UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

Comité permanent de la sécurité publique et nationale

La cybersécurité dans le secteur financier en tant que question de sécurité économique nationale

Mémoire présenté par

Christopher Parsons, Ph. D.

Attaché de recherche

Citizen Lab, Munk School of Global Affairs & Public Policy

de l'Université de Toronto

munkschool.utoronto.ca

At Trinity College
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

At the Observatory
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

Introduction

1. Je suis attaché de recherche au Citizen Lab de la Munk School of Global Affairs & Public Policy de l'Université de Toronto. Mes recherches s'intéressent à l'intersection du droit, des politiques et de la technologie, en mettant l'accent sur des questions de sécurité nationale, de sécurité des données et de protection des renseignements personnels. Je présente ces commentaires à titre professionnel afin d'exprimer mes opinions et celles du Citizen Lab.

L'état de l'insécurité informatique

2. Les organismes gouvernementaux canadiens, les entreprises privées, les institutions financières et les particuliers comptent sur des infrastructures informatiques courantes. Les appareils iPhone d'Apple et Android sont utilisés dans la vie professionnelle et personnelle, tout comme les ordinateurs Windows et Mac. Les vulnérabilités présentes dans les systèmes d'exploitation de tels appareils et ordinateurs peuvent être exploitées de façon prospective pour accéder aux données stockées sur les appareils ciblés ou utilisées pour se déplacer latéralement dans les environnements informatiques en réseau à des fins de reconnaissance, d'espionnage ou d'attaque. Ces menaces sont accentuées dans un monde où les gens apportent régulièrement leurs appareils personnels au travail, ce qui soulève la possibilité que ces appareils puissent être compromis et donner accès à des environnements professionnels plus sécurisés.
3. De la même façon, les applications sur lesquelles nous comptons pour mener des activités commerciales ont tendance à être utilisées dans l'ensemble de l'économie. Les vulnérabilités des applications de service à la clientèle, comme les applications bancaires mobiles, touchent toutes les catégories d'entreprises, de ministères et de particuliers. De plus, des bibliothèques partagées, des interfaces de programme d'application (API) et des générateurs de nombres aléatoires sous-tendent bon nombre des programmes couramment utilisés. Les vulnérabilités telles que les bases de codes sont partagées entre toutes les applications qui incorporent ces éléments de code, mettant ainsi en danger des dizaines, des centaines voire des milliers d'applications et de systèmes. Ce partage d'utilisation des logiciels entre le secteur public et le secteur privé, et la vie professionnelle et privée, est de plus en plus fréquent avec la croissance des systèmes communs de messagerie, de base de données et de stockage, et deviendra de plus en plus courant au fil du temps.

4. En outre, tous les secteurs de l'économie dépendent de plus en plus des services infonuagiques de tiers pour le traitement, le stockage et l'analyse de données essentielles aux activités des entreprises et du gouvernement, ainsi qu'à la vie personnelle. Les serveurs qui alimentent ces infrastructures infonuagiques présentent régulièrement de graves vulnérabilités, que ce soit dans le code qui les alimente ou, sinon, en raison de l'isolement insuffisant des serveurs virtuels les uns des autres. Il en résulte que des vulnérabilités ou des erreurs dans la configuration des infrastructures infonuagiques permettent à des tiers d'accéder, de modifier ou d'exfiltrer de l'information de façon inappropriée.
5. En résumé, l'état d'insécurité informatique est grave. De nouvelles vulnérabilités sont découvertes (et corrigées) chaque jour. Chaque semaine, de nouvelles atteintes importantes à la sécurité des renseignements personnels sont signalées par les principaux organes de presse. De telles atteintes peuvent être utilisées soit pour faire de l'hameçonnage ciblé (obtenir un accès privilégié à l'information détenue par des cadres, employés ou autres personnes bien placés), soit pour faire du chantage (comme ceux qui ont fait l'objet de menaces après la divulgation des données d'Ashley Madison), soit pour mener d'autres activités malveillantes. Les vulnérabilités touchant la sécurité informatique dans son ensemble menacent le secteur financier et tous les autres secteurs de l'économie, avec la possibilité que les renseignements soient utilisés au détriment des intérêts du Canada en matière de sécurité nationale.

Politiques de chiffrement responsable

6. Compte tenu de l'état d'(in)sécurité informatique, il est impératif que le gouvernement du Canada adopte et préconise des politiques responsables de chiffrement. Ces politiques impliquent des engagements à préserver le droit de tous les groupes au Canada (gouvernement, entreprises privées et particuliers) d'utiliser des logiciels à l'aide d'un chiffrement fort. Un chiffrement fort peut largement être défini comme des algorithmes de chiffrement pour lesquels aucune faiblesse ou vulnérabilité n'est connue ou n'a été intégrée, ainsi que des applications informatiques qui ne contiennent pas délibérément des faiblesses visant à miner l'efficacité des algorithmes susmentionnés.
7. Certaines organisations canadiennes[1] ainsi que des organismes d'application de la loi de pays alliés[2] ont demandé que des portes dérobées soient installées ou que le chiffrement

[1] « RCMP's ability to police digital realm 'rapidly declining,' commissioner warned », https://www.cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340.
[2] « In the dark about 'going dark' », https://www.cyberscoop.com/fbi-going-dark-encryption-ari-schwartz-op-ed/.

soit autrement affaibli. Le fait de succomber à de telles demandes mettra fondamentalement en danger la sécurité de tous les utilisateurs des logiciels touchés[3] et, de façon plus générale, menacera la sécurité de toute transaction financière qui repose sur les applications, algorithmes de chiffrement ou bibliothèques de logiciels touchés.

8. Certains des plus proches alliés du Canada, comme l'Australie, ont adopté des politiques de chiffrement irresponsables qui risquent d'introduire des vulnérabilités systémiques dans les logiciels utilisés par le secteur financier, ainsi que par d'autres éléments de l'économie et fonctions gouvernementales[4]. Une fois introduites, ces vulnérabilités pourraient être exploitées par les services de renseignement de l'Australie et les organismes d'application de la loi dans le cadre de leurs activités, mais également par des acteurs qui ont des intérêts contre le Canada ou l'économie canadienne. Par exemple, le réseau SWIFT pourrait être la cible d'activités de menaces[5].
9. Il est important de noter que même les plus proches alliés du Canada surveillent les renseignements bancaires canadiens, souvent au-delà des mécanismes de surveillance convenus, comme le CANAFE. Par exemple, des renseignements rendus publics par le *Globe and Mail* ont révélé que la National Security Agency (NSA) des États-Unis surveillait les tunnels du réseau privé virtuel de la Banque Royale du Canada. L'article laisse entendre que les activités de la NSA pourraient constituer une étape préliminaire d'efforts plus vastes visant « à déterminer, à étudier et, au besoin, à "exploiter" les réseaux de communication internes des organisations »[6].
10. L'accès à une technologie de chiffrement fort et sans compromis est essentiel pour l'économie. Dans un environnement technologique marqué par des enjeux financiers élevés, une grande interdépendance et une complexité extraordinaire, il est extrêmement important et difficile d'assurer la sécurité numérique. Le chiffrement permet d'assurer la sécurité des opérations financières et de préserver la confiance du public dans le marché numérique. Les coûts liés à une atteinte à la sécurité, à un vol ou à la perte de données de clients ou d'entreprises peuvent avoir des répercussions dévastatrices sur les intérêts du secteur privé et les droits des particuliers. Toute faiblesse dans les systèmes mêmes qui

[3] Voir : « Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications », https://dspace.mit.edu/handle/1721.1/97690; « Shining A Light On The Encryption Debate: A Canadian Field Guide », https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/.
[4] « Civil Society Letter to Australian Government », 21 février 2019, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_Australia_Assistance_and_Access_Law_2018_Feb_21_2019.pdf; « Australia's Encryption Law Deals a Serious Blow to Privacy and Security », https://nationalinterest.org/feature/australia's-encryption-law-deals-serious-blow-privacy-and-security-39212.
[5] « That Insane, $81M Bangladesh Bank Heist? Here's What We Know », https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.
[6] « NSA trying to map Rogers, RBC communications traffic, leak shows », https://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/.

nous protègent contre ces menaces constituerait une politique irresponsable. L'accès à un chiffrement fort encourage les consommateurs à croire que la technologie qu'ils utilisent est sûre.

11. Compte tenu des menaces susmentionnées, je **recommande** que le gouvernement du Canada adopte une politique de chiffrement responsable. Une telle politique exigerait un engagement ferme et peut-être législatif afin d'exiger que tous les secteurs de l'économie aient accès à des produits de chiffrement forts et s'opposerait à des politiques de chiffrement irresponsables, comme celles qui préconisent les « portes dérobées ».

Programme d'équité en matière de vulnérabilités

12. Le gouvernement canadien dispose actuellement d'un processus en vertu duquel le Centre de la sécurité des télécommunications (CST) recueille les vulnérabilités informatiques et détermine s'il y a lieu de les conserver ou de les divulguer à des entreprises privées ou à des responsables de maintenance de logiciels en vue de les corriger. Le CST est motivé à conserver des vulnérabilités pour avoir accès à des systèmes étrangers dans le cadre de son mandat de renseignements électromagnétiques, ainsi qu'à divulguer certaines vulnérabilités afin de mieux protéger les systèmes gouvernementaux. À ce jour, le CST a refusé de rendre public le processus d'équité précis qu'il utilise pour déterminer s'il doit conserver ou divulguer ces vulnérabilités[7]. Il n'est toujours pas clair si d'autres organismes gouvernementaux ont leurs propres processus d'équité. La politique actuelle du gouvernement canadien contraste avec celle des États-Unis, où la Maison-Blanche a publié la façon dont tous les organismes du gouvernement fédéral doivent évaluer l'existence d'une vulnérabilité, la retenir ou la divulguer[8].
13. Lorsque des organismes comme le CST gardent secrètes les vulnérabilités découvertes afin de les utiliser plus tard contre des cibles précises, les vulnérabilités non corrigées laissent les systèmes essentiels ouverts à l'exploitation par d'autres acteurs malveillants qui les découvrent. Les réserves de vulnérabilités conservées par nos organismes peuvent être découvertes et utilisées par des adversaires. Les vulnérabilités de la NSA et de la Central Intelligence Agency (CIA) ont fait l'objet

[7] « When do Canadian spies disclose the software flaws they find? There's a policy, but few details », https://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007.
[8] « Vulnerabilities Equities Policy and Process for the United States Government », 15 novembre 2017, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

de fuites au cours des dernières années[9], l'une des vulnérabilités de la NSA ayant été utilisée par des acteurs malveillants pour causer des dommages commerciaux d'au moins 10 milliards de dollars[10].

14. À l'heure actuelle, il n'est pas clair quelles considérations guident le processus décisionnel des organismes de renseignement du Canada lorsque vient le temps de décider s'il faut conserver une vulnérabilité découverte pour utilisation future ou la divulguer afin qu'elle soit corrigée. Rien n'indique non plus que des entités susceptibles d'être touchées, comme des entreprises privées ou des organisations de la société civile, participent au processus décisionnel.
15. Afin de rassurer les entreprises canadiennes et prouver que les agences de renseignement et de sécurité canadiennes ne conservent pas de vulnérabilités qui pourraient être exploitées par des acteurs non gouvernementaux afin de mettre en danger le secteur financier du Canada, je **recommanderais** que le gouvernement du Canada diffuse son ou ses programmes actuels d'équité en matière de vulnérabilités et tienne des consultations sur l'efficacité de ceux-ci à protéger les logiciels et équipements canadiens utilisés dans le cadre d'activités financières, parmi d'autres activités économiques.
16. De plus, je **recommanderais** que le gouvernement du Canada inclue des intervenants du milieu des affaires et de la société civile dans le programme (actuel ou mis à jour) d'équité en matière de vulnérabilités. Ces intervenants seraient en mesure de déterminer les risques liés à la conservation de certaines vulnérabilités pour l'économie canadienne, comme faciliter de manière prospective l'utilisation de rançongiciels, la suppression ou la modification de données, le vol d'identité à des fins commerciales ou d'espionnage, ou l'accès aux données et l'exfiltration de ces dernières à l'avantage d'autres États-nations.

Programmes de divulgation des vulnérabilités

17. Les chercheurs en sécurité découvrent régulièrement des vulnérabilités dans les systèmes et les logiciels utilisés dans tous les milieux, y compris dans le secteur financier. Ces vulnérabilités peuvent, dans certains cas, être utilisées de façon inappropriée pour accéder à des données, modifier et exfiltrer ces dernières ou

[9] « Who Are the Shadow Brokers? », https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/; « WikiLeaks Starts Releasing Source Code For Alleged CIA Spying Tools », https://motherboard.vice.com/en_us/article/qv3xxm/wikileaks-vault-7-vault-8-cia-source-code.
[10] « The Untold Story of NotPetya, the Most Devastating Cyberattack in History », https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

manipuler autrement des systèmes informatiques d'une manière qui nuit aux parties qui contrôlent les systèmes et les renseignements informatiques connexes. Toutefois, relativement peu d'organisations ont des procédures explicites qui guident les chercheurs dans la façon de divulguer de façon responsable ces vulnérabilités aux entreprises touchées. La divulgation des vulnérabilités en l'absence d'un programme de divulgation peut amener les entreprises à menacer les chercheurs éthiques en sécurité informatique d'intenter indûment des poursuites contre eux. Ces risques réduisent la volonté des chercheurs de divulguer les vulnérabilités sans programme de divulgation des vulnérabilités[11].

18. La divulgation responsable des vulnérabilités comporte habituellement les éléments suivants. Premièrement, les entreprises indiquent clairement à qui les vulnérabilités peuvent être signalées, garantissent aux chercheurs qu'ils ne seront pas légalement menacés en divulguant les vulnérabilités et expliquent la période approximative qu'une entreprise prendra pour corriger la vulnérabilité signalée. Deuxièmement, les chercheurs s'engagent à ne pas divulguer publiquement la vulnérabilité avant qu'une certaine période (p. ex., de 30 à 90 jours) se soit écoulée depuis le signalement, ou jusqu'à ce que la vulnérabilité soit corrigée, selon la première éventualité. La délimitation d'une période avant que la vulnérabilité soit divulguée publiquement vise à encourager les entreprises à corriger rapidement les vulnérabilités signalées, plutôt que d'attendre trop longtemps avant de le faire.
19. Je **recommanderais** tout d'abord que le gouvernement du Canada s'engage à établir une ébauche de politique que les entreprises du secteur financier, ainsi que les entreprises d'autres secteurs, pourraient adopter et qui établirait les conditions selon lesquelles les chercheurs en sécurité informatique pourraient signaler les vulnérabilités aux entreprises du secteur financier. Une telle politique de divulgation devrait déterminer les personnes à qui les vulnérabilités sont signalées, la manière dont les rapports sont traités à l'interne, le temps qu'il faudra pour corriger une vulnérabilité et la manière dont les chercheurs en sécurité ne peuvent être tenus responsables tant qu'ils ne divulguent pas publiquement la vulnérabilité avant la fin de la période établie.
20. Je **recommanderais** également que le gouvernement du Canada rende obligatoire l'adoption de programmes de divulgation des vulnérabilités pour ses propres ministères, étant donné que ces derniers pourraient être ciblés par des adversaires dont le but serait de s'avantager financièrement au détriment du Canada. De telles politiques ont été

[11] « Vulnerability Disclosure Policies (VDP): Guidance for Financial Services », https://www.hackerone.com/sites/default/files/2018-07/VDP%20for%20Financial%20Services_Guide%20%281%29.pdf.

adoptées par le département de la Défense des États-Unis[12] et analysées par le département d'État[13], ce qui a eu pour effet le signalement et la correction de centaines de vulnérabilités. Le fait d'encourager les gens à signaler les vulnérabilités au gouvernement du Canada réduit la probabilité que les infrastructures du gouvernement soient exploitées avec succès au détriment des intérêts nationaux du Canada.

21. Enfin, je **recommanderais** que nos lois concernant l'accès non autorisé soient étudiées dans le but de déterminer si celles-ci sont trop générales en ce qui a trait à leur effet dissuasif et à leur incidence sur les chercheurs légitimes en sécurité.

Processus d'authentification à deux facteurs

22. Les paires de nom d'utilisateur et de mot de passe sont couramment exfiltrées des bases de données des entreprises privées. Étant donné que de nombreuses personnes utilisent la même paire dans plusieurs services (p. ex., pour des comptes de médias sociaux et des comptes professionnels) et que de nombreux mots de passe sont trivialement devinés, il est impératif que les comptes en ligne des entreprises privées intègrent l'authentification à deux facteurs. Ce type d'authentification désigne une situation dans laquelle une personne doit être en possession d'au moins deux « facteurs » pour obtenir l'accès à son compte. Les « facteurs » les plus généralement utilisés pour l'authentification comprennent quelque chose que vous connaissez (p. ex., un NIP ou un mot de passe), quelque chose que vous avez (p. ex., un jeton matériel ou un générateur de jeton aléatoire) ou quelque chose que vous êtes (de la biométrie, p. ex., le balayage d'une empreinte digitale ou de l'iris)[14].
23. Bien que de nombreuses entreprises du secteur financier utilisent l'authentification à deux facteurs avant que les employés puissent avoir accès à leurs systèmes professionnels, cette réalité est beaucoup moins présente dans les systèmes d'ouverture de session destinés aux clients. Il est important que ces derniers systèmes intègrent un solide processus d'authentification à deux facteurs afin d'empêcher des tiers non autorisés d'accéder à des comptes financiers personnels. Un tel accès peut mener à une meilleure analyse pour savoir si des personnes pourraient être ciblées par un adversaire

[12] « The Department of Defense wants more people to 'hack the Pentagon' — and is willing to pay them too », https://www.businessinsider.com/department-defense-wants-people-hack-pentagon-2018-10; « DoD Vulnerability Disclosure Policy », https://hackerone.com/deptofdefense.
[13] « House panel approves bill to 'hack' the State Department », https://thehill.com/policy/cybersecurity/386897-house-panel-approves-bill-to-hack-the-state-department.
[14] Blogue Savoir Techno du Commissariat à la protection de la vie privée du Canada : Votre identité –Moyens dont disposent les services pour une solide authentification, https://www.priv.gc.ca/fr/blogue/20170105/.

étranger à des fins de recrutement d'espionnage, causer des situations financières personnelles chaotiques (p. ex., transférer de l'argent à un tiers, annuler des paiements automatisés de factures, etc.) afin de distraire une personne pendant qu'une autre activité informatique est entreprise (p. ex., distraire un administrateur de systèmes avec des activités financières personnelles pendant une tentative d'infiltration dans des systèmes importants ou dans des comptes gérés par l'administrateur en question), ou transférer de l'argent à des parties inscrites à des listes de surveillance de terroristes.

24. Certaines institutions financières canadiennes offrent l'authentification à deux facteurs, mais le processus d'authentification généralement utilisé par défaut est faible. Cette situation est problématique, car les messages textes sont un médium de communication faible qui peut facilement être contourné par divers moyens[15]. C'est pourquoi des entités comme le National Institute of Standards and Technology des États-Unis ne recommandent plus les messages textes dans le cadre de l'authentification à deux facteurs[16].
25. Pour améliorer la sécurité des comptes destinés à la clientèle, je **recommande** que les institutions financières soient tenues d'offrir l'authentification à deux facteurs à tous les clients et, en outre, qu'un tel processus d'authentification utilise des jetons matériels ou logiciels (p. ex., des générateurs de mots de passe uniques ou de jetons aléatoires). La mise en œuvre de cette recommandation réduira le risque que des parties non autorisées obtiennent l'accès à des comptes à des fins d'activités de recrutement ou de perturbation.

L'organisation

26. Les opinions que j'ai présentées sont les miennes et sont fondées sur des recherches que mes collègues et moi avons effectuées à mon lieu de travail, le Citizen Lab. Le Citizen Lab est un laboratoire interdisciplinaire de la Munk School of Global Affairs and Public Policy, à l'Université de Toronto, qui se concentre sur la recherche, le développement et l'engagement stratégique et juridique de haut niveau à l'intersection des technologies de l'information et de la communication, des droits de la personne et de la sécurité mondiale.

[15] « Cybercriminals intercept codes used for banking to empty your accounts », https://www.kaspersky.com/blog/ss7-hacked/25529/; « AT&T gets sued over two-factor security flaws and $23M cryptocurrency theft », https://www.fastcompany.com/90219499/att-gets-sued-over-two-factor-security-flaws-and-23m-cryptocurrency-theft.
[16] « Standards body warned SMS 2FA is insecure and nobody listened », https://www.theregister.co.uk/2016/12/06/2fa_missed_warning/.

27. Nous utilisons une approche de « méthodes mixtes » pour la recherche qui combine les méthodes découlant des études en sciences politiques, en droit, en informatique et territoriales. Nos recherches portent notamment sur l'enquête de l'espionnage numérique contre la société civile, la documentation des filtres Internet et d'autres technologies et pratiques qui ont une incidence sur la liberté d'expression en ligne, l'analyse de la protection de la vie privée, de la sécurité et des contrôles de l'information des applications populaires, ainsi que l'examen des mécanismes de transparence et de responsabilisation pertinents à la relation entre les sociétés et les organismes gouvernementaux concernant les données personnelles et d'autres activités de surveillance.