hébergée par le Conseil ou par l'organisation de blocage. Bell Canada, RCCI et SaskTel ont fait valoir que, pour des raisons de sécurité, il est préférable de fournir des renseignements génériques aux utilisateurs plutôt que des renseignements détaillés.

145. La CIRA a indiqué qu'il est essentiel que les FST aient, et que les utilisateurs finals continuent d'avoir, la possibilité de choisir entre les fournisseurs de cybersécurité de leur choix. La CIRA a argué que la divulgation relative au traitement des renseignements personnels, comme l'étendue de la collecte et la durée de la conservation, devrait être exigée. La CIRA a également suggéré que le Conseil établisse des normes sur la façon dont les abonnés sont informés lorsque leur FST détecte que l'appareil d'un abonné est infecté par un logiciel malveillant.

146. La coalition manitobaine a fait valoir que les consommateurs doivent être bien informés du fonctionnement et des répercussions du cadre de blocage, et notamment avoir accès à des renseignements transparents sur ses coûts.

147. La CIBC et autres ont recommandé que les FST divulguent une grande variété de renseignements, y compris, mais sans s'y limiter, le but général de leur programme de blocage, la manière dont le trafic est surveillé, utilisé et divulgué, les mesures de protection en vue d'assurer que les données ne sont pas utilisées à mauvais escient et assurer l'efficacité de leur programme (au moyen du nombre d'événements bloqués et de faux positifs, entre autres).

148. Benoit Dupont a fait valoir que le fait que les FST participants conservent un certain degré d'indépendance quant à la façon dont les infections sont traitées rend plus difficile l'évaluation du programme dans son ensemble et, à moins qu'une approche de divulgation publique ne soit adoptée, il est peu probable que les données sur la performance de chaque FST individuel fassent l'objet d'un examen public. Benoit Dupont a ajouté que la justification des initiatives en matière de divulgation publique est d'influencer les FST peu performants en augmentant la quantité de renseignements relatifs au blocage disponible au public.

149. Xplornet a indiqué que les abonnés doivent être informés que la participation à un cadre de blocage à l'échelle des réseaux ne peut servir de substitut à l'entretien des logiciels de sécurité sur leurs appareils.

Résultats de l'analyse du Conseil

150. Le Conseil estime que les consommateurs devraient être suffisamment informés de la nature et de la portée du programme de blocage d'un FST pour leur permettre de prendre des décisions éclairées quant à leur choix de services et de fournisseurs de services.

151. Le Conseil estime que la transparence est un principe essentiel d'un cadre de blocage à l'échelle des réseaux, et qu'elle peut être obtenue par des mesures complémentaires imposées aux FST, tel qu'indiqué à l'annexe 1 de la présente décision. Ces mesures sont les suivantes :

- fournir des renseignements au public concernant la nature générale et la portée du programme de blocage d'un FST;

- le signalement de renseignements précis et d'indicateurs de rendement au Conseil afin qu'il puisse publier des renseignements comme des statistiques agrégées ou analyser ces indicateurs afin de déterminer si d'autres mesures réglementaires sont nécessaires (le format et la fréquence restent à déterminer)[24].

152. Les exigences particulières en matière de rapports seront déterminées après réception du rapport du CDCI. Par exemple, de telles exigences en matière de rapports peuvent comprendre, pour chaque liste de blocage utilisée au cours d'une période de rapport, la divulgation du nombre total d'IC uniques sur une liste de blocage, le nombre total d'IC uniques véritablement bloqués, le nombre total de plaintes concernant des faux positifs rapporté, le nombre total d'IC échangés avec les parties prenantes, et le nombre total d'abonnés aux services Internet impliqués dans le blocage.

Précision et mesures concernant la protection contre le blocage excessif et les faux positifs

Position du Conseil dans l'avis de consultation

153. Dans l'avis de consultation, le Conseil a affirmé que plusieurs services en ligne peuvent être fournis à la même adresse IP et que les serveurs de commande et de contrôle des réseaux de zombies ne restent généralement pas sur le même appareil pendant de longues périodes. Bloquer une adresse IP peut donc empêcher par inadvertance l'accès à des services légitimes, et bloquer un serveur de commandement et de contrôle ne sera efficace que pour une durée limitée. Par conséquent, la liste de blocage doit être mise à jour régulièrement pour rester exacte, ce qui amène des risques relatifs au blocage excessif et aux faux positifs.

154. Le Conseil a invité les parties à formuler des observations sur les dispositions d'un cadre de blocage où les conditions qui pourraient empêcher le blocage excessif et les faux positifs, ou qui pourraient atténuer les risques associés. Le Conseil a demandé aux parties de :

- commenter sur la probabilité de l'apparition d'un blocage excessif et de faux positifs et les répercussions de cette situation dans le cadre de l'utilisation de mesures de protection contre le trafic des réseaux de zombies;

---

[24] Pour des raisons d'efficacité, les exigences de signalement des renseignements précis et des indicateurs de rendement pourraient être combinées avec les exigences existantes du Conseil relatives à la divulgation des buts de gestion du trafic Internet.

- définir les attentes en matière de résolution des faux positifs et les dispositions pour assurer la rapidité d'exécution et l'équité procédurale dans le processus de résolution;

- suggérer des options, accompagnées des avantages et des inconvénients que chacune représente, de moyens automatisés qui seraient utilisés pour résoudre les services bloqués de manière incorrecte.

Positions des parties

Probabilité et répercussions concernant le blocage excessif et les faux positifs dans le cadre des mesures de protection contre le trafic des réseaux de zombies

155. Les parties étaient largement d'accord sur le fait que le blocage excessif et les faux positifs sont inévitables, mais étaient divisées sur leur probabilité ou leur prévalence. L'éventail des opinions variait d'un risque élevé (le M3AAWG ou Xplornet, lorsque le blocage se fait uniquement au moyen des noms de domaine et des adresses IP) ou important (Eastlink et l'Internet Society) à un risque peu probable (Shaw), faible (Vidéotron, concernant particulièrement le blocage basé sur le domaine) ou non concluant (le CDIP).

156. Cogeco et Vidéotron ont plaidé en faveur du blocage par domaine et ont estimé qu'il présentait un risque de faux positifs moins élevé que le blocage par adresses IP. Vidéotron a affirmé qu'elle met actuellement en œuvre un blocage par domaine et que, d'après son expérience, le risque de faux positifs est faible.

157. Les parties ont également reconnu que les systèmes présentant de faibles risques de blocage excessif et de faux positifs sont moins efficaces.

158. Le CCC a indiqué que la liste de blocage actuelle qu'elle fournit au Bouclier canadien de la CIRA est constituée d'IC de haute confiance.

Attentes relatives à la résolution des faux positifs et dispositions permettant de garantir la rapidité d'exécution et l'équité procédurale de la procédure de résolution

159. La coalition manitobaine a avancé qu'avant d'ajouter un IC à une liste de blocage, l'organisation chargée de gérer la liste devrait appliquer des critères de blocage d'une manière qui est fondée sur des éléments de preuve, et qui est flexible et exempte de tout parti pris commercial ou politique et sensible aux commentaires des utilisateurs d'Internet. Eastlink a également indiqué qu'il est essentiel que l'entité qui gère une liste de blocage ait mis en place les procédures nécessaires pour faire en sorte que les domaines et les adresses ne soient pas ajoutés à la liste sans éléments de preuve suffisants démontrant la nécessité et la pertinence de les bloquer. Bell Canada a avancé qu'une vérification indépendante de tous les renvois générés par des tiers, y compris ceux des groupes de travail sur la cybersécurité, devrait être effectuée. Bell Canada a ajouté que l'entité qui gère la liste de blocage devrait être hautement convaincue qu'une source est malveillante avant de la bloquer. Électricité

Canada a ajouté que le blocage doit être spécifique et ciblé, et utiliser plusieurs sources d'information.

160. Le CCC a indiqué que, dans le cadre de son expérience de protection des réseaux du gouvernement du Canada, il a mis en place un processus de contrôle des IC avant de les bloquer afin de réduire au minimum le blocage excessif et les faux positifs.

161. Plutôt que de contrôler les IC, la CIRA a suggéré qu'une partie indépendante soit uniquement responsable de l'accréditation des fournisseurs de listes de blocage. Ces fournisseurs de listes de blocage devraient se conformer à des normes de service afin d'être accrédités. Ces normes de service comprennent l'obligation de répondre aux demandes de mise à jour urgentes des FST, d'agir rapidement en cas d'urgence et de se conformer aux normes de rapidité d'exécution pour garantir un redressement de base.

Moyens automatisés pour résoudre les services bloqués incorrectement, et leurs avantages et inconvénients associés

162. Nokia a indiqué qu'il est facile d'ajouter des entrées à ces listes de blocage, mais qu'il est difficile de décider quand il est approprié de supprimer une entrée. Benoit Dupont ainsi que Fenwick McKelvey et Reza Rajabiun ont argué que le blocage ne devrait être que transitoire, suggérant qu'une date d'expiration soit attribuée à chaque IC de la liste de blocage.

163. Eastlink a fait valoir que l'entité qui gère une liste de blocage devrait déterminer rapidement et avec précision quels domaines et quelles adresses devraient être retirés de la liste en se fondant sur sa propre surveillance de routine et sur les faux positifs signalés.

164. En ce qui concerne la réception des rapports de faux positifs, la plupart des parties ont suggéré qu'un processus soit mis en place pour les recevoir et traiter le problème en temps opportun en mettant à jour la liste de blocage et en supprimant tout faux positif confirmé. Électricité Canada a affirmé que la création d'un portail permettant aux utilisateurs de donner leur rétroaction sur les faux positifs perçus pourrait être utile. Selon la CIBC et autres, les faux positifs peuvent être signalés de manière centralisée ou à chaque FST. Une fois le signalement effectué, le destinataire du signalement serait chargé de le valider, notamment en s'assurant qu'il ne s'agit pas d'une tentative de déblocage d'un indicateur malveillant, et en vérifiant que la méthode de blocage existante reste appropriée.

165. Cependant, il n'y a pas eu d'entente entre les parties sur le responsable de la mise à jour de la liste de blocage (y compris la gestion des mises à jour résultant des déclarations de faux positifs).

166. Cogeco, la coalition manitobaine et Xplornet étaient d'avis que la gestion de la liste de blocage, y compris sa mise à jour, devrait être dirigée par une partie indépendante possédant une expertise en matière cybersécurité et non par les FST. Selon Vidéotron, la centralisation du blocage sous une organisation experte

permettrait une approche d'ensemble et constante, et limiterait le risque de faux positifs. Vidéotron a également suggéré de mettre en place un canal de communication à utiliser par les FST afin de signaler les faux positifs à l'organisation de blocage, qui serait alors en mesure de les évaluer et de les traiter en temps opportun. RCCI a également indiqué que la mise à jour de la liste ne devrait pas être la responsabilité des FST, mais plutôt celle de l'organisme gouvernemental approprié qui gère la liste. RCCI a ajouté que les FST n'auraient aucune idée de ce qui figure sur la liste. Marc Nanni et RCCI ont ajouté que les FST ne seraient pas en mesure de gérer une augmentation des plaintes des clients auprès des centres d'appels et ne peuvent pas être responsables de l'offre d'un soutien aux clients en ce qui concerne les déclarations de faux positifs. Électricité Canada a avancé que le Conseil pourrait souhaiter tirer parti de l'expertise du CCC.

167. SaskTel a suggéré que les déclarations de faux positifs soient traitées par les FST. TCI a également estimé que les FST ont réussi à prévenir et à atténuer les risques liés au blocage excessif et aux faux positifs dans leurs pratiques de blocage actuelles. TCI a ajouté que la nécessité pour les FST de disposer d'une flexibilité opérationnelle et d'une capacité d'adaptation en fonction de la nature et de la portée de la menace particulière que représentent les réseaux de zombies signifie qu'ils ne peuvent pas mettre en œuvre des dispositions uniformes pour réduire les risques de blocage excessif et de faux positifs au-delà de ce qui est déjà prévu dans la Politique sur les pratiques exemplaires en matière de sécurité pour les fournisseurs canadiens de services de télécommunications (FCST) du CCCST.

168. Le CCC a supposé que les faux positifs seraient gérés par les FST. Le CCC a recommandé au Conseil d'examiner l'article 1.3 des *Normes d'intervention en cas d'incidents de sécurité pour les fournisseurs canadiens de services de télécommunications (FCST)* du CCCST, étant donné qu'elle comprend une pratique en vue de garantir que les activités de blocage ont une probabilité minimale d'avoir des répercussions sur le trafic légitime.

169. La M3AAWG s'est opposée aux méthodes de réponse *ad hoc* aux plaintes en indiquant que le rythme rapide possible de génération d'indicateurs, qui peut dépasser des taux de 500 nouveaux indicateurs par minute, signifie que les évaluateurs de faux positifs et de blocage excessif peuvent être facilement submergés de plaintes. Elle a argué que l'industrie a besoin de mécanismes de filtrage qui fonctionnent à l'échelle industrielle.

170. SaskTel a indiqué qu'en cas de faux positifs, les FST doivent agir rapidement pour déterminer si le trafic devrait être bloqué ou non et remédier à la situation, au besoin. Cela ne serait pas efficace s'il y avait un processus d'approbation et d'attribution.

Prise d'une décision définitive concernant les faux positifs et surveillance générale

171. Un certain nombre de parties ont convenu qu'une procédure de transmission à l'échelon supérieur ou d'appel devrait être disponible lorsque le blocage est

maintenu. Par exemple, Nokia a indiqué que la mise en place d'un mécanisme permettant de résoudre les différends sur la question de savoir si un site spécifique devrait être bloqué pourrait réduire au minimum le blocage excessif. Fenwick McKelvey et Reza Rajabiun ont argué que la surveillance judiciaire est essentielle. Vaxination Informatique a avancé que la transmission à l'échelon supérieur d'une plainte au Conseil devrait être possible.

172. Le CCC a soutenu que le cadre devrait intégrer un élément de prise de décision normalisé autour des décisions de blocage, mais a recommandé que le CCC lui-même n'ait pas ce pouvoir décisionnel.

173. La CIPPIC a fait valoir que tout cadre doit inclure une surveillance active de la part du Conseil, y compris des vérifications ponctuelles des mécanismes de blocage pour faire en sorte que les services appropriés ne soient pas bloqués. La CIPPIC a ajouté que lorsque la gestion du trafic dérape, les éléments de preuve sont difficiles à rassembler pour les utilisateurs finals. Elle fait particulièrement référence aux lettres du personnel chargé de la conformité et des enquêtes à RCCI après que des essais complets des mesures d'étranglement de RCCI ont démontré des violations estimées du cadre des PGTI.

Résultats de l'analyse du Conseil

174. Le Conseil reconnaît que le blocage excessif et les faux positifs sont un élément inévitable du blocage à l'échelle des réseaux. Les services malveillants peuvent être intégrés ou fournis parallèlement à des services légitimes, ou les analyses peuvent interpréter à tort des artefacts ou du trafic de réseau comme étant de nature malveillante alors qu'ils sont inoffensifs.

175. Tel que mentionné ci-dessus, les entreprises ne devraient pas être limitées à un type particulier de technique de blocage. Dans le choix de leurs techniques de blocage, les entreprises doivent toutefois veiller à ce que toutes répercussions sur les services légitimes soient réduites au minimum et limitées à ce qui est nécessaire en vue d'atteindre le but de blocage du trafic malveillant.

176. Indépendamment de l'approche et de la liste de blocage utilisés, le Conseil estime que des mesures de protection doivent être mises en place afin d'atténuer le risque de faux positifs et de blocage excessif, notamment des mécanismes en vue de :

- contrôler les IC avant leur inscription sur toute liste;
- recevoir et enquêter sur les plaintes du public concernant les faux positifs;
- mettre à jour la liste de blocage à la suite d'une plainte en temps opportun;
- mettre à jour la liste de blocage régulièrement, et pas seulement à la suite d'une plainte (un mélange de révision manuelle et de retrait de la liste automatisé des IC

peut être approprié[25] et le blocage sur une base temporaire en appliquant une date d'expiration à la présence d'un IC sur une liste de blocage contribuerait encore plus à réduire les faux positifs);

- veiller à ce que les FST consignent leur blocage efficace des IC et vérifient périodiquement que leurs systèmes de blocage fonctionnent comme prévu.

177. La coordination entre le gestionnaire de la liste de blocage et les FST ainsi que leurs responsabilités respectives pour chacune des étapes énumérées ci-dessus restent à être déterminées pour chaque approche (centralisée et décentralisée). Le Conseil fait remarquer que les FST devraient avoir la capacité de réduire au minimum et de traiter les faux positifs associés aux mécanismes de blocage conformément à l'article 1.3[26] des *Normes d'intervention en cas d'incidents de sécurité pour les fournisseurs canadiens de services de télécommunications (FCST)* du CCCST, mais que cette norme ne précise pas comment cette capacité est mise en œuvre par les FST.

178. Une liste de blocage centralisée aurait l'avantage de réduire le risque de blocage excessif et de faux positifs. En plus d'avoir un gestionnaire central de liste de blocage choisi pour son expertise en matière de contrôle des IC, une liste centralisée serait soumise à un examen plus approfondi par les FST et les autres parties prenantes que toute liste de blocage utilisée par un FST de manière isolée. Elle permettrait également de consolider les évaluations de faux positifs afin de mieux faire en sorte que les rapports de faux positifs soient traités de manière efficace et en temps opportun. Le Bouclier canadien de la CIRA utilise une liste de blocage comprenant des IC de haute confiance fournis par le CCC et, comme indiqué sur la page Web du Bouclier canadien de la CIRA, son ratio de faux positifs par rapport aux blocages valides est très proche de zéro.

179. Une approche décentralisée ne présente pas les mêmes avantages. La majorité des FST qui ont déjà mis en œuvre des listes de blocage commerciales n'ont pas fourni de renseignements concernant leurs taux de faux positifs ni précisé s'ils surveillent ce risque. Le Conseil estime que, avec une approche décentralisée, des mesures de protection supplémentaires doivent être mises en place (p. ex. concernant la manière dont les fournisseurs commerciaux de listes de blocage sont accrédités et par qui), afin que les FST s'assurent que les tiers qui gèrent les listes de blocage atténuent le

---

[25] Le retrait manuel de la liste se produit lorsqu'une personne de confiance, ayant des connaissances techniques, examine les déclarations de faux positifs pour déterminer si un blocage devrait être retiré. Le retrait automatique de la liste se produit lorsque des déclarations de faux positif sont acceptées, mais que le blocage est automatiquement rétabli s'il est ultérieurement confirmé comme étant malveillant. Un exemple de liste de blocage qui utilise le retrait automatique de la liste est la Composite Block List maintenue par Spamhaus.

[26] Cet article énonce que les FST « doivent avoir la capacité de […] mettre en œuvre des stratégies qui permettront de réduire, de filtrer ou de bloquer efficacement le trafic problématique tout en réduisant au minimum les répercussions possibles sur le trafic légitime. »

risque de faux positifs. Des questions particulières sur cette question sont adressées au CDCI à l'annexe 2 de la présente décision.

Conclusion

180. Le Conseil conclut que le trafic des réseaux de zombies constitue un problème important en matière de cybersécurité, tant en termes de volume que de gravité des préjudices.

181. Le Conseil conclut que des mesures réglementaires sont nécessaires, car i) les pratiques actuelles des FST sont diverses et ne sont pas transparentes et manquent un mécanisme pratique et constant pour partager les IC des réseaux de zombies; ii) les FST ont un rôle important à jouer dans le blocage des réseaux de zombies, conformément à une stratégie de défense en profondeur en matière de cybersécurité; iii) les programmes de blocage à l'échelle des réseaux sont efficaces et appropriés; et iv) il existe une confusion entre les parties concernant la base réglementaire du blocage actuel des réseaux de zombies par les FST.

182. Le Conseil conclut que des mesures réglementaires sont nécessaires afin de faire en sorte que le blocage des réseaux de zombies à l'échelle des réseaux fourni par les entreprises canadiennes offre un degré de protection de base. En résumé, lorsque le blocage à l'échelle des réseaux est fourni, il doit se conformer aux principes directeurs suivants : i) la nécessité, ii) la vie privée des clients, iii) la responsabilité, iv) la transparence et v) l'exactitude. Ces principes, décrits à l'annexe 1 de la présente décision, sont destinés à être technologiquement neutres en vue de permettre une flexibilité dans les outils et les techniques de blocage afin que les entreprises puissent s'adapter rapidement aux cybermenaces sophistiquées associées à mesure qu'elles évoluent.

183. Le Conseil demande au Groupe de travail Réseau du CDCI de proposer les paramètres techniques de base du mécanisme de blocage qui pourraient être utilisés, conformément aux principes énoncés à l'annexe 1 de la présente décision, et de déposer un rapport auprès du Conseil. Les paramètres techniques de base du mécanisme de blocage doivent comprendre, au minimum, i) qui déterminera ce qui est bloqué, ii) ce qui est précisément bloqué, et iii) d'autres détails techniques relatifs à la mise en œuvre du mécanisme de blocage, comme indiqué à l'annexe 2 de la présente décision.

184. Le Conseil demande au CDCI de soumettre un rapport **dans les neuf mois** suivant la date de publication de la présente décision, traitant les questions ci-dessus. Les intéressés auront la possibilité de commenter le rapport avant que le Conseil ne tire d'autres conclusions concernant les normes minimales qui feront partie du cadre à appliquer au blocage des réseaux de zombies.

Instructions

185. Les Instructions de 2006[27] et de 2019[28] énoncent que le Conseil, dans l'exercice de ses pouvoirs et de ses fonctions en vertu de la *Loi*, doit mettre en œuvre les objectifs de la politique énoncés à l'article 7 de la *Loi*, conformément aux considérations énoncées dans les Instructions, et devrait préciser comment ses décisions peuvent, le cas échéant, promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation.

186. Le blocage à l'échelle des réseaux du trafic des réseaux de zombies qui se conforme aux principes directeurs énoncés à l'annexe 1 de la présente décision contribuera à protéger les Canadiens contre les préjudices des réseaux de zombies. En décidant d'établir les normes minimales applicables à la fourniture du blocage de réseaux de zombies à l'échelle des réseaux, le Conseil se fie au libre jeu du marché dans la plus grande mesure du possible et ne fait obstacle au fonctionnement d'un libre marché concurrentiel que dans la mesure minimale nécessaire pour atteindre les objectifs. En décidant d'établir des principes directeurs et un processus afin de déterminer les paramètres techniques minimaux, le Conseil emploie des mesures qui sont efficaces et proportionnelles à l'objectif de prévenir le préjudice important causé aux Canadiens par les réseaux de zombies. En outre, le cadre de blocage des réseaux de zombies est destiné à être neutre sur le plan technologique et flexible afin d'encourager l'innovation des entreprises dans le traitement des communications des réseaux de zombies. Enfin, mettre en œuvre un tel cadre favorisera l'atteinte des objectifs stratégiques énoncés aux alinéas 7a), 7b), 7f), 7g), 7h) et 7i) de la *Loi*[29].

Secrétaire général

Documents connexes

- *Appel aux observations – Développement d'un cadre de blocage à l'échelle des réseaux pour limiter le trafic des réseaux de zombies et renforcer la sécurité en*

---

[27] *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication*, DORS/2006-355, 14 décembre 2006

[28] *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation*, DORS/2019-227, 17 juin 2019

[29] Les objectifs de la politique cités sont les suivants : 7a) favoriser le développement ordonné des télécommunications partout au Canada en un système qui contribue à sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions; 7b) permettre l'accès aux Canadiens dans toutes les régions — rurales ou urbaines — du Canada à des services de télécommunication sûrs, abordables et de qualité; 7f) favoriser le libre jeu du marché en ce qui concerne la fourniture de services de télécommunication et assurer l'efficacité de la réglementation, dans le cas où celle-ci est nécessaire; 7g) stimuler la recherche et le développement au Canada dans le domaine des télécommunications ainsi que l'innovation en ce qui touche la fourniture de services dans ce domaine; 7h) satisfaire les exigences économiques et sociales des usagers des services de télécommunication; et 7i) contribuer à la protection de la vie privée des personnes.

ligne des Canadiens, Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2021-9, 13 janvier 2021; modifiée par l'Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2021-9-1, 29 juin 2021

- *Application des obligations réglementaires directement aux entreprises autres que les entreprises de télécommunication qui offrent et qui fournissent des services de télécommunication*, Politique réglementaire de télécom CRTC 2017-11, 17 janvier 2017

- *Mesures réglementaires liées aux dispositions relatives à la confidentialité et à la protection de la vie privée*, Politique réglementaire de télécom CRTC 2009-723, 25 novembre 2009

- *Examen des pratiques de gestion du trafic Internet des fournisseurs de services Internet*, Politique réglementaire de télécom CRTC 2009-657, 21 octobre 2009

- *Accès des entreprises de services locaux concurrentes aux systèmes de soutien à l'exploitation des entreprises de services locaux titulaires*, Décision de télécom CRTC 2005-14, 16 mars 2005

- *Clauses de confidentialité des entreprises canadiennes*, Décision de télécom CRTC 2003-33, 30 mai 2003; modifiée par la Décision de télécom CRTC 2003-33, 11 juillet 2003

- *Examen des règlements généraux des transporteurs publics de télécommunications terrestres assujettis à la réglementation fédérale*, Décision télécom CRTC 86-7, 26 mars 1986

Annexe 1 à la Décision de Conformité et Enquêtes et de Télécom 2022-170

Principes directeurs pour un cadre de blocage des réseaux de zombies à l'échelle des réseaux

Nécessité

Le blocage doit être effectué exclusivement à des fins de cybersécurité[30] et non à d'autres fins, y compris le blocage d'activités autrement illégales, ou le blocage à des fins commerciales, concurrentielles ou politiques.

Précision

Toute répercussion sur les services légitimes doit être aussi minimale que possible, limitée à ce qui est nécessaire pour atteindre le but de blocage du trafic malveillant. Le public doit avoir la possibilité de signaler et de résoudre les faux positifs et le blocage excessif de manière efficace et en temps opportun.

Transparence

Les clients et les clients potentiels doivent recevoir des renseignements clairs concernant les solutions de blocage à l'échelle des réseaux de cybersécurité appliquées par les entreprises. Les renseignements à divulguer doivent être suffisants afin de permettre aux Canadiens de prendre des décisions éclairées concernant les entreprises avec lesquelles ils souhaitent faire affaire, mais ils ne devraient pas être détaillés au point de compromettre l'efficacité du cadre en fournissant des renseignements exploitables aux acteurs malveillants sur la manière de contourner le mécanisme de blocage. En outre, les entreprises doivent maintenir et déposer des indicateurs précis auprès du Conseil afin de permettre la divulgation publique de statistiques concernant l'adoption et l'efficacité du cadre de blocage.

Vie privée des clients

En plus de se conformer à leurs obligations existantes en matière de protection de la vie privée[31], les entreprises devraient mettre en œuvre des pratiques qui renforcent ces obligations afin de tenir compte des spécificités d'un cadre de blocage pour fournir le plus haut niveau de protection de la vie privée des consommateurs.

Responsabilité

Les entreprises devraient documenter et revoir périodiquement tous leurs systèmes de blocage utilisés à des fins de cybersécurité afin de vérifier que leur programme de blocage fonctionne comme prévu.

---

[30] Voir la définition fournie dans la note de bas de page 7.

[31] Voir la *Loi sur la protection des renseignements personnels et les documents électroniques* et les obligations existantes du Conseil concernant la protection des renseignements confidentiels des clients.

Annexe 2 à la Décision de Conformité et Enquêtes et de Télécom 2022-170

Résumé des questions à examiner par le CDCI

Champ d'application technique du cadre (c.-à-d. ce qui est bloqué)

Tel qu'indiqué dans la décision du Conseil ci-dessus, étant donné que les indicateurs de compromission (IC) utilisés par les spécialistes en matière de cybersécurité, y compris les propriétaires de listes de blocage, aux fins du blocage du trafic ne ciblent pas particulièrement les réseaux de zombies, mais plutôt, de manière plus générale, le trafic de logiciels malveillants ou le trafic suggérant des intrusions informatiques, il peut ne pas être pratique d'isoler le trafic des réseaux de zombies au moyen d'IC particuliers. Le Conseil estime à titre préliminaire que le blocage d'autres IC aux fins de cybersécurité devrait, en règle générale, être soumis aux mêmes principes directeurs. Toute approche plus large centrée sur les IC doit être extrêmement bien circonscrite afin d'éviter les risques que l'approche s'élargisse progressivement pour inclure le blocage à d'autres fins.

Questions pour le CDCI

- Existe-t-il des obstacles techniques à l'application des mêmes principes directeurs au blocage de tous les IC?
- Les définitions de la cybersécurité et des IC citées dans les notes de bas de page 7 et 8, respectivement, sont-elles exactes? Dans le cas contraire, il est demandé au CDCI de modifier ces définitions.

Responsabilité des parties prenantes – option de liste de blocage centralisée

Tel qu'indiqué dans la décision du Conseil ci-dessus, une liste de blocage centralisée est l'option la plus efficace et efficiente. Avec cette option, une organisation experte indépendante, telle que, par exemple, le CCC ou la CIRA, pourrait se porter volontaire pour être chargée de la mise à jour d'une liste de blocage de base, y compris l'ajout et la suppression des IC ciblés en vue d'être bloqués, l'évaluation de diverses autres listes de blocage et leur ajout à la liste de base le cas échéant, et la mise à disposition de la liste de blocage de base à tous les FST.

Questions pour le CDCI

- Existe-t-il une organisation experte indépendante, telle que le CCC ou la CIRA, qui est techniquement disposée et capable de maintenir une liste de blocage centralisée à l'usage des FST? Existe-t-il un forum ou une plateforme actuellement utilisée par les FST qui peut mettre cette liste de blocage à la disposition de tous les FST et autres parties prenantes? Si tel est le cas, le Conseil demande que le CDCI indique dans son rapport ces parties et la liste de blocage à utiliser.
- Cette organisation experte indépendante traiterait-elle également les déclarations de faux positifs qui pourraient survenir à la suite de l'application de sa liste de

blocage et actualiserait-elle la liste en conséquence? Dans le cas contraire, qui traitera ces demandes (p. ex. les FST) et comment la liste de blocage centralisée sera-t-elle mise à jour en conséquence? Dans tous les cas, comment le public soumettra-t-il les rapports de faux positifs?

- Les FST et les autres parties prenantes (p. ex. les experts en matière de cybersécurité et les organisations d'application de la loi) auraient-ils la capacité technique de demander l'ajout ou le retrait d'IC particuliers à la liste?

Responsabilité des parties prenantes – option de liste de blocage décentralisée

Tel qu'indiqué dans la décision du Conseil ci-dessus, en complément d'une liste de blocage centralisée ou à la place d'une liste de blocage centralisée si celle-ci n'est pas une option possible, les FST peuvent utiliser d'autres solutions de blocage pour assurer la cybersécurité afin de maintenir la flexibilité et de favoriser l'innovation. Ces solutions incluent le recours à des fournisseurs commerciaux de listes de blocage, pourvu qu'ils soient accrédités pour répondre à certaines exigences.

Questions pour le CDCI

- Qui accréditera les listes de blocage d'une tierce partie pour garantir la conformité aux principes directeurs établis par le Conseil (p. ex. chaque FST ou une organisation centrale)?
- Quels pourraient être les critères pertinents pour l'accréditation d'une liste de blocage d'une tierce partie[32]?
- Par quel mécanisme le public pourra-t-il soumettre un rapport de faux positif pour faire en sorte que les fournisseurs de listes de blocage d'une tierce partie mettent à jour leur liste le cas échéant?
- Y a-t-il d'autres éléments à prendre en compte ou exigences pratiques qui devraient s'appliquer à la gestion et à la mise à jour des listes de blocage des tiers? Un intervenant aurait-il la capacité technique de demander l'ajout d'IC particuliers à toutes les listes existantes utilisées par tous les FST canadiens ou leur retrait?

---

[32] Il existe des exemples de critères d'accréditation de listes de blocage déjà établis, tels que ceux définis par la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) pour établir les listes de réputation et de blocage utilisées dans le système de signalement des cas d'utilisation malveillante des noms de domaine (DAAR) : avoir une certaine longévité, avoir des antécédents au sein des communautés de sécurité opérationnelle, avoir une utilisation omniprésente dans les organisations publiques et privées, faire l'objet d'un examen minutieux de la part des universités et de l'industrie, et avoir des taux de faux positifs suffisamment faibles. Parmi les autres critères possibles, on peut citer, par exemple, l'expérience de la tenue de listes de blocage de réseaux de zombies et de logiciels malveillants, la certification par une organisation de normalisation réputée ou l'approbation par les professionnels du secteur concernés, et l'existence de normes de service pour la prise de mesures en réponse à une déclaration de faux positif.

Méthodes de blocage autres que les listes de blocage centralisées ou décentralisées

Tel qu'indiqué dans la décision du Conseil ci-dessus, les FST peuvent mettre en œuvre d'autres initiatives de blocage en matière de cybersécurité (p. ex. les systèmes exclusifs des FST, des pratiques telles que le blocage des ports de service standard et d'autres meilleures pratiques recommandées).

Question pour le CDCI

- En ce qui concerne les autres initiatives de blocage en matière de cybersécurité, existe-t-il des éléments à prendre en compte ou des exigences techniques qu'il serait pertinent pour le Conseil d'examiner[33]?

Autres détails techniques et de mise en œuvre

Tel qu'indiqué dans la décision du Conseil ci-dessus, le blocage des réseaux de zombies à l'échelle des réseaux fourni par les FST devrait être appliqué par défaut, de sorte que les clients n'aient pas l'option d'y adhérer ou de s'en retirer, car cela irait à l'encontre de le but du cadre. Cependant, il peut y avoir des circonstances dans lesquelles ces options sont nécessaires, comme une phase pilote pendant le processus de mise en œuvre.

Questions pour le CDCI

- Existe-t-il un besoin technique pour permettre à chaque consommateur d'adhérer au système de blocage à l'échelle des réseaux ou de s'y retirer s'il est mis en œuvre par leur opérateur (p. ex. phase pilote pendant le processus de mise en œuvre)?
- Quels autres attributs techniques permettraient de maximiser son adoption et son efficacité?

---

[33] Deux des documents (en anglais seulement) sur les meilleures pratiques de l'Internet Engineering Task Force (Recommendations for Remediation of Bots in ISP Networks RFC 6561et Technical Considerations for Internet Service Blocking and Filtering RFC 7754) et le Port Blocking Report du Broadband Internet Technical Advisory Group peuvent être pertinents et faciliter la recommandation de paramètres techniques du CDCI.