UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

Comité spécial sur les relations entre le Canada et la Chine

Mémoire de
Christopher Parsons
Associé de recherche
principal
Citizen Lab, Munk School of Global Affairs & Public Policy
Université de Toronto

Présentation

1. Je suis associé de recherche principal au Citizen Lab de la Munk School of Global Affairs & Public Policy, à l'Université de Toronto. Ma recherche explore les recoupements entre la loi, les politiques et la technologie et met l'accent sur les questions de sécurité nationale, de sécurité des données et de confidentialité des données. Je soumets ces commentaires à titre professionnel représentant mes points de vue et ceux du Citizen Lab.

Contexte

2. Les efforts successifs déployés à l'échelle internationale pour mondialiser le commerce et les chaînes d'approvisionnement ont mené à la conception, au développement, à la fabrication ou à l'expédition de nombreux produits en Chine. Cela signifie en partie que les entreprises chinoises participent régulièrement à la création et à la distribution de produits utilisés dans la vie quotidienne de milliards de personnes partout dans le monde, y compris des produits intégrés à la vie personnelle des Canadiens et aux infrastructures essentielles dont ils dépendent. L'assurance croissante du gouvernement chinois sur la scène internationale et ses comportements belliqueux, conjugués à des lois opaques sur la sécurité nationale, ont amené de nombreux pays occidentaux à se demander dans quelle mesure on peut faire confiance aux produits provenant de la Chine. De manière plus précise, deux questions sont régulièrement soulevées : les chaînes d'approvisionnement pourraient-elles être utilisées comme levier diplomatique ou commercial, ou autrement les produits fabriqués, transportés ou exploités en Chine serviront-ils à faciliter les opérations de renseignement, d'attaque ou d'influence du gouvernement de ce pays?
3. Depuis des décennies, la gestion des chaînes d'approvisionnement des produits technologiques suscite des préoccupations constantes[1]. Ces dernières années, on s'est concentré sur l'équipement de télécommunications, comme celui produit par ZTE et Huawei[2], ainsi que sur les façons dont les médias sociaux comme WeChat ou TikTok pourraient servir subrepticement à faire avancer les intérêts du gouvernement de la Chine. En raison de ces préoccupations, certains alliés du Canada ont officiellement ou officieusement bloqué, des infrastructures essentielles, l'équipement des fournisseurs de services de télécommunications chinois. Aux États-Unis, les militaires qui se trouvent à la base ne peuvent se procurer que certains appareils mobiles. On leur demande de ne pas utiliser d'applications comme TikTok, et l'administration Trump cherchait activement à modifier les conditions de disponibilité des médias sociaux sur le marché américain.
4. Des législateurs et certains professionnels de la sécurité s'inquiètent que les produits de ZTE ou de Huawei puissent être délibérément modifiés de manière à faciliter les opérations chinoises de renseignement ou d'attaque, ou faire l'objet de négociations bilatérales ou de conflits avec le gouvernement de la Chine. De plus, les plateformes de médias sociaux pourraient être utilisées pour faciliter la surveillance des utilisateurs internationaux des applications ou les algorithmes des plateformes pourraient être configurés de manière à censurer les contenus ou à mener des opérations d'influence imperceptible.
5. Tout comme les chaînes d'approvisionnement suscitent des préoccupations généralisées, l'état de la sécurité (ou de l'insécurité) informatique suscite également de profondes inquiétudes. De graves vulnérabilités informatiques sont exposées et exploitées quotidiennement. Les exploitants d'État tirent parti des vulnérabilités du matériel et des logiciels pour faciliter les opérations de découverte,

[1] Voir : Clair Brown et Greg Linden. (2005). « Offshoring in the Semiconductor Industry: A Historical Perspective » (Délocalisation dans l'industrie des semi-conducteurs : une perspective historique), à http://isapapers.pitt.edu/58/1/2005 -02_Brown.pdf.

[2] Le Citizen Lab a publié un rapport exhaustif sur Huawei et la 5G, ainsi que sur les actions canadiennes en jeu. De nombreux commentaires dans cette présentation découlent de la recherche en question. Voir : https://citizenlab.ca/2020/12/huawei-5g-clarifying-the-canadian-equities-and-charting-a-strategic-path-forward/.

d'exploitation et d'attaque de réseaux informatiques, les opérations étant souvent réparties entre les organes officiels de sécurité nationale, les sections des forces armées nationales et les exploitants informels adjacents à l'État (et souvent criminels). De même, les responsables d'organisations criminelles font la découverte de vulnérabilités des systèmes numériques et en tirent parti pour procéder au vol d'identité ou propriété intellectuelle pour le compte de leurs clients ou vendre ces vulnérabilités sur les marchés noirs, les utiliser ainsi que les monnayer dans le cadre de campagnes de rançongiciels, et pour autrement s'adonner à des activités socialement délétères.

6. Dans l'ensemble, les problèmes de gestion de la chaîne d'approvisionnement et d'insécurité informatique soulèvent des questions fondamentales de confiance : comment pouvons-nous avoir l'assurance que l'équipement ou les plateformes n'ont pas été délibérément modifiés ou exploités au détriment des intérêts canadiens? Et compte tenu de l'état d'insécurité informatique, comment pouvons-nous compter sur les technologies dotées d'équipes distribuées et internationales de développement et de production? Dans le reste de cette présentation, j'approfondis les préoccupations particulières liées à la confiance et je trouve des moyens d'instaurer la confiance ou, à tout le moins, de déterminer dans quelles circonstances nous devrions faire moins confiance au matériel ou aux services offerts aux Canadiens et aux organisations canadiennes.

Atténuation des dépendances à la chaîne d'approvisionnement

7. Les chaînes d'approvisionnement peuvent être opposées aux Canadiens de plusieurs façons, mais je traiterai d'abord des risques liés aux dépendances à la fabrication ou au développement. Les États, y compris la Chine, ont adopté des politiques industrielles pour protéger et favoriser les entreprises technologiques autochtones. Huawei, à titre d'exemple, existe en partie en raison des politiques du gouvernement chinois visant à la protéger[3]. L'entreprise produit de l'équipement largement utilisé partout dans le monde et vendu à des tarifs incroyablement concurrentiels. L'entreprise bénéficie de sources de revenus nationales fiables tout en étant en mesure d'offrir des prêts à faible coût de la part de banques garanties par l'État afin que les entreprises puissent acquérir des produits Huawei à des coûts en capital à court et à long terme comparativement plus faibles. Résultat : Huawei et d'autres entreprises chinoises peuvent proliférer sur les marchés mondiaux grâce à un soutien notable de l'État.
8. Les infrastructures de télécommunications sans fil contemporaines et celles de prochaine génération seront probablement principalement produites par Nokia et Ericsson, ainsi que par Huawei, et d'autres entreprises fourniront des éléments de piles de réseaux 5 G. Les équipements de réseaux ont tendance à être « persistants », dans la mesure où les fournisseurs conçoivent souvent leurs équipements de manière à ce qu'ils fonctionnent ensemble et qu'ils aient tendance à être moins efficaces avec les produits des concurrents. En conséquence, l'adoption des produits d'un fournisseur dès le début d'une importante dépense d'infrastructure essentielle, comme la 5G, peut faire en sorte qu'il soit très difficile d'intégrer les produits d'un autre fournisseur pour les éléments subséquents du chemin de mise à niveau du réseau. Il a été constaté que les équipements Huawei, en particulier, étaient très « persistants »; l'adoption des produits de l'entreprise dès maintenant fera augmenter les coûts d'intégration des équipements autres que ceux d'Huawei dans les réseaux de télécommunications[4].
9. Si les entreprises canadiennes étaient autorisées à acheter de l'équipement de Huawei pour leurs réseaux 5G, elles pourraient avoir une motivation financière à le faire. Il existe toutefois un risque que le gouvernement chinois utilise des dépendances à l'égard de l'équipement de Huawei à son avantage dans le cadre de futures négociations commerciales ou diplomatiques, sans quoi une monoculture basée sur un seul fournisseur pourrait en découler. Dans le premier cas, le

[3] Le fondateur de l'entreprise a déclaré : « [S]'il n'y avait pas eu de politique gouvernementale pour protéger [les entreprises appartenant à l'échelle nationale], Huawei n'existerait plus. » Voir : Alberto F. De Toni. (2011). *International Operations Management, Lessons in Global Business*. Londres : Routledge, p. 128. Citant Xiao, 2002, p. 127.

[4] Voir : https://www.ncuscr.org/technology-regulation-industry-impact.

gouvernement du Canada pourrait subir des pressions pour adopter des politiques « favorables à la Chine » afin que les entreprises canadiennes puissent continuer à recevoir l'équipement nécessaire au maintien ou à l'entretien de leurs réseaux 5G ou de leurs futures infrastructures 6G. Dans le second cas, le fait de n'avoir qu'un seul fournisseur, ou même un seul fournisseur principal, assurant la prestation d'un réseau de télécommunications donné, risque d'augmenter la probabilité qu'une vulnérabilité à la sécurité trouvée dans un certain appareil puisse être reproduite dans tous les appareils semblables du fournisseur dans un réseau. Scott Jones, chef adjoint de la Sécurité des technologies de l'information au CST, a soulevé cette question auprès du Comité permanent de la sécurité publique et nationale : « [...] on ne veut pas d'un seul et unique fournisseur. Cela vous rend vulnérable, dans tout votre spectre et dans toutes vos entreprises de télécommunications, au même élément exactement. Il est préférable de faire appel à différents fournisseurs… c'est très sécuritaire, parce que vous ne pouvez pas aisément monter et descendre dans la supposée pile de communications. C'est l'un des éléments clés de la 5G[5] ».

10. Nous **recommandons** au gouvernement du Canada d'adopter une politique selon laquelle aucun produit d'un seul fournisseur ne peut composer une majorité écrasante de l'équipement d'un réseau privé de fournisseurs de télécommunications. L'objectif est triple. Premièrement, il faut réduire la capacité d'un gouvernement étranger à tirer parti des dépendances excessives à l'égard d'un fournisseur pour mener des négociations diplomatiques, commerciales ou de défense. Deuxièmement, cette politique indépendante des fournisseurs nuirait à la probabilité que des monocultures basées sur un seul fournisseur découlent de propriétés de sécurité négatives simultanées. Troisièmement, cela encouragerait la concurrence entre les fournisseurs de télécommunications et pourrait donc réduire les coûts en capital pour les fournisseurs canadiens de télécommunications.
11. En l'absence d'entreprises technologiques autochtones, les Canadiens doivent pouvoir compter sur les produits fabriqués par des entreprises actives en Europe occidentale ou en Asie et leur faire confiance. Dans une certaine mesure, il s'agit d'un résultat normal de la mondialisation, mais en même temps, cela signifie que la détermination de la façon de faire confiance aux produits dépend maintenant des évaluations des fournisseurs étrangers en fonction du renseignement étranger et des considérations des lois sur la sécurité nationale des pays étrangers, de la façon dont ces lois pourraient être appliquées aux produits des entreprises étrangères, ainsi que de l'évaluation technique des produits des entreprises. En fait, un certain nombre d'évaluations de la fiabilité sont effectuées notamment pour déterminer si un produit conçu par une entreprise dans un pays occidental et fabriqué au moins partiellement dans des pays où les lois sur la sécurité nationale sont opaques ou moins bien comprises, comme la Chine, devrait être considéré comme un produit plus ou moins fiable que ceux qui sont également presque entièrement fabriqués en Chine et expédiés depuis ce pays. En outre, même dans le cas des entreprises occidentales qui produisent de l'équipement de télécommunications[6] ou fournissent des plateformes de réseautage social, l'histoire montre que ces entreprises peuvent être cooptées par les intérêts des États occidentaux[7].
12. Étant donné l'état actuel de la fabrication de produits et de la prestation de services, nous **recommandons** que toute politique adoptée pour renforcer la confiance dans les produits et les services demeure indépendante des fournisseurs et qu'elle soit conçue pour reconnaître que les nations concurrentes évidentes et les nations alliées peuvent être motivées à obliger les entreprises à ajuster leurs produits pour atteindre des objectifs nationaux.

Établissement de normes et gouvernance d'Internet

13. À l'heure actuelle, un petit nombre d'entreprises sont bien placées pour fournir de l'équipement 5G. À

[5] Voir : https://hillnotes.ca/2020/02/13/5g-technology-opportunities-challenges-and-risks/
[6] Voir par exemple : https://www.zdnet.com/article/congress-asks-juniper-for-the-results-of-its-2015-nsa- backdoor-investigation/.
[7] Voir par exemple : https://fr.wikipedia.org/wiki/PRISM_(programme_de_surveillance).

moins de changements importants, cette situation persistera probablement lorsque les infrastructures 6G seront prêtes à être déployées. Cela est en partie attribuable à une défaillance industrielle : Nortel n'est plus, et les entreprises américaines dans le domaine des infrastructures ne se concentrent pas sur les normes et les technologies sans fil autant que leurs homologues européens et chinois.

14. Il est peut-être beaucoup trop tard pour que les Canadiens influencent considérablement la mise au point de normes 5G, mais les membres des groupes de travail 6G ont déjà commencé à se rencontrer. Le gouvernement canadien devrait encourager activement les entreprises et les experts canadiens à participer à ces groupes de travail pour, à tout le moins, s'assurer que les propriétés de sécurité et de protection de la vie privée sont intégrées de façon agressive aux normes à titre d'éléments par défaut.
15. Nous **recommandons** au gouvernement canadien de s'assurer que les fournisseurs de télécommunications canadiens activent toutes les propriétés de sécurité disponibles qui sont énumérées dans les normes 5G et dont l'activation est parfois considérée comme optionnelle. Cela, de concert avec les politiques de sécurité existantes, pourrait renforcer la confiance dans les nouveaux réseaux 5G que les Canadiens utiliseront pendant des décennies.
16. Nous **recommandons** également au gouvernement du Canada d'explorer des manières de veiller à ce que les intérêts canadiens soient mieux représentés pendant les processus d'établissement des normes 6G, qui sont déjà en cours. De manière plus précise, le gouvernement pourrait accorder des incitatifs fiscaux aux sociétés et offrir des fonds à des organisations non gouvernementales ou à des organismes de bienfaisance, de sorte que les Canadiens et les intérêts canadiens soient davantage intégrés aux processus d'élaboration des normes.
17. En outre, le gouvernement doit évaluer attentivement les efforts déployés par l'Union internationale des télécommunications (UIT) et d'autres organismes de normalisation[8], au sein desquels Huawei et le gouvernement de la Chine tentent de faire progresser le Nouvel IP, protocole censé permettre des fonctionnalités de l'Internet des objets à faible latence, mais qui pourrait également favoriser une surveillance et un contrôle accrus des données à l'intérieur des frontières nationales[9]. Pour parler franchement, les propriétés pourraient, si elles sont mises en œuvre, permettre davantage aux États autoritaires de s'engager dans la répression intérieure.
18. Nous **recommandons** au gouvernement du Canada de continuer de collaborer avec ses partenaires et alliés internationaux pour étudier attentivement le Nouvel IP, de faire participer des experts non gouvernementaux à ses délégations de l'UIT qui discutent du Nouvel IP et de coordonner avec ses alliés les efforts visant à modifier ou à s'opposer à des éléments de la norme proposée qui sont susceptibles d'être utilisés pour améliorer les pratiques autoritaires.

Vulnérabilités de sécurité fortuites ou délibérées

19. La complexité des systèmes numériques contemporains signifie que les erreurs logicielles et matérielles sont incluses accidentellement ou accessoirement dans ces systèmes. Dans certains cas, ces erreurs peuvent être assez graves (p. ex. l'inclusion d'un code vulnérable ancien et connu dans un logiciel) ou plus semblables à des fautes d'orthographe ou de grammaire (p. ex. l'absence de délimitation correcte d'un bloc de code[10]). Quoi qu'il en soit, les personnes qui travaillent pour des États-nations ou des entreprises privées ou encore à titre personnel recherchent régulièrement ces erreurs et peuvent élaborer des façons de les utiliser pour obliger les systèmes numériques à aller à l'encontre des intérêts de leurs propriétaires ou de leurs utilisateurs.
20. Individuellement, les gouvernements des États-nations peuvent obliger les responsables

[8] Hoffmann, Stacie, Dominique Lazanski et Emily Taylor. « Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet. » *Journal of Cyber Policy* 5, no 2 (3 mai 2020) : 239–64. https://doi.org/10.1080/23738871.2020.1805482.
[9] Pour en savoir plus, consultez https://oxil.uk/publications/2020-08-29-standardising-the-splinternet/.
[10] Pour en savoir plus, consultez https://www.wired.com/2014/02/gotofail/.

d'organisations à injecter des vulnérabilités dans le matériel ou les logiciels. Par le passé, l'équipement a été interrompu et modifié avant la livraison finale, les protocoles de chiffrement ont été affaiblis et diffusés par les organismes de normalisation et les logiciels ont été délibérément modifiés pour permettre des activités non autorisées. Tout comme les gouvernements occidentaux ont entrepris chacune des activités susmentionnées, on craint que le gouvernement chinois ait recours à sa loi nationale sur le renseignement ou à sa loi contre l'espionnage pour obliger les fournisseurs chinois à modifier de la même façon les produits qui sont produits ou fabriqués en Chine avant d'être livrés à des clients étrangers.

21. Les allégations selon lesquelles Huawei aurait modifié des équipements avant de les fournir à certains clients, bien qu'elles soient courantes, ne sont pas fondées sur les faits : à ce jour, peu d'informations de source ouverte appuient ces affirmations, qui ont été faites par les États-Unis et d'autres gouvernements occidentaux. Si des analyses publiques du Centre d'évaluation de la cybersécurité de Huawei (HCSEC) du Royaume-Uni ont permis de révéler d'importantes vulnérabilités dans les équipements de Huawei, aucune n'est considérée comme ayant été délibérément insérée. Les conclusions de ces analyses mettent en valeur la vérification publique de l'équipement qui compose les infrastructures essentielles. Malgré les conclusions du HCSEC, la possibilité de modifier le matériel ou les logiciels à la demande du gouvernement demeure, et les techniques qui pourraient être employées, comme la modification des composants matériels ou l'introduction d'instructions de système d'exploitation dont les exploitants de l'État pourraient tirer parti, restent plausibles.
22. Aucune politique ne peut atténuer les risques posés par des vulnérabilités imprévues ou délibérées. Certaines politiques peuvent toutefois réduire la prévalence des vulnérabilités imprévues et augmenter le coût de l'introduction délibérée de vulnérabilités dans les systèmes numériques.
23. Premièrement, nous **recommandons** que les organisations soient tenues de fournir une « liste de biens logiciels » pour tout produit d'infrastructure essentielle, la facture fournissant une identification structurée des bibliothèques de logiciels et des dépendances ainsi que de leurs versions qui sont incluses dans les systèmes numériques[11]. Cela aiderait les organisations qui vérifient le code numérique et les dépendances à évaluer plus rapidement s'il existe des vulnérabilités préexistantes connues dans la base de codes qui sous-tend un produit donné. Par exemple, si une organisation vendait un routeur de télécommunications et divulguait qu'elle utilise un logiciel désuet ou vulnérable, sa vente pourrait être interdite avant son entrée sur le marché canadien. Si une vulnérabilité était constatée dans un composant logiciel sous-jacent après la vente de l'appareil, les agences canadiennes pourraient mieux déterminer quels produits vendus au Canada dépendaient de ce composant. Cela ne remédierait pas à tous les problèmes de sécurité, mais fournirait des renseignements qui font actuellement défaut sur le marché canadien ou mondial.
24. Au Canada, certains produits informatiques sont actuellement assujettis au programme des Critères communs[12], dans le cadre duquel les laboratoires de recherche canadiens et ceux des pays alliés effectuent des évaluations officielles de sécurité des produits, et des évaluations plus coûteuses (et relativement rarement effectuées) ayant pour objet de déterminer si les produits possèdent réellement les propriétés de sécurité qu'ils sont officiellement censés posséder. Les évaluations canadiennes de l'équipement de télécommunications, y compris celui de Huawei, sont drapées dans le secret des entreprises et du gouvernement, bien qu'elles permettent de découvrir et de corriger au moins certaines vulnérabilités[13]. Par contre, au Royaume-Uni, on évalue plus intensivement l'équipement de Huawei par l'entremise de son HCSEC et on publie les résultats de ces évaluations, qui ont maintes fois permis de révéler des vulnérabilités imprévues critiques nécessitant l'apport de mesures correctives. Le gouvernement du Canada n'a aucun moyen d'évaluer lui-même toutes les infrastructures essentielles, mais il pourrait établir des partenariats avec des alliés pour que les pays

[11] Pour en savoir plus, consultez : https://www.ntia.gov/SBOM.
[12] Pour une liste des produits des Critères communs, consultez le site https://www.commoncriteriaportal.org/products/. [13] Pour en savoir plus, consultez : https://cyber.gc.ca/fr/nouvelles/programm-dexamen-de-la-securite-du-cst-visant-les-technologies-3g-4g-et-lte
[13] Voir : https://www.cse-cst.gc.ca/fr/media/media-2019-03-08.

évaluent collectivement les produits d'infrastructures essentielles et publient ensuite leurs constatations; dans l'ensemble, leurs travaux feraient augmenter la probabilité que des vulnérabilités soient découvertes et corrigées, tout en rendant plus difficile pour les exploitants étatiques d'en intégrer délibérément aux produits achetés en vue d'être utilisés au Canada ou dans les pays alliés.

25. Deuxièmement, nous **recommandons** la création de cadres et de processus d'évaluation officiels, de préférence en tandem avec les gouvernements d'États alliés, pour des catégories de systèmes qui composent l'infrastructure essentielle canadienne (p. ex. les systèmes de télécommunications ou d'énergie), et par la suite, la coordination des évaluations de l'infrastructure essentielle par le gouvernement et ses alliés, et leur publication.
26. Au Centre de la sécurité des télécommunications (CST), on utilise actuellement un cadre de gestion des actions (CGA) pour déterminer s'il y a lieu de conserver les vulnérabilités des services de renseignement étrangers, de l'aide gouvernementale et des cyberopérations défensives ou offensives ou, plutôt, de divulguer ces vulnérabilités aux fournisseurs ou aux responsables des collectivités pour y remédier [14]. À l'heure actuelle, le Cadre permet au Centre d'établir les vulnérabilités soit dans le cadre de l'évaluation de l'équipement qui est installé dans des réseaux canadiens ou qui devrait l'être, soit parce que des chercheurs canadiens les ont signalées au Centre en vue de leur correction. Dans les cas où des vulnérabilités sont découvertes dans des systèmes se rapportant à des infrastructures essentielles ou dans des dispositifs électroniques qui sont utilisés de façon importante par la population, les responsables du CST devraient être tenus de les divulguer, afin de les corriger et ainsi de mieux s'assurer que la population peut faire confiance aux dispositifs et aux infrastructures dont elle a besoin.
27. Troisièmement, nous **recommandons** que le gouvernement adopte une politique selon laquelle il divulgue toutes les vulnérabilités du matériel de télécommunications et d'autres infrastructures essentielles ainsi que les vulnérabilités des dispositifs personnels utilisés de façon importante dans le cadre des activités d'assurance de l'information qui consistent à évaluer le matériel pouvant être installé dans les réseaux de télécommunications canadiens, dans d'autres infrastructures essentielles ou dans des dispositifs électroniques utilisés de façon importante par les Canadiens et les résidents du Canada.
28. Quatrièmement, nous **recommandons** que toutes les vulnérabilités signalées au Centre canadien pour la cybersécurité soient divulguées aux fournisseurs ou aux responsables des collectivités de pouvoir faire l'objet de correctifs, et que le CST ne les utilise jamais dans le cadre de ses activités de renseignement étranger, d'aide gouvernementale ou de cyberopérations défensives ou offensives avant ces divulgations.

Médias sociaux chinois

29. Les pays occidentaux sont de plus en plus méfiants à l'égard des plateformes de médias sociaux chinoises, car elles se sont étendues au-delà de l'Asie et sont devenues populaires auprès des auditoires occidentaux. En 2019, la plateforme WeChat comptait 1,15 milliard d'utilisateurs en Chine et à l'étranger, et 45 milliards de messages ont été envoyés quotidiennement au moyen de celle-ci. Les dirigeants de Bytedance, la société mère de TikTok/Douyin, ont déclaré qu'il y avait 1,29 milliard d'utilisateurs actifs en novembre 2020, dont environ 689 millions utilisaient le service TikTok[15]. Alors que l'application WeChat fonctionne actuellement comme une plateforme numérique complète en Chine, avec des miniprogrammes servant à étendre massivement son utilité, bon nombre de ses fonctions principales, dont WeChat Pay, sont de plus en plus utilisées au Canada. TikTok, en revanche, continue d'offrir principalement sa fonctionnalité de base, soit la possibilité de créer et de visualiser du contenu court, tandis que l'évaluation algorithmique du contenu préféré peut être fondée sur les consultations passées et sur les décisions prises par le personnel.

[14] Voir : https://backlinko.com/tiktok-users.
[15] Voir : https://citizenlab.ca/2020/05/we-chat-they-watch/.

30. Comme pour les autres entreprises de matériel et de logiciels situées en Chine, les entreprises de plateformes de médias sociaux doivent se conformer aux lois d'État en matière de sécurité nationale et de contre-espionnage. Des recherches menées par le passé par le Citizen Lab ont permis de démontrer qu'il existe des écarts considérables entre les façons dont les entreprises censurent leurs plateformes, et, en outre, que la façon dont les responsables des plateformes surveillent, censurent et suppriment l'information divulguée évolue souvent.
31. Les législateurs et les organismes gouvernementaux partout en Occident soulèvent de plus en plus de préoccupations au sujet de ces deux plateformes. Dans le cas de WeChat, la recherche de Citizen Lab a révélé que même les utilisateurs internationaux de la plateforme qui enregistrent leurs comptes hors de Chine et utilisent des numéros de téléphone non chinois peuvent faire l'objet d'une surveillance politique qui : par la suite, est utilisée pour développer la censure politique pour les utilisateurs chinois de WeChat[16]. Le même projet de recherche a révélé que les modalités de service publiques et les politiques de confidentialité de WeChat ne révélaient pas que ces activités avaient lieu et que les efforts visant à utiliser les lois canadiennes sur la protection de la vie privée pour mieux comprendre la nature de cette surveillance étaient vains. La journaliste du Toronto Star Joanna Chiu a souligné dans son rapport que le contenu canadien comme celui de Meng Wanzhou avait été bloqué par le passé, alors que les mèmes à l'appui de la détention de Michael Kovrig pouvaient être affichés et partagés[17]. Le SCRS a averti les députés qu'ils devaient éviter d'utiliser WeChat en raison de risques nébuleux de cybersécurité[18]. Individuellement, lors des dernières élections fédérales, Tencent n'a pas produit de registres de publicité numérique, comme l'exige la loi canadienne, mais a accepté les publicités politiques[19]. En outre, dans un rapport de l'Australian Strategic Policy Institute (ASPI) sont rassemblés des exemples de messages d'utilisateurs de WeChat en dehors de la Chine, comme des messages publics d'ambassades étrangères, qui restent soumis à la censure. Le même rapport présentait également des exemples d'autorités chinoises qui exigeaient de particuliers, sous la menace, qu'ils se censurent, sans quoi leur famille risquait d'en subir les conséquences[20].
32. Dans le cas de TikTok, il existe au moins deux principaux ensembles de préoccupations[21.] Tout d'abord, on craint que de grands volumes de renseignements sur les utilisateurs soient recueillis par l'entremise de l'application et ensuite utilisés, maintenant ou dans un proche avenir, pour contribuer à faciliter la sécurité de l'information chinoise ou les opérations de renseignement étrangères. Ces inquiétudes reposent sur l'idée que les données recueillies par TikTok, qui rappellent les activités de collecte des entreprises occidentales de médias sociaux, pourraient être utiles dans les opérations de ciblage numérique étatique. Ensuite, on craint que les algorithmes de présentation de contenu de TikTok puissent être utilisés dans le cadre d'opérations d'influence pour développer des perceptions positives de la Chine en faisant la promotion de certains contenus et en empêchant les utilisateurs occidentaux d'accéder à d'autres contenus. Dans le rapport susmentionné d'ASPI sont résumés les cas survenus jusqu'à présent, y compris l'interdiction d'accès au réseau de certains contenus LGBTQ+ (c.-à-d. que le contenu peut être affiché sur la plateforme, mais est largement ou entièrement caché aux autres utilisateurs), certains documents concernant les manifestations aux États-Unis sur le définancement des forces de police, et la promotion de contenus prochinois sur le Xinjiang. En août 2020, le gouvernement chinois a ajouté des algorithmes de recommandation de contenu à sa liste de contrôle des exportations en réponse aux efforts américains visant à forcer TikTok à vendre ou à divulguer ses algorithmes de promotion de contenu (entre autres efforts).
33. Bien que l'administration Trump ait cherché à entraver le fonctionnement de WeChat et de TikTok aux États-Unis, les efforts ont jusqu'ici été inefficaces. Au Canada, on n'a pas déployé d'efforts

[16] Voir : https://www.vice.com/fr/article/zmana5/experts-say-we-should-watch-out-for-wechats-influence-in-canadas-election.
[17] Voir : https://ipolitics.ca/2019/07/05/mps-staff-warned-not-to-use-chinese-app-wechat-due-to-cybersecurity-risks/.
[18] Voir : https://www.cbc.ca/news/politics/wechat-election-social-media-1.5318589.
[19] Voir : https://www.aspi.org.au/report/tiktok-wechat.
[20] Pour une discussion plus détaillée et axée sur les États-Unis, voir : https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks.

équivalents pour empêcher les citoyens ou les résidents d'utiliser ces applications. À l'heure actuelle, empêcher ces entreprises de fournir des services représente vraisemblablement un manifeste dépassement des limites lorsque l'on tient compte des risques réels que représentent les services. Toutefois, le gouvernement canadien pourrait exiger que toutes les plateformes de médias sociaux, y compris les plateformes chinoises, se conforment à un ensemble d'exigences afin de continuer à fonctionner légalement au Canada et il importe de mieux comprendre comment ces entreprises fonctionnent en ce qui concerne les données des utilisateurs et la conformité aux demandes gouvernementales de données ou de modification de la livraison du contenu des plateformes.

34. Tout d'abord, nous **recommandons** que les entreprises soient tenues de publier leurs directives sur la modération du contenu dans lesquelles elles devraient expliquer l'endroit où se trouvent les modérateurs de contenu, la manière dont ces directives cadrent avec les lois nationales, ainsi que les processus entrepris pendant la modération. Dans le cadre de ces directives, elles devraient aussi expliquer la façon dont elles utilisent des processus algorithmiques et humains pour définir l'accès au contenu, le restreindre ou le retirer.
35. Deuxièmement, nous **recommandons** que les entreprises soient tenues de publier des lignes directrices expliquant comment leurs plateformes sont soumises à la surveillance imposée par l'État et, le cas échéant, à la censure. Cela devrait comprendre une description détaillée des lois pertinentes au fur et à mesure de leur mise en œuvre sur la plateforme et de tous les processus que l'organisation met en place pour contester les efforts de surveillance ou de censure du contenu ainsi que des explications détaillées sur la manière dont les personnes sont informées de l'intégration de leur contenu aux processus de surveillance ou de censure de la plateforme, accompagnées d'exemples d'infraction par certains contenus des lois ou des règlements.
36. Troisièmement, nous **recommandons** que les organisations soient tenues de publier leurs lignes directrices sur la sécurité et l'accès des organismes gouvernementaux, qui expliquent comment et dans quelles circonstances une organisation répondra aux ordres ou aux demandes des organismes étatiques. Ces lignes directrices devraient expliquer comment l'organisation répond aux demandes du gouvernement où se trouve son siège social, ainsi qu'aux demandes des autorités internationales comme celles du Canada. Elle doit préciser les processus en place pour protéger les utilisateurs et les communautés de la plateforme.
37. Quatrièmement, nous **recommandons** que les organisations soient tenues de publier des rapports de transparence. Ces rapports doivent indiquer la régularité à laquelle les autorités gouvernementales font des demandes de renseignements sur les utilisateurs, les motifs de ces demandes, la réceptivité de l'organisation à ces demandes ainsi que la quantité et le type de données qui sont divulguées. Ces rapports doivent également inclure des renseignements sur le nombre de fois où les autorités ont demandé directement que des contenus précis soient supprimés ou fassent l'objet d'une interdiction d'accès au réseau, ainsi que sur la question de savoir si les organismes gouvernementaux ont exigé de certaines classes ou de certains types de renseignements particuliers qu'ils soient bloqués ou supprimés ou qu'ils fassent l'objet d'une interdiction d'accès. Cette dernière catégorie d'information peut comprendre de l'information politique, de l'information relative aux droits de la communauté LGBTQ+ ou encore de l'information des affaires étrangères ou d'autres typologies à développer en association avec des organisations internationales de défense des libertés civiles.
38. Cinquièmement, nous **recommandons** que les organisations soient tenues de mettre leurs algorithmes à la disposition du gouvernement, afin de lui permettre de vérifier dans quelles situations il y a lieu de soupçonner que ces algorithmes servent à bloquer ou à censurer les communications licites au Canada ou à interdire leur accès au réseau, à faciliter des opérations d'influence, ou encore à s'immiscer dans les opérations nationales ou les relations internationales.
39. Sixièmement, nous **recommandons** que les organisations soient tenues de divulguer dans quels cas elles échangent de l'information sur les utilisateurs ou du contenu se trouvant sur leur plateforme entre leur siège social et leurs bureaux régionaux, ainsi que dans quelles conditions et de quelle

manière elles le font, et ce, en particulier lorsque leur siège social ou leurs bureaux régionaux sont situés dans des régions ayant de piètres antécédents en matière de droits de la personne, d'application régulière de la loi ou encore de lois ou de pratiques en matière de protection de la vie privée.

Mot de la fin

40. Les recommandations susmentionnées visent à mieux faire en sorte que les Canadiens puissent se fier à l'infrastructure essentielle, aux appareils électroniques et aux services et plateformes numériques dont ils ont besoin au quotidien. Les présents commentaires sont présentés dans le contexte des risques posés par le gouvernement de la Chine, mais il convient de souligner que la menace la plus importante des derniers mois en matière de cybersécurité et de renseignement est le fait que des exploitants russes et chinois ont pénétré dans l'outil de surveillance du rendement des réseaux de SolarWinds et, par la suite, accédé aux réseaux d'organisations de nature délicate qui utilisent les produits de l'entreprise. Le fait que SolarWinds était une organisation exploitée aux États-Unis n'a pas intrinsèquement rendu son produit plus sûr ou résilient, dans le contexte des opérations de renseignement étrangères, que ceux développés ou fabriqués dans un pays autoritaire.
41. En effet, toute position adoptée par le gouvernement canadien doit reconnaître que les auteurs de menaces recherchent les vulnérabilités qui existent dans les produits, sans trop se préoccuper de l'endroit où ces produits sont développés ou produits. En conséquence, nous invitons les membres du Comité à examiner attentivement toutes les recommandations qui seront adoptées afin de s'assurer que non seulement ces recommandations touchent les entreprises chinoises ou celles ayant des activités en Chine, mais également qu'elles contribuent à l'amélioration de la sécurité intégrée de toutes les technologies d'infrastructure essentielle, des appareils électroniques utilisés par la population et les résidents, ainsi que des services numériques auxquels ces derniers ont recours. Ce n'est qu'en améliorant de façon générale la sécurité intégrée des technologies contemporaines que l'on protégera mieux la population contre des exploitants nationaux et étrangers qui travaillent à l'encontre des intérêts nationaux et étrangers.

L'organisation

42. Les points de vue que j'ai présentés sont les miens et sont fondés sur des recherches que mes collègues et moi-même avons effectuées à mon lieu de travail, le Citizen Lab. Le Citizen Lab est un laboratoire interdisciplinaire établi à la Munk School of Global Affairs and Public Policy de l'Université de Toronto. Il met l'accent sur la recherche, le développement et les politiques stratégiques de haut niveau ainsi que l'engagement juridique au croisement des technologies de l'information et des communications, des droits de la personne et de la sécurité mondiale.
43. Nous utilisons une approche « mixte » pour la recherche combinant les pratiques des sciences politiques, du droit, de l'informatique et des études régionales. Nos recherches comprennent les enquêtes sur l'espionnage numérique contre la société civile; la documentation du filtrage d'Internet et d'autres technologies et pratiques qui ont une incidence sur la liberté d'expression en ligne; l'analyse des contrôles de protection de la vie privée, de la sécurité et de l'information des applications populaires; ainsi que l'examen des mécanismes de transparence et de responsabilisation pertinents pour la relation entre les entreprises et les organismes d'État concernant les données personnelles et d'autres activités de surveillance.