CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

LA CYBERDÉFENSE DU CANADA

Rapport du Comité permanent de la défense nationale

L'honorable John McKay, président

JUIN 2023
44e LÉGISLATURE, 1re SESSION

LA CYBERDÉFENSE DU CANADA

Rapport du Comité permanent de la défense nationale

Le président
L'hon. John McKay

JUIN 2023

44e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DÉFENSE NATIONALE

PRÉSIDENT

L’hon. John McKay

VICE-PRÉSIDENTS

James Bezan

Christine Normandin

MEMBRES

Darren Fisher

Cheryl Gallant

Pat Kelly

Shelby Kramp-Neuman

Emmanuella Lambropoulos

Lindsay Mathyssen

Bryan May

Jennifer O’Connell

Charles Sousa

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Jenica Atwin

Taylor Bachrach

Alexandre Boulerice

Blaine Calkins

Luc Desilets

Andy Fillmore

Jean-Denis Garon

Mark Gerretsen

Yves Perron

Karen Vecchio

GREFFIER DU COMITÉ

Andrew Wilson

BIBLIOTHÈQUE DU PARLEMENT

Services d'information, d'éducation et de recherche parlementaires

Martin Auger

Katherine Simonds

LE COMITÉ PERMANENT DE LA DÉFENSE NATIONALE

a l'honneur de présenter son

CINQUIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(2) du Règlement, le Comité a étudié la cybersécurité et la cyberguerre et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1

Que le gouvernement du Canada mette en place une plateforme multilatérale permanente pour susciter la collaboration et l'engagement des divers intervenants en matière de cybersécurité. La plateforme devrait avoir des objectifs fondés sur ceux du programme Industry 100 du Royaume Uni. Elle devrait aussi former un espace collaboratif dans lequel les responsables de l'industrie et de la cybersécurité pourront se réunir pour échanger des informations et des pratiques exemplaires et établir des moyens de signaler les cyberattaques commises contre le secteur privé en vue d'améliorer le partage d'informations et de prévenir d'autres attaques. 58

Recommandation 2

Que le gouvernement du Canada investisse dans la cybersécurité de sa propre infrastructure réseau et évalue de façon exhaustive les mesures supplémentaires nécessaires pour renforcer les systèmes du gouvernement et l'infrastructure réseau des tierces parties qui hébergent ses données, afin d'assurer la sécurité de ses données critiques. 58

Recommandation 3

Que le gouvernement du Canada collabore avec ses partenaires du Groupe des cinq pour adopter une norme CMMC (Cybersecurity Maturity Model Certification) compatible avec celles de ses partenaires et reconnue par ces derniers afin d'éviter que l'utilisation d'une norme distincte au Canada ne défavorise les entreprises de l'industrie de défense canadienne par rapport à celles des autres pays membres du Groupe des cinq. 59

LA CYBERDÉFENSE DU CANADA

INTRODUCTION

De nos jours, Internet et les appareils électroniques comme les ordinateurs et les téléphones intelligents font partie du quotidien, et les infrastructures et les systèmes dont dépendent chaque jour les Canadiens et les gens d'autres pays sont de plus en plus connectés entre eux. On se sert couramment d'Internet pour faire toutes sortes d'activités : les achats, les opérations bancaires, les recherches, le divertissement, les communications avec la famille et les amis, les rencontres, les interactions sur les réseaux sociaux, les rendez-vous avec le médecin, l'éducation, la formation et le travail. Chez plusieurs d'entre nous, cette habitude s'est développée au début de la pandémie de COVID-19 et s'est maintenue même après que nos vies ont repris leur cours normal. Il est désormais relativement fréquent de voir des gens mener des activités parfois en personne, parfois à distance. L'ère numérique a radicalement transformé le fonctionnement de nos sociétés, y compris la manière dont nous travaillons, dont nous faisons des affaires et dont nous interagissons les uns avec les autres.

Or, le nombre et la complexité des cybermenaces augmentent au même rythme que le temps que les gens passent sur Internet et que la quantité de données personnelles, commerciales et financières qui sont accessibles en ligne. Plusieurs acteurs étatiques et non étatiques dans le monde profitent de la vulnérabilité et de la dépendance croissantes des sociétés modernes à des systèmes et des technologies numériques complexes et connectés entre eux pour se livrer à des activités malveillantes en ligne, comme la criminalité, l'espionnage ou le sabotage. De plus, des États autoritaires belliqueux comme la Chine et la Russie exploitent les failles des technologies et des réseaux numériques pour mener des campagnes de désinformation, des activités d'influence étrangère et d'autres formes de guerre cognitive dans le but de manipuler et diviser l'opinion publique et de miner la confiance et la cohésion dans les pays démocratiques.

La cybersécurité relève des secteurs public et privé et intègre des éléments de la sécurité nationale, de la politique extérieure, de technologies, de la gouvernance et des finances. Divers acteurs étatiques et non étatiques qui sont animés par des motifs variés emploient une gamme d'outils pour perpétrer des cyberattaques — par exemple des attaques par rançongiciel, des attaques contre des infrastructures essentielles ou la perturbation de réseaux. En outre, comme les cyberattaques sont difficiles à déceler et à attribuer et qu'il est relativement facile pour leur auteur d'en nier la responsabilité, un doute s'est installé sur la bonne manière de s'y opposer.

Qui plus est, ces dernières années, le cyberespace est devenu un nouveau théâtre de guerre, de rivalité et d'affrontement au sein de pays et entre pays. À plus grande échelle encore, des acteurs parrainés par des États profitent des ambiguïtés juridiques, techniques et politiques sur la conduite dans le cyberespace pour réaliser leurs objectifs politiques et militaires. Dans le monde entier, des armées rehaussent leur présence dans le cyberespace et investissent dans l'acquisition de cybercapacités sophistiquées pour protéger leurs systèmes et leurs réseaux contre les cyberattaques et pour mener des cyberopérations offensives contre d'éventuels adversaires. La façon dont la Russie a utilisé ses cyberarmes pour faire la guerre à l'Ukraine montre à quel point la cyberguerre et la militarisation du cyberespace ont été intégrées à la guerre moderne. Un autre changement digne de mention est le perfectionnement des campagnes de désinformation et des autres campagnes d'influence étrangère menées par des États autoritaires belliqueux comme la Chine et la Russie contre des pays démocratiques comme le Canada. Ces activités montrent toute l'importance d'agir pour assurer la cybersécurité et faire échec à la cyberguerre.

Tout comme d'autres pays, le Canada a créé des stratégies nationales, a mis sur pied et financé des initiatives de cybersécurité, a adopté des lois et a stimulé la coopération internationale dans le cyberespace, mais il peut encore renforcer sa cybersécurité, accroître ses efforts en matière de cyberguerre, et améliorer la résilience de ses institutions, de ses entreprises et de sa population par rapport aux cybermenaces venant de l'intérieur et à celles venant de l'étranger.

C'est dans ce contexte que, le 6 octobre 2022, le Comité permanent de la défense nationale de la Chambre des communes (le Comité) a adopté une motion visant la tenue d'une étude sur la cybersécurité et la cyberguerre. Selon cette motion, le Comité devait étudier « la sophistication évolutive des menaces associées à la cyber sécurité et les capacités des acteurs étrangers à pirater, perturber et démanteler les moyens de communication, les réseaux électriques, les bases de données et d'autres infrastructures essentielles », ce qui devait inclure « l'ensemble des capacités des pays avancés à mener une cyberguerre », « la menace que représentent les acteurs non étatiques pour notre cyber sécurité »; ce que le Canada et ses alliés font pour « défendre le Canada contre les cyber menaces étrangères », et « le rôle des particuliers et du secteur privé dans la cyber sécurité ».

Aux fins de cette étude, le Comité a tenu cinq réunions du 7 février au 31 mars 2023, auxquelles ont comparu 17 témoins comprenant des représentants du gouvernement du Canada, des officiers militaires, des universitaires et d'autres parties intéressées. Le Comité a également reçu des mémoires de la part de personnes qui n'ont pas comparu devant lui.

Le présent rapport contient un résumé des observations présentées au Comité en personne ou par écrit, ainsi que d'autres informations pertinentes du domaine public. La première partie présente une analyse du contexte des cybermenaces. La deuxième partie porte sur les organes du gouvernement fédéral qui contribuent à la cybersécurité et sur les rôles et responsabilités de trois de ces organes : le Centre de la sécurité des télécommunications (CST), le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). La troisième partie décrit certaines difficultés que les organismes du gouvernement du Canada doivent surmonter en matière de cybersécurité ainsi que les domaines où des améliorations pourraient être apportées. La quatrième et dernière partie porte sur les éléments de la cybersécurité qui relèvent de l'ensemble de la société et sur les moyens possibles d'améliorer la cyberrésilience du Canada, plus particulièrement en ce qui concerne la protection des infrastructures essentielles; la coopération entre les secteurs public et privé; la recherche et le développement; les activités d'éducation, de sensibilisation et de formation à l'intention du public; et la protection du droit à la vie privée des particuliers et des libertés civiles. Pour terminer, le rapport présente les réflexions et les recommandations du Comité.

LE CONTEXTE DES CYBERMENACES

Au Canada et dans le reste du monde, les réseaux informatiques sont de plus en plus connectés entre eux, à l'intérieur comme au-delà des frontières, ce qui s'explique en partie par le nombre croissant de services essentiels qui dépendent des systèmes numériques. Cette interconnexion n'est pas sans danger. La facilité d'accès à Internet et la dépendance croissante aux technologies créent toutes sortes d'occasions — pour les cybercriminels, les pirates informatiques, les terroristes et les auteurs de menace parrainés par un État — de perpétrer des cyberattaques qui menacent nos activités quotidiennes. À cela s'ajoute une autre menace maintenant bien établie pour la sécurité nationale : celle des gouvernements autoritaires belliqueux qui font usage du cyberespace pour y mener des campagnes de désinformation, des opérations d'influence étrangère et d'autres formes de guerre cognitive contre le Canada et ses alliés. Les cybermenaces sont maintenant notre réalité quotidienne et, puisqu'elles évoluent constamment et rapidement, il est nécessaire d'accorder une attention soutenue à la cybersécurité pour s'en protéger.

C'est dans ce contexte que des témoins ont parlé au Comité des cybermenaces qui pèsent sur le Canada et ses alliés, de la cyberguerre, de la guerre cognitive et des nouvelles technologies liées à la cybersécurité.

Cybermenaces

Les cybermenaces sont de plus en plus nombreuses et sophistiquées. Le Centre canadien pour la cybersécurité définit une cybermenace comme « une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient, ou à perturber le monde numérique en général[1] ».

Pour communiquer au Comité l'urgence du problème que les cybermenaces représentent pour la sécurité du Canada, des témoins ont parlé de la nature de ces menaces et de la fréquence des attaques qui se produisent au pays. Selon Alexander Rudolph, doctorant au département de science politique de l'Université Carleton, la « cybermenace peut être décrite comme étant un état de conflit et de tension perpétuel ». En mars 2022, au cours de l'étude du Comité sur la défense du Canada dans un contexte de menace en évolution[2], Cherie Henderson, directrice adjointe, Exigences au Service canadien du renseignement de sécurité, a indiqué qu'à sa connaissance, « le Canada subit quotidiennement des milliers de cyberattaques dans tout le pays, et de nombreuses organisations font l'objet de ces attaques ».

Des acteurs étatiques et non étatiques ont utilisé des cyberprogrammes offensifs pour s'en prendre au secteur financier, aux infrastructures essentielles et aux institutions démocratiques du Canada. Sami Khoury, dirigeant principal du Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications, a affirmé que « la cybercriminalité demeure la plus grande activité de cybermenace visant la population canadienne », mais que « les cyberprogrammes parrainés par les États chinois, russe, iranien et nord-coréen [représentent] la plus grande cybermenace stratégique pour le Canada ». Il a aussi fait remarquer que les cybercriminels et les auteurs de menace parrainés par un État s'en prennent surtout aux infrastructures essentielles, et que les rançongiciels représentent une menace grave et persistante pour les organisations canadiennes. Alia Tayyeb, chef adjointe des renseignements électromagnétiques du CST, a abondé dans le même sens, en ajoutant que « la gravité des cybercrimes et des cyberincidents qui ciblent les Canadiens et les infrastructures essentielles du pays connaissent une croissance exponentielle ».

1 Voir Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications (CST), *Introduction à l'environnement de cybermenace 2023–2024*, 2022, p. 2.

2 Comité permanent de la défense nationale de la Chambre des communes (NDDN), *Rapport provisoire sur la défense du Canada dans un contexte de menace en évolution*, 44e législature, 1re session, juin 2022.

Des témoins ont attiré l'attention du Comité sur la hausse du nombre d'attaques par rançongiciels et par autres types de maliciels[3]. Alexander Rudolph a affirmé que « les rançongiciels ont complètement révolutionné la façon dont les États adverses et les acteurs non étatiques » commettent leurs cyberattaques, en précisant que la Russie, la Corée du Nord et d'autres acteurs étatiques s'en servent couramment dans le cadre de leurs cyberopérations, et que la Corée du Nord « a très bien réussi » à exploiter des rançongiciels pour dérober des renseignements à des particuliers, des institutions financières, des gouvernements et des entreprises du monde entier. M. John de Boer, directeur principal, Affaires gouvernementales et politiques publiques chez BlackBerry, a indiqué qu'au cours des 90 jours précédents, BlackBerry, qui protège plus de 500 millions de systèmes dans le monde entier, avait « intercepté plus de 1,5 million de cyberattaques par logiciels malveillants, dont 200 000 étaient de nouveaux échantillons, avant leur exécution ». Il a ajouté qu'« on dénombre plus de 400 000 nouveaux types de logiciels malveillants par jour ».

M. de Boer a aussi affirmé que les soins de santé, la finance et la fabrication ont été les trois secteurs les plus ciblés au cours des 12 derniers mois, en précisant que la fabrication est le secteur le plus souvent visé, peut-être à cause des « vulnérabilités de la chaîne d'approvisionnement » et du « lien intrinsèque entre la sécurité économique et la sécurité nationale ». Selon lui, durant la dernière année, le nombre de cyberattaques dans le secteur manufacturier a augmenté de 2 000 %. Tadej Nared, président du conseil d'administration de l'organisme Slovenian Certified Ethical Hackers Foundation, a indiqué que la cybercriminalité est devenue « la troisième économie mondiale » et que, « [d'ici] 2025, les dégâts causés par la cybercriminalité s'élèveront à 15 billions de dollars », en ajoutant que ces dégâts « augmentent de 1 500 milliards de dollars par an » et qu'il s'agit d'« un énorme problème ».

Le brigadier-général à la retraite John Turnbull a observé que « la cybercriminalité, qu'elle soit perpétrée par des individus, par le crime organisé ou par des entités parrainées ou soutenues par l'État, peut représenter une menace réelle pour la sécurité nationale ». À son avis, « le résultat d'une cyberattaque remet en cause l'efficacité de tous les ordres de gouvernement, plombe l'économie et finit par miner la confiance [du

3 Selon le Centre canadien pour la cybersécurité, le mot « maliciel » est l'abréviation des mots « malveillant » et « logiciel » et « désigne tout logiciel ou code conçu pour infiltrer ou endommager un système informatique »; tandis que le mot « rançongiciel » désigne « un programme malveillant qui permet de bloquer l'accès à un ordinateur ou à un dispositif et à son fonctionnement; l'accès au système n'est rendu qu'après le versement d'une rançon ». Le Centre affirme que les auteurs de menace utilisent souvent le chiffrement, mais peuvent aussi « avoir recours à diverses méthodes d'extorsion ». Voir Centre canadien pour la cybersécurité, CST, *Introduction à l'environnement de cybermenace 2023–2024*, 2022, p. 13–14.

public] en la capacité des institutions nationales à protéger la population[4] ». Alia Tayyeb a mentionné que « des États et des cyberacteurs parrainés par des États [constituent aussi] une menace constante pour le Canada ». Sami Khoury a souligné que la Chine, la Russie, la Corée du Nord et l'Iran « ont diverses raisons de s'en prendre au Canada ». Par exemple, il a mentionné que la Chine utilise ses cyberoutils pour s'attaquer « à la recherche, aux données techniques, à la propriété intellectuelle des entreprises et aux capacités militaires », tandis que la Corée du Nord « cherche à accroître sa valeur économique en volant des données d'authentification, ainsi que des fonds ».

Aaron Shull, directeur général et avocat général du Centre for International Governance Innovation, a affirmé que les cyberattaques sont « souvent menées par des acteurs étatiques qui visent à voler des renseignements sensibles ou à perturber des infrastructures essentielles sur une longue période ». À titre d'exemple, il a expliqué que des acteurs parrainés par des États autoritaires comme la Chine et la Russie utilisent des rançongiciels pour faire de l'extorsion et perturber des chaînes d'approvisionnement et des infrastructures essentielles partout dans le monde. Il a ajouté que ces acteurs se servent de moyens cybernétiques pour s'ingérer dans des élections démocratiques, diffuser de la désinformation et manipuler les médias sociaux, le tout dans le but d'influencer et de diviser l'opinion publique dans d'autres pays.

Selon Alex Rapin, chercheur en résidence et titulaire de la Chaire Raoul-Dandurand en études stratégiques et diplomatiques à l'Université du Québec à Montréal, on a consigné dans une base de données publique 93 cyberincidents géopolitiques qui ont visé le Canada depuis 2010 — dont 14 ont eu lieu en 2022 –, y compris des activités d'espionnage économique menées contre des entreprises et des universités canadiennes, de surveillance électronique clandestine d'activistes et d'organisations non gouvernementales basées au Canada, et de collecte de renseignements visant des organisations gouvernementales canadiennes. À son avis, « la très grande majorité de ces incidents proviennent de quatre pays seulement : la Chine, la Russie, l'Iran et la Corée du Nord ». À propos des tendances actuelles relativement aux cybermenaces, M. Rapin a parlé de « la menace grandissante des cyberattaques par rançongiciels » utilisées contre des entités canadiennes pour faire la collecte clandestine de renseignements ou perturber des infrastructures essentielles, des « ciblages de plus en plus agressifs d'activistes, d'exilés et de dissidents basés au Canada […] à des fins d'espionnage, d'intimidation et de harcèlement », ainsi que de « la hausse du nombre de cybermercenaires, qui commencent à cibler des entités canadiennes, fort probablement à la demande de puissances étrangères ».

4 Document soumis au Comité NDDN par John Turnbull, brigadier-général à la retraite, le 13 février 2023.

Cyberguerre

Des témoins ont entretenu le Comité de la cyberguerre et du recours croissant à des moyens cybernétiques dans le cadre des opérations militaires. Jonathan Quinn, directeur général, Politique de défense continentale du ministère de la Défense nationale, a affirmé que « [l]e cyberespace est devenu un autre domaine d'opérations militaires et de sécurité nationale, qui se caractérise par une concurrence constante en deçà du seuil qui attire tant les alliés que les adversaires ». D'après Alexander Rudolph, « la cyberdéfense et la cyberguerre sont très ciblées sur les différentes menaces [pour la défense nationale] et font intervenir dans la plupart des cas des États, plutôt que des acteurs non étatiques ».

Des témoins ont cité la guerre en Ukraine comme un exemple de cyberguerre. Selon Jonathan Quinn, « [le] conflit en Ukraine montre que les cybercapacités jouent un rôle essentiel dans la guerre moderne ». Alexander Rudolph a évoqué le recours de la Russie aux « cyberopérations associées à des opérations militaires cinétiques interarmées quasi simultanées » en Ukraine au cours de la dernière année. Sami Khoury a exprimé un point de vue similaire, affirmant que les cyberattaques russes dirigées contre l'Ukraine sont la preuve que la Russie est « un cyberacteur redoutable ». Il a précisé que les Russes ont employé des cyberoutils comme des armes et qu'ils ont mené plusieurs fois des cyberattaques parallèlement à des attaques militaires cinétiques contre des cibles en Ukraine.

M. Wesley Wark, agrégé supérieur au Centre for International Governance Innovation, a remarqué que la guerre en Ukraine a servi de terrain d'essai pour la cyberguerre et « nous offre d'importantes indications bien concrètes quant à la manière dont les cyberarmes peuvent et vont dorénavant être utilisées en temps de guerre, de concert avec des attaques militaires plus conventionnelles ». Il a soutenu que le Canada et ses alliés doivent « prêter attention » à la façon dont les armées russe et ukrainienne ont mené leurs cyberopérations et ont fait de leur conflit « un laboratoire pour la cyberguerre », car il s'agit de la toute première guerre au cours de laquelle des méthodes de cyberguerre ont été employées dans une large mesure. À son avis, « [il est] très important que nous étudiions tout ce qui a été utilisé par la Russie contre l'Ukraine, et la façon dont l'Ukraine a répondu ». Il a aussi indiqué que nous pouvons retenir trois choses de la cyberguerre que la Russie fait à l'Ukraine : « Premièrement, les civils sont une cible de choix. Deuxièmement, les cyberarmes ne sont pas des munitions de précision. Troisièmement, les cyberagressions ne connaissent ni règles ni limites. »

Qui plus est, M. Wark a fait remarquer que les cyberopérations russes menées contre l'Ukraine sont devenues « plus sophistiquées et étendues » depuis février 2022 et

qu'elles témoignent de la volonté de la Russie d'attaquer les infrastructures énergétiques et d'autres infrastructures essentielles de l'Ukraine « pour détruire les sources civiles d'alimentation électrique et saper du même coup le moral des Ukrainiens ». Il a ajouté que « les Russes lançaient en novembre 2022 une moyenne de 10 cyberattaques par jour à l'encontre des infrastructures énergétiques essentielles de l'Ukraine ». Il a également soutenu que l'Ukraine avait « renforcé » ses capacités de cyberguerre avec l'aide « d'alliés importants de l'Ouest et de tous les partenaires du Groupe des cinq », et qu'elle avait su mener des contre-attaques efficaces. « Au-delà du théâtre ukrainien », M. Wark a affirmé que « les auteurs de cybermenaces parrainés par la Russie se livraient à de vastes campagnes de cyberespionnage visant les pays de l'OTAN » et que la Russie cherchait à « se donner de nouvelles cybercapacités pour s'attaquer à ces cibles, [notamment] au Canada ».

Guerre cognitive

Des témoins se sont penchés sur la menace de guerre cognitive[5], qui regroupe l'influence étrangère, l'espionnage et les campagnes de désinformation, de mésinformation et de malinformation[6]. Marcus Kolga, agrégé supérieur à l'Institut Macdonald-Laurier, a attiré l'attention du Comité sur « les opérations d'information dans un contexte de guerre cybernétique et les menaces qui en découlent pour notre environnement d'information et notre sécurité nationale ». Il a décrit la guerre cognitive comme « un outil extrêmement important dans la boîte à outils » de la Russie, de la Chine et d'autres États antagonistes, et a affirmé que « nous devons nous assurer que nous disposons des capacités nécessaires pour faire face à ces menaces et passer à l'offensive contre nos adversaires lorsqu'ils s'engagent dans ce type de guerre ». Il a aussi précisé que la désinformation est une menace pour la cybersécurité et que les adversaires du Canada l'utilisent souvent comme une forme de « communication

5 Dans un récent rapport d'étude, la « guerre cognitive » (*cognitive warfare* en anglais) est définie comme la « militarisation de l'opinion publique, par une entité externe, dans le but 1) d'influencer la politique publique et gouvernementale, et 2) de déstabiliser les institutions publiques ». Selon ce rapport, la guerre cognitive « ne se limite pas à exercer un contrôle sur la circulation de l'information; elle consiste aussi à conditionner la réaction des gens à l'information qu'ils reçoivent, pour que les ennemis s'entredéchirent de l'intérieur ». Voir Alonso Bernal et coll., *Cognitive Warfare: An Attack on Truth and Thought*, Organisation du Traité de l'Atlantique Nord et Université Johns Hopkins, 2020, p. 3 [TRADUCTION].

6 Le Centre canadien pour la cybersécurité définit la « désinformation » comme « le fait de diffuser intentionnellement une fausse information dans le but de manipuler ou de tromper des personnes, des organisations et des États ou bien de leur faire du tort », la « mésinformation » comme « le fait de diffuser intentionnellement une fausse information sans avoir de mauvaises intentions », et la « malinformation » comme « le fait de diffuser de l'information qui repose sur un fait, mais qui est souvent exagérée de façon à tromper ou même à causer des préjudices ». Voir Centre canadien pour la cybersécurité, CST, *Introduction à l'environnement de cybermenace 2023–2024*, 2022, p. 8.

numérique » à l'aide de différentes plateformes de médias sociaux, de site Web et de services de courrier électronique.

Des témoins ont mentionné que la Chine et la Russie ont employé des méthodes de guerre cognitive contre le Canada. Marcus Kolga a souligné qu'au cours de la dernière décennie, « la guerre de l'information est effectivement devenue l'un des outils de prédilection au sein de l'arsenal hybride et cybernétique de la Russie ». Il a aussi avancé que la Russie avait « directement ciblé » le Canada. D'après lui,

> [l]a guerre de l'information livrée par la Russie a d'abord et avant tout pour but de miner la confiance de la population envers nos démocraties et la cohésion de nos sociétés. On utilise comme armes à cette fin les enjeux et les discours les plus susceptibles de polariser les gens. On pousse à l'extrême des argumentaires exploitant les préjugés aussi bien conservateurs que libéraux en mettant de l'avant toutes les questions susceptibles de diviser les Canadiens.

À titre d'exemple, il a mentionné les campagnes de désinformation russes menées contre les Canadiens durant la pandémie de COVID-19 et contre les membres des Forces armées canadiennes déployés en Lettonie, en Ukraine et dans d'autres pays d'Europe dans le cadre des opérations REASSURANCE et UNIFIER depuis 2015.

Par ailleurs, Marcus Kolga a signalé que les opérations d'information du gouvernement chinois mettent « constamment en péril » la sécurité nationale et la défense du Canada; il a déclaré que « le Canada a souvent été la cible [d'opérations de désinformation chinoises] » au cours des dernières années et que la Chine « se dote de moyens de plus en plus sophistiqués » de faire la guerre cognitive, en précisant que « la Chine nous a pris pour cible et a tenté de miner notre démocratie au moyen de campagnes de désinformation au cours des trois dernières élections ». Il a aussi encouragé le gouvernement du Canada à surveiller la Chine « de très près » et l'a mis en garde contre un éventuel « rapprochement » entre la désinformation chinoise et la désinformation russe. Il a émis l'opinion que la Chine et la Russie « se soutiennent mutuellement » dans le domaine de la guerre cognitive.

De même, M. Wark a remarqué que la Chine et la Russie « sont de véritables experts » des campagnes de désinformation, de mésinformation et de malinformation. Il a indiqué que ces pays sont à créer de nouveaux moyens sophistiqués de répandre de fausses informations et d'influencer l'opinion publique au Canada et chez ses pays alliés, en ajoutant que le Canada doit demeurer vigilant et se tenir prêt à réagir à ce genre d'activités.

Aaron Shull a parlé du besoin de « résilience sociétale » par rapport à la menace de la guerre cognitive. Selon lui, « [q]u'il soit question de désinformation, de mésinformation

ou de malinformation, le fait est que les gens sont influençables. Des campagnes perfectionnées sont sans cesse menées pour essayer de changer notre discours, de semer la discorde au sein de la société et d'amener les gens dans des directions différentes alors même qu'il nous faut être unis. »

Technologies nouvelles

Des témoins ont attiré l'attention du Comité sur les cybermenaces que les technologies nouvelles font peser dans le cyberespace, en particulier l'intelligence artificielle (IA) et l'informatique quantique. Marcus Kolga a exprimé sa grande préoccupation à propos des « technologies futures […] du domaine de l'information ». Il a notamment fait remarquer que l'IA « évolue très rapidement » et que, grâce à cette technologie, « [la] vitesse à laquelle nos adversaires étrangers peuvent diffuser de l'information et de la désinformation va devenir très alarmante ». D'après lui, les « hypertrucages » — « de fausses vidéos, de fausses images et de faux enregistrements audio qui sont de plus en plus créés par l'intelligence artificielle » — sont une autre nouvelle technologie préoccupante « qui prend de l'ampleur et qui deviendra problématique dans les années à venir ». À titre d'exemple, il a expliqué que l'hypertrucage permet de prendre une image d'une personne — comme celle du président des États-Unis — et de faire croire que cette personne « dit quelque chose [qu'elle] ne dit pas en réalité ». M. Kolga a ajouté que « la technologie utilisée pour créer ces vidéos devient d'une précision terrifiante ». À son avis, le Canada n'est pas prêt à « faire face à l'émergence » de l'IA et des hypertrucages et à la menace croissante qui en provient.

M. Thomas Keenan, professeur à la School of Architecture Planning and Landscape de l'Université de Calgary, a aussi fait une mise en garde à propos de l'IA. Il croit que cette technologie « révolutionnera notre monde, notamment les domaines de la cybersécurité et de la cyberguerre, et ce beaucoup plus rapidement que l'on pourrait le croire ». Il a souligné que la société civile se sert déjà de l'IA dans de nombreux domaines, que celle-ci « peut détecter de minuscules tumeurs sur l'IRM comme elle peut aider les villes à optimiser leurs feux de circulation », et il a averti le Comité que « de nombreux secteurs, notamment celui de la défense, adoptent cette technologie sans pleinement comprendre la façon dont elle peut être utilisée contre nous ». Au sujet des inquiétudes suscitées par l'IA par rapport à la formation, à l'éthique et aux bases de données du domaine public utilisées par les forces armées, M. Keenan a soutenu qu'« il faut absolument avoir une politique en place » sur les limites de l'utilisation de l'IA dans l'armée et a avancé qu'il faudrait élaborer cette politique « en consultation avec l'industrie et les universitaires ».

Tim Callan, directeur de l'expérience client et directeur de la conformité chez Sectigo, s'est penché sur l'informatique quantique. Il a indiqué que, pour le moment, « une utilisation adéquate et complète de l'identité numérique est essentielle pour fournir des processus numériques sécurisés aux entreprises, aux gouvernements, aux infrastructures, au secteur de la finance, aux transports, aux soins de santé, à l'éducation et pour presque tous les autres aspects de la vie ». Selon lui, « [l]a sécurisation des identités numériques est assurée par l'infrastructure à clés publiques », une « méthode éprouvée d'échange de clés cryptographiques pour vérifier les systèmes connectés et crypter les données ». Il a affirmé que « les enjeux augmentent avec l'avènement des ordinateurs quantiques [qui] seront capables de vaincre facilement plus de 99 % des systèmes de cryptage du monde » dans quelques années, et que cela « rendra les données cryptées susceptibles d'être exposées par tout attaquant ayant accès à un ordinateur quantique ». Par conséquent, il a préconisé que le gouvernement du Canada et le secteur privé commencent à se préparer à cette menace, en ajoutant que « [n]ous devons agir dès aujourd'hui ».

Kristen Csenkey, doctorante à la Balsillie School of International Affairs de l'Université Wilfrid Laurier, a qualifié les technologies émergentes de l'IA et des ordinateurs quantiques de « perturbatrices » et a indiqué que « nous avons besoin d'une plus grande collaboration pour contrer les menaces associées à l'utilisation de ces technologies en particulier, tout en gardant à l'esprit que la technologie ne constitue pas la seule menace ». D'après elle, il existe une « possibilité que certains acteurs malhonnêtes utilisent certaines technologies d'une manière qui pourrait causer du tort ».

LE MILIEU DE LA CYBERSÉCURITÉ AU SEIN DU GOUVERNEMENT DU CANADA

Au Canada, la cybersécurité n'est pas la responsabilité d'un organisme unique : on la considère plutôt comme une activité à laquelle doivent contribuer la société en général et divers organismes des secteurs public et privé en particulier. Au gouvernement du Canada, le milieu de la cybersécurité compte au bas mot une douzaine de ministères et organismes, dont le CST, le MDN et les FAC. Chacun a des responsabilités distinctes en matière de cybersécurité, et chacun coopère avec les autres pour protéger le Canada contre les cybermenaces. À cela s'ajoutent la collaboration et le partage d'informations avec les gouvernements provinciaux et territoriaux, le secteur privé et des partenaires internationaux comme les membres du Groupe des cinq — l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis — et les 31 États membres de l'Organisation du Traité de l'Atlantique Nord (OTAN).

Des témoins ont entretenu le Comité des mesures de cybersécurité employées par le gouvernement du Canada pour protéger le pays contre les cybermenaces et la menace de guerre cognitive. Ils ont mentionné des mesures faisant intervenir tous les membres de la société; les principaux ministères et organismes fédéraux qui font partie de l'appareil de cybersécurité du gouvernement du Canada; les rôles et responsabilités du CST, du MDN et des FAC; ainsi que la coopération qui existe entre les organismes du portefeuille de la Défense nationale sur la question de la cybersécurité.

Contribution de la société

Des témoins ont indiqué que tout le monde a un rôle à jouer pour assurer la cybersécurité. Aaron Shull a affirmé que « la cybersécurité devrait être une préoccupation pour l'ensemble de la société canadienne ». Il a souligné que la cybersécurité est une affaire de gouvernance et a des répercussions tant sur le secteur public que sur le secteur privé. Il estime que, « [d]ans le contexte des tendances géopolitiques actuelles […] il est de notre devoir de mieux préparer le pays » au combat contre les cybermenaces et à la guerre cognitive.

Kristen Csenkey a décrit la cybersécurité comme un effort pansociétal « dynamique », en soulignant que la cybersécurité est « une notion complexe qui ne cesse de changer en faisant intervenir un grand nombre un grand nombre d'acteurs, de contextes et d'idées », de même qu'« une opération combinant des considérations sociales, politiques et techniques dans le cadre de laquelle ressources humaines et technologiques s'imbriquent ». En conséquence, dit-elle, « nous ne pouvons pas envisager les enjeux de cybersécurité en vase clos » et nous devons reconnaître que « [n]ous vivons dans un monde cybermatériel, en ce sens que de nombreux aspects de nos existences se déroulent dans des espaces numériques reliés à des composantes physiques ».

Lorsque Kristen Csenkey a mentionné le besoin d'un effort concerté pour assurer la cybersécurité, elle a mis l'accent sur une coordination et une coopération faisant intervenir le secteur privé, le secteur public et les pays alliés qui ont des vues similaires aux nôtres et qui possèdent les capacités techniques voulues. À son avis, si l'on veut protéger efficacement le Canada contre les cybermenaces et faire face au « caractère évolutif de ces menaces, et notamment du potentiel et des capacités technologiques des différents acteurs, » il faut accorder la priorité à la coordination et à la coopération « entre les divers acteurs ayant un rôle à jouer à l'égard des aspects politiques, sociaux et techniques dont la combinaison influe sur la cybersécurité ».

Appareil de la cybersécurité du gouvernement du Canada

En 2018, le gouvernement du Canada a publié la *Stratégie nationale de cybersécurité : Vision du Canada pour la sécurité et la prospérité dans l'ère numérique* (la Stratégie nationale de cybersécurité), qui a conduit à la création du Centre canadien pour la cybersécurité et du Centre national de coordination en cybercriminalité. Le plan d'action de la Stratégie nationale de cybersécurité se divise en trois volets : sécuriser les systèmes gouvernementaux; nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral; et aider les Canadiens à se protéger en ligne.

Comme nous l'avons mentionné plus haut, au moins 12 ministères et organismes fédéraux assument des responsabilités liées à la cybersécurité au Canada[7]. Jonathan Quinn a affirmé que « le cyberespace est compliqué », car « [o]n compte beaucoup de joueurs fédéraux dans ce domaine ». Il a cependant précisé que « [l]e premier rôle fédéral en matière de cybersécurité — assurer la sécurité des réseaux de l'État, prêter assistance aux détenteurs de réseaux d'infrastructures essentielles et ce genre de choses — appartient globalement à [Sécurité publique Canada] ».

En tant que responsable de la politique de cybersécurité du gouvernement du Canada et coordonnateur de la majorité des activités fédérales pour la cybersécurité, Sécurité publique Canada collabore avec les autres ministères et organismes fédéraux sur une grande variété de questions d'ordre politique et opérationnel. Quant au CST, il dirige le développement et la mise en œuvre des capacités pour la cybersécurité. Les autres ministères et organismes fédéraux suivants veillent aussi à la cybersécurité au Canada[8] :

- le Centre antifraude du Canada;
- le Conseil de la radiodiffusion et des télécommunications canadiennes;
- le Service canadien du renseignement de sécurité;
- Recherche et développement pour la défense Canada;
- le MDN et les FAC;
- Innovation, Sciences et Développement économique Canada;

7 Sécurité publique Canada, « Cybersécurité au gouvernement fédéral du Canada ».

8 *Ibid*.

- le Commissariat à la protection de la vie privée du Canada;
- la Gendarmerie royale du Canada;
- Services partagés Canada;
- le Secrétariat du Conseil du Trésor.

Parmi cette liste, les témoins ont parlé au Comité des activités menées par les principaux organismes du portefeuille de la Défense nationale — le CST, le MDN et les FAC — au chapitre de la cybersécurité, de façon indépendante et en coopération les uns avec les autres.

Centre de la sécurité des télécommunications

Lors des réunions du Comité, il a été question du CST, l'un des trois principaux ministères et organismes fédéraux qui assument des responsabilités liées à la cybersécurité. Sami Khoury et Alia Tayyeb ont décrit le CST comme l'organisme canadien responsable des opérations de renseignement électromagnétique étranger et des cyberopérations, ainsi que comme l'autorité technique du Canada en matière de cybersécurité. Dans le *Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques*, le Comité des parlementaires sur la sécurité nationale et le renseignement a affirmé que le CST « recueille des renseignements sur les menaces pour les systèmes et les réseaux du gouvernement, dirige un réseau de défense perfectionné et en couches de capteurs qui trouvent et bloquent ces menaces, et fournit des directives et des conseils aux organisations gouvernementales (et de plus en plus aux Canadiens et aux organisations du secteur privé) pour renforcer leur propre sécurité en matière de technologie de l'information ».

Le CST gère aussi le Centre canadien pour la cybersécurité, « la source unifiée de conseils, d'avis, de services et de soutien spécialisés en matière de cybersécurité » pour les ministères et organismes fédéraux, les provinces et territoires, les municipalités, les propriétaires d'infrastructures essentielles, les entreprises, les universitaires et le grand public au Canada. Jonathan Quinn a expliqué que le Centre canadien pour la cybersécurité est un organisme « qui relève du Centre de la sécurité des télécommunications, mais qui harmonise son travail avec la politique établie par Sécurité publique [Canada] ». Il a ajouté que le Centre a un rôle important à jouer « dans la diffusion des pratiques exemplaires, l'aide aux entreprises canadiennes et l'identification ainsi que l'atténuation des menaces ».

Sami Khoury a expliqué que, même si le CST défend les réseaux du gouvernement du Canada, alors que le Centre canadien pour la cybersécurité dirige la réaction du gouvernement aux cyberincidents, « [la] cybersécurité ne représente toutefois pas une responsabilité et une préoccupation seulement pour le gouvernement fédéral, puisque les cybermenaces continuent de cibler et de toucher des citoyens et des organisations du Canada ». Selon lui, le CST travaille avec des partenaires à l'intérieur et à l'extérieur de la fonction publique, y compris des partenaires du secteur privé, « pour échanger de l'information sur les menaces et les pratiques exemplaires en matière de cybersécurité ». Il a ajouté que le Centre canadien pour la cybersécurité « publie constamment des avis et des conseils d'experts à l'intention des Canadiennes et des Canadiens » et a attiré l'attention du Comité sur l'*Évaluation des cybermenaces nationales 2023–2024*, qui décrit les tendances actuelles touchant la population canadienne en matière de cybersécurité.

Alia Tayyeb a fait savoir qu'en août 2019, on a modifié la *Loi sur le Centre de la sécurité des télécommunications* pour que les « cyberopérations actives » (c'est-à-dire les cyberopérations offensives) soient ajoutées au mandat du CST se rapportant au renseignement étranger et à la cybersécurité. À son avis, ce changement a permis au CST « d'élargir son arsenal afin de mener des opérations actives et défensives, réunies sous le nom de cyberopérations étrangères ». La *Loi* définit les « cyberopérations actives » comme « des activités [menées] dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étranger, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités ». Les opérations du CST ne peuvent pas viser des Canadiens ou des personnes situées au Canada, et elles doivent être autorisées par le ministre fédéral compétent.

Qui plus est, Alia Tayyeb a déclaré que, « [d]epuis qu'on lui a accordé ces nouveaux pouvoirs [de mener des cyberopérations offensives], le CST a tiré parti de ses capacités liées aux cyberopérations pour nuire aux efforts extrémistes basés à l'étranger visant à recruter des Canadiens, à mener des opérations en ligne et à diffuser du contenu violent et extrémiste », ainsi que « pour perturber les activités de cybercriminels planifiant des attaques au moyen de rançongiciels ». Elle a toutefois tenu à préciser que « le CST n'a pas le droit, de quelque façon que ce soit, de cibler des Canadiens ou toute personne au Canada » et que cette « interdiction fondamentale » s'applique tant au renseignement étranger et qu'aux cyberopérations du CST.

Sami Khoury a décrit le CST comme un organisme tourné vers l'avenir et déterminé à s'« adapter à l'évolution de la menace, renforcer les défenses et mieux protéger le Canada et les Canadiens ». Il a dit espérer que le projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, « continuera de progresser au Parlement[9] ». Il a expliqué que ce projet de loi vise à renforcer la cybersécurité pour quatre types d'infrastructures essentielles sous réglementation fédérale — les télécommunications, les infrastructures énergétiques, les institutions financières et les systèmes de transport –, que « cette mesure législative établirait un cadre de réglementation pour renforcer la cybersécurité dans les services et les systèmes essentiels à la sécurité nationale et publique, et conférerait au gouvernement un nouvel outil pour réagir aux cybermenaces émergentes ».

Qui plus est, Sami Khoury a souligné le travail actuellement effectué par Sécurité publique Canada pour renouveler la Stratégie nationale de cybersécurité de 2018, « laquelle établira la stratégie à long terme du Canada afin de protéger notre sécurité et notre économie nationales, de dissuader les acteurs présentant une cybermenace et de favoriser l'adoption de comportements fondés sur des normes dans le cyberespace ». Il a précisé que « [p]our le CST, le renouvellement de la Stratégie est l'occasion de faire le point et de poursuivre sur la lancée des réalisations du Centre canadien pour la cybersécurité des cinq dernières années » et a ajouté que « la création de ce Centre était l'une des principales initiatives de la Stratégie nationale de cybersécurité de 2018 ».

Enfin, Sami Khoury a indiqué que le CST s'emploie « à renforcer [ses] relations avec l'industrie canadienne et d'autres ordres de gouvernement » et mise sur « la collaboration avec [ses] partenaires étrangers dans le cadre du Groupe des cinq et d'autres organisations ».

Ministère de la Défense nationale et Forces armées canadiennes

Des témoins ont reconnu que — tout comme le CST — le MDN et les FAC sont des membres importants du milieu de la cybersécurité au gouvernement du Canada et ont entretenu le Comité des rôles, responsabilités et capacités de chacun. Jonathan Quinn et le contre-amiral Lou Carosielli, commandant de la Force cybernétique des FAC, ont fait

9 Le projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, a été déposé à la Chambre des communes le 14 juin 2022, a franchi l'étape de la première lecture le même jour et a franchi l'étape de la deuxième lecture le 27 mars 2023. En date du 19 juin 2023, il avait été renvoyé pour étude au Comité permanent de la sécurité publique et nationale de la Chambre des communes.

remarquer que la cyberguerre est une source de préoccupation croissante pour le MDN et les FAC depuis plusieurs années, et que l'armée canadienne s'efforce de développer et de renforcer ses cybercapacités en collaboration avec les autres ministères et organismes fédéraux, les partenaires et les pays alliés.

Lorsqu'ils ont décrit les rôles, les responsabilités et les capacités liés à la cybersécurité, Jonathan Quinn et le contre-amiral Carosielli ont précisé que la responsabilité du MDN et des FAC consiste surtout à défendre leurs propres systèmes informatiques contre les cybermenaces plutôt qu'à protéger ceux des autres ministères et organismes fédéraux ou du secteur privé. Jonathan Quinn a ajouté que le document *Protection, Sécurité, Engagement : La politique de défense du Canada* publié en 2017 charge le MDN et les FAC d'adopter « une posture plus délibérée dans le cyber domaine en renforçant nos défenses et en menant des cyber opérations actives contre d'éventuels adversaires dans le contexte de missions militaires autorisées par le gouvernement ». Il a souligné qu'à cette fin, les MDN et les FAC travaillent « de près avec le Centre de la sécurité des télécommunications ».

Le contre-amiral Carosielli a affirmé que « [l]e cyberespace est essentiel dans la conduite des opérations militaires modernes et est considéré par le Canada et ses alliés comme un domaine d'opérations militaires, un véritable domaine de combat ». Il a ajouté que « les FAC s'en remettent à l'effet multiplicateur de force qu'ont les systèmes de communication, de renseignement et d'armes axés sur la technologie, qui doivent être adéquatement sécurisés et protégés contre les cybermenaces ». Il a attiré l'attention sur les cyberforces des FAC, qui ont été créées en 2017 pour défendre les réseaux et les systèmes informatiques du MDN et des FAC contre les auteurs de cybermenaces et pour appuyer leurs partenaires et leurs alliés « selon leurs capacités ». À son avis, les cyberforces des FAC « contribuent à la paix et à la sécurité internationale à l'aide du partage de renseignement sur les cybermenaces avec [leurs] alliés et [leurs] partenaires et de la conduite de la gamme complète des cyberopérations autorisées par le gouvernement du Canada ».

De plus, le contre-amiral Carosielli a reconnu que, même si les cyberforces des FAC ont pour mission « de défendre les réseaux et les systèmes informatiques » du MDN et des FAC, elles travaillent aussi « de près » avec des partenaires fédéraux comme le CST et la Gendarmerie royale du Canada pour « mettre en commun tous les renseignements que, entre les partenaires, nous recevons […] pour que tous, nous ayons amplement de renseignements et une bonne compréhension de ce qui se passe dans les autres réseaux ».

D'après le contre-amiral Carosielli, en matière de cybersécurité, les FAC estiment que leurs rapports avec les alliés du Canada à l'étranger leur sont « indispensables ». Il a souligné que les cyberforces des FAC sont « sur la même longueur d'onde que l'U.S. Cyber Command, à tel point qu'[elles ont] un officier de liaison intégré dans ce dernier de même que de nombreux opérateurs, qui vont des cyberopérateurs aux planificateurs de cyberopérations ». Selon lui, les cyberforces des FAC ont ainsi des « conversations quotidiennes » avec l'U.S. Cyber Command et entretiennent une solide relation avec les pays membres du Groupe des cinq et de l'OTAN en matière de cybersécurité.

Pour illustrer l'ampleur de la collaboration qui existe entre les cyberforces des FAC et nos pays alliés, le contre-amiral Carosielli a mentionné qu'en réponse à l'invasion de l'Ukraine par la Russie en février 2022, « les Forces armées canadiennes ont immédiatement mis sur pied une cyberforce opérationnelle pour aider l'Ukraine à renforcer ses cybercapacités de défense ». Il a ajouté qu'actuellement, « [l]e Canada fournit à l'Ukraine une expertise en cybersécurité, des renseignements sur les cybermenaces, des outils logiciels et des solutions techniques qui lui permettent de mieux défendre ses réseaux contre la cyberactivité malveillante ». Selon lui, en réponse à la demande du gouvernement de la Lettonie, « les FAC ont déployé une cyberforce opérationnelle pour mener des opérations conjointes de repérage des menaces afin d'aider ce pays à mieux se défendre contre les [cyber]menaces ».

Jonathan Quinn a affirmé que le MDN et les FAC « sont résolus à saisir les occasions offertes par le cyberespace d'une façon responsable. Ils continueront de travailler pour l'avancement des capacités de leurs cyberforces militaires afin de mener des cyberopérations de façon autonome avec les alliés et d'autres ministères fédéraux et, ainsi, de mieux protéger le Canada contre les cybermenaces. »

Coopération au sein du portefeuille de la Défense nationale

Les témoins qui ont parlé de la coopération entre le CST, le MDN et les FAC ont décrit les façons dont ces organismes interagissent entre eux et dont elles partagent leurs ressources et leurs renseignements pour la cybersécurité. Alia Tayyeb a déclaré que le CST collabore étroitement avec le MDN et les FAC et qu'il a « utilisé ses capacités pour appuyer la mission des Forces armées canadiennes ». Elle a expliqué que les deux organismes ont « essentiellement un effectif combiné », c'est-à-dire qu'ils ont « rassemblé les agents des deux secteurs afin de […] travailler efficacement » sur les questions liées à la cybersécurité.

Jonathan Quinn et le contre-amiral Carosielli ont abondé dans son sens. Le contre-amiral Carosielli a observé que le CST, le MDN et les FAC « ont des relations de

longue date, qui se prolongent dans la cyberdéfense », et que « [l]es deux collaborent quotidiennement en liaison étroite ». Et d'ajouter :

> Certains [des membres du Centre de la sécurité des télécommunications] sont intégrés dans des équipes des Forces armées canadiennes et vice versa. Nous partageons l'information, les outils, le renseignement et nous nous appuyons mutuellement dans des opérations pour le Centre de la sécurité des télécommunications comme pour les Forces armées canadiennes.

Le contre-amiral Carosielli a cependant souligné que les cybercapacités des FAC et du CST diffèrent principalement « parce que nous ne voulons pas de redondance ». D'après lui, « [l]e Centre de la sécurité des télécommunications se spécialise dans l'aspect technique, tandis que les Forces armées canadiennes servent ordinairement à franchir le dernier bout de chemin ». Il a précisé qu'habituellement, « le personnel du Centre de la sécurité des télécommunications ne va pas en zone de guerre ou de conflit, de sorte que, pendant les missions canadiennes, cette distance est parcourue par le personnel des Forces armées canadiennes ».

Le contre-amiral Carosielli a en outre indiqué que les FAC et le CST « agissent de concert selon le soutien nécessaire et en fonction des autorités sous lesquelles certaines opérations sont réalisées » et a fourni l'explication suivante :

> Si telle opération militaire se fait sous l'autorité des Forces armées canadiennes et que nous ayons besoin d'appui sous la forme de renseignements ou d'outils, nous pouvons les obtenir sous le régime de l'article 20 de la *Loi sur le Centre de la sécurité des télécommunications*. De même, si le Centre de la sécurité des télécommunications travaille à un projet et a besoin de nos experts en la matière, il lui est possible de demander notre appui. Nous pouvons le lui fournir et l'appuyer en vertu des pouvoirs qu'il possède, pour répondre aux exigences du Canada.

Jonathan Quinn et le contre-amiral Carosielli ont entretenu le Comité des manières dont le CST et les FAC collaborent lorsqu'ils mènent des cyberopérations offensives[10]. Le

10 Selon la définition de l'Association des industries canadiennes de défense et de sécurité, les « cybercapacités défensives » sont des « activités ou opérations menées dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci pour protéger l'information électronique et les infrastructures de l'information d'une institution aux fins de l'assurance de la mission. Lors d'une cyberopération défensive, il n'y a généralement aucune interaction directe avec l'adversaire. » Toujours selon la définition de l'Association, les « cybercapacités offensives » sont les « opérations menées pour manipuler ou perturber les réseaux et les systèmes d'un adversaire afin d'affaiblir ou de supprimer les capacités opérationnelles de celui-ci. Bien que des entreprises puissent développer des cyberarmes ou des cybercapacités offensives seules ou en partenariat avec le gouvernement, les opérations qui tirent parti de ces capacités sont souvent dirigées par des États-nations et nécessitent une autorisation prévue par la loi, ou encore une autorisation ministérielle ou son équivalent. » Voir Association des industries canadiennes de défense et de sécurité, *From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence*, 2019, p. 8, 9 [TRADUCTION].

contre-amiral Carosielli a expliqué que le CST et les FAC ont le pouvoir de mener des cyberopérations offensives uniquement dans le cadre de missions autorisées. Il a fait remarquer que les autorisations accordées aux FAC proviennent du gouvernement du Canada ou du Cabinet et que, dans le cas des opérations menées « en vertu d'un mandat donné [au] CST […] celui-ci doit recevoir les autorisations du ministère de la Défense nationale et de celui des Affaires étrangères ». Au sujet des mandats, Jonathan Quinn a expliqué ce qui suit :

> Les Forces armées canadiennes possèdent l'autorité pour mener des cyberopérations offensives dans le contexte de missions militaires autorisées. Dans ce cas, c'est elles qui les dirigent et les mènent sous [leur] propre autorité, souvent avec l'aide de collègues du Centre de la sécurité des télécommunications. D'autres opérations de cette nature sont menées sous l'autorité du Centre de la sécurité des télécommunications, en application de la *Loi sur le Centre de la sécurité des télécommunications* […] quand le Centre de la sécurité des télécommunications conduit ces opérations sous le régime de la loi susmentionnée, il peut adresser des demandes d'aide aux Forces armées canadiennes, comme il est prévu dans l'article 20 de la même loi.

Au sujet du rôle joué par le CST dans le cadre des cyberopérations offensives, Alia Tayyeb a précisé que le CST ne travaille pas « de façon indépendante » et a expliqué ceci :

> Nous collaborons très étroitement avec les Forces armées canadiennes et le ministère des Affaires étrangères […] La ministre des Affaires étrangères est tenue de donner son consentement pour [les cyberopérations actives]. Nous travaillons en très étroite collaboration à la planification et à la conception de ces opérations, ainsi qu'à l'évaluation des risques.

M. Christian Leuprecht, professeur au Collège militaire royal du Canada, appuie les pouvoirs conférés au CST, au MDN et aux FAC par le gouvernement du Canada au cours des dernières années pour leur permettre de mener des cyberopérations offensives contre les auteurs de menace, mais il a affirmé que le Canada devrait être plus audacieux et mener sans hésiter des opérations de ce genre pour défendre ses intérêts dans le cyberespace. À son avis, le gouvernement est peu enclin à mener des cyberopérations offensives et « s'est montré extrêmement réticent à utiliser les pouvoirs conférés au Centre de la sécurité des télécommunications » en août 2019. Il a avancé l'idée que, ce faisant, le Canada montre qu'il n'a pas la volonté politique « de faire preuve d'un leadership international indépendant pour réduire l'instabilité et l'incertitude », et que le pays devrait se prévaloir de ces nouveaux pouvoirs pour défendre ses intérêts et ceux de ses alliés dans le cyberespace. À son avis,

> [l]a raison pour laquelle nous devons y recourir, c'est que l'État a un rôle très particulier à jouer dans ce domaine, car les acteurs du secteur privé et d'autres acteurs du secteur public ne disposent pas de capacités actives et offensives. Seul l'État peut déployer ces capacités; par conséquent, seul l'État peut agir de façon proactive en interdisant ou, au

> besoin, dans le cyberespace, en sabotant les capacités des acteurs malveillants émanant d'un État ou tolérés par un État.

Qui plus est, M. Leuprecht a soutenu que le Canada devrait abandonner son approche défensive traditionnelle dans la lutte contre les cybermenaces et les comportements malveillants d'acteurs étatiques et non étatiques dans le cyberespace. Selon lui, le gouvernement du Canada devrait « être plus robuste et musclé en démontrant à ces adversaires que certains types de comportements ne seront pas tolérés dans le cyberespace et entraîneront des répercussions, qu'elles soient cybernétiques ou cinétiques ». Pour ce faire, il a suggéré que le Canada se dote d'une cyberdoctrine qui définirait nettement la manière dont le pays pourrait utiliser ses cybercapacités contre les acteurs malveillants.

RENFORCER LES EFFORTS DE CYBERSÉCURITÉ À L'ÉCHELON FÉDÉRAL

Assurer la cybersécurité exige une vigilance constante, de même que des investissements continus et considérables en matière de ressources financières, humaines, matérielles et technologiques. Étant donné l'apparition quotidienne de nouvelles cybermenaces et menaces de guerre cognitive, les ministères et organismes fédéraux ayant des rôles et responsabilités en matière de cybersécurité doivent rapidement s'adapter pour les déjouer et protéger le Canada. En matière de cybersécurité, il est toujours possible de faire mieux.y a toujours place à l'amélioration lorsqu'il s'agit d'assurer la cybersécurité.

Exposant certains des enjeux liés à la cybersécurité auxquels font face les intervenants du milieu fédéral de la cybersécurité, les témoins ont proposé des solutions. Plus particulièrement, ils ont parlé au Comité du renforcement des capacités et des relations en matière de cyberguerre, de la centralisation des efforts de cybersécurité, des moyens de remédier aux problèmes de main-d'œuvre dans le domaine, de la réponse aux menaces de guerre cognitive, de la réforme des processus d'approvisionnement pour la défense, de l'amélioration de la coopération globale et du développement de cadres juridiques internationaux régissant le cyberespace.

Renforcement des capacités et des relations en matière de cyberguerre

De manière générale, les témoins ont reconnu les liens importants qu'entretiennent à l'interne et entre eux le CST, le MDN et les FAC en ce qui concerne la cybersécurité, mais certains ont recommandé la prise de mesures pour renforcer les capacités et la

coopération. D'après Alexander Rudolph, il faut mieux définir les rôles et responsabilités en matière de cybersécurité du CST et des FAC à l'aide d'un cadre juridique ou d'un « projet de loi pour aborder la cyberdéfense des forces armées et du CST ». À son avis,

> [i]l faut surtout une structure officielle de force et de commandement qui organise le CST et l'armée, ce qui n'existe pas à l'heure actuelle. Tout est fait de façon ponctuelle […] Il faut qu'une structure de commande officielle soit en place pour assurer la médiation en cas de conflit.

Les témoins ont émis des critiques au sujet des capacités de cybersécurité et de l'état de préparation à ce chapitre du MDN et des FAC. Alexander Rudolph a déclaré que le Canada a besoin « d'une intervention très ciblée en matière de cyberdéfense » pour faire face aux cybermenaces, ajoutant que les FAC « ne sont aucunement préparées à une cyberguerre en cas de conflit ». Selon lui, la « politique de cyberdéfense du Canada est à tout le moins incomplète et ponctuelle. Sa stratégie et sa définition ne s'harmonisent pas à celles des alliés du Canada, notamment les États-Unis. » De même, Tadej Nared a affirmé que les « Forces armées canadiennes ne sont pas prêtes à faire face aux cybermenaces, même modérées » et qu'elles « ne seront pas prêtes à relever les défis modernes de la cybernétique dans un avenir prévisible ». À son avis, il faut en faire plus pour renforcer les cybercapacités du MDN et des FAC.

Dans le même ordre d'idées, des témoins ont soutenu qu'il faut redoubler d'efforts pour renforcer les cybercapacités du CST, notamment en augmentant les ressources financières et autres du Centre canadien pour la cybersécurité. Selon Alexander Rudolph, il faut

> tout d'abord […] mieux financer le Centre canadien pour la cybersécurité, et assurer une meilleure communication entre le Centre et le reste du gouvernement. Il faut aussi que le gouvernement tienne compte de la différence entre les besoins des provinces et ceux du fédéral en vue de l'offre des services et de la protection contre les menaces.

M. Leuprecht a avancé qu'il pourrait y avoir « beaucoup plus de collaboration intergouvernementale » entre le CST et les gouvernements provinciaux et territoriaux du Canada. À titre d'exemple, il a noté que « l'Australian Signals Directorate, l'équivalent du Centre de la sécurité des télécommunications au Canada, ou CST, a des bureaux dans chacun des États australiens ».

Centralisation des efforts liés à la cybersécurité

Les témoins ont attiré l'attention sur le fait que les efforts de cybersécurité du gouvernement du Canada ne sont pas centralisés et ont exprimé des préoccupations au sujet de la reddition de comptes. M. de Boer a souligné que « les cyberresponsabilités

sont actuellement réparties entre une douzaine de ministères et d'organismes, sinon plus », ajoutant que « [p]lusieurs ministères ont des responsabilités dans ce domaine, mais il est impossible de déterminer qui dirige et qui assure la cohérence et la concertation des efforts ». À son avis, « [s]i personne n'a la responsabilité claire de promouvoir et de défendre le dossier de la cybersécurité, il risque d'être relégué au énième rang parmi les autres priorités du gouvernement ».

Par ailleurs, M. de Boer a fait observer que dans plusieurs pays, ces efforts sont centralisés et relèvent d'un seul responsable. C'est le cas notamment de l'Australie et des États-Unis, qui ont attaqué cet enjeu « de front en nommant un cyberresponsable ». Dans le cas des États-Unis, il s'agit d'une personne désignée par le président et approuvée par le Congrès. Selon ce témoin, le « Canada devrait envisager la création d'un cabinet ou d'un poste supérieur auquel serait rattachée la responsabilité d'assurer la cohérence et l'action en matière de cybersécurité à l'échelle du gouvernement », car à l'heure actuelle, il « n'y a pas d'unité d'action » et on ne sait trop quelle personne ou quel organisme est responsable de la protection des infrastructures essentielles du Canada contre les cybermenaces.

De même, Tim McSorley, coordonnateur national de la Coalition pour la surveillance internationale des libertés civiles, a soutenu qu'il doit y avoir une centralisation des efforts en matière de cybersécurité au Canada :

> [N]ous avons besoin d'un bureau centralisé pour la cybersécurité […] Il serait également important de disposer d'un organisme chargé non seulement de veiller à ce que la cybersécurité soit gérée correctement, mais aussi à ce qu'elle fasse l'objet d'un examen et d'une reddition de comptes, et à ce qu'elle soit transparente.

M. Leuprecht a indiqué que le gouvernement du Canada devrait envisager le modèle centralisé du Québec, selon lequel les activités de cybersécurité sont dirigées et coordonnées par le ministère de la Cybersécurité et du Numérique, qui est soutenu par un groupe de conseillers. Jugeant les efforts du Québec « très intéressants », il a affirmé que le gouvernement du Canada « pourrait apprendre plusieurs choses du Québec ». Il a également déclaré que l'« ennui avec les processus actuels de prise de décision politique […] c'est que […] nous tergiversons trop longtemps avant de prendre des décisions clés dans des dossiers où nous devons assurer une autorité, une autorisation et une orientation politiques ». Ce témoin estime que le Canada doit prendre plus rapidement des décisions sur la cybersécurité, car « [p]lus nous attendons, plus notre marge de manœuvre se réduit et moins nous avons d'options dans notre boîte à outils ». Selon lui, « [n]ous avons besoin de processus décisionnels plus agiles [en matière de cybersécurité], et il nous faut aussi des processus décisionnels politiques plus rapides

afin de maximiser les options politiques mises à la disposition du gouvernement et les instruments en matière d'opérations pour obtenir l'effet voulu par le gouvernement ».

Moyens de remédier aux problèmes de main-d'œuvre

Au sujet des effectifs, les témoins ont souligné la pénurie de cyberspécialistes qui frappe les secteurs privé et public au Canada, notamment le CST, le MDN et les FAC. M. de Boer a déclaré « qu'il n'y a pas assez de cyberprofessionnels dans le monde », expliquant qu'il « y a plus de trois millions de postes vacants à l'échelle mondiale et, au Canada, il y en a probablement autour de 200 000 ». Selon lui, ce manque d'effectifs dans le domaine constitue un enjeu critique et pressant pour le Canada.

Sami Khoury a exposé certaines des difficultés qu'éprouve le CST pour ce qui est du recrutement et du maintien en poste de spécialistes de la cybersécurité, reconnaissant que le CST et différents ministères et organismes font concurrence avec le secteur privé pour trouver du personnel dans un domaine où il y a un manque criant. Il a déclaré que le CST effectue des investissements tant pour maintenir ses effectifs actuels que pour embaucher de nouveaux employés dans divers postes. Il a précisé que le CST « est très conscient des défis actuels que crée la situation de l'emploi » et s'efforce « d'attirer les talents de diverses parties du Canada », s'intéressant particulièrement aux « Canadiens qui représentent la richesse et la diversité de la société dans laquelle nous vivons ». Par ailleurs, il a souligné que le CST ne concentre pas seulement ses efforts de recrutement dans la région de la capitale nationale, mais essaie aussi d'embaucher des personnes de partout au Canada qui ont une expertise dans divers domaines. Il a ajouté que le CST ne cherche pas seulement à embaucher des gens « qui sont prêts à déménager à Ottawa »; il veut aussi des personnes qui souhaitent habiter en région un peu partout au pays et qui sont prêtes à soutenir les activités de cybersécurité à l'échelle locale.

Soulignant que le CST s'efforce aussi d'engager des étudiants, notamment ceux qui y font des stages coop, Sami Khoury a fait valoir que le CST modernise son « effort de recrutement multidisciplinaire pour attirer les meilleurs talents » et investit « dans un programme d'emplois pour étudiants et un programme d'alternance travail-études afin d'assurer la richesse de [son] bassin de talents ». Il a aussi mentionné que le CST collabore « de près » avec des collectivités « pour sensibiliser les étudiants à la cybersécurité en leur faisant des exposés afin de les intéresser aux domaines des sciences, de la technologie, de l'ingénierie et des mathématiques ».

Alia Tayyeb a ajouté qu'il « y a beaucoup d'intérêt » pour les activités du CST, notamment dans le domaine de la cybersécurité, et que le recrutement va bien :

> Depuis que la visibilité de notre centre de cybersécurité a augmenté, nous avons certainement fait d'importants progrès en matière de sensibilisation du public, d'où le grand nombre de personnes qui souhaitent travailler ici. Nous embauchons une variété de personnes issues de différents domaines techniques; il ne s'agit pas d'un seul type de profession. Nous avons des ingénieurs, des mathématiciens, des experts en cybersécurité, et j'en passe.

Cela dit, elle a reconnu que le CST doit demeurer concurrentiel pour continuer à attirer des cyberspécialistes et qu'il doit entre autres constamment innover et s'assurer de « rester à la hauteur de [ses] concurrents ». Elle a notamment attiré l'attention sur des initiatives conçues pour faire « du CST un excellent lieu de travail » et l'aider à « devenir un employeur de premier plan au Canada », par exemple en offrant « un environnement propice à l'innovation » et en favorisant « un milieu inclusif afin de pouvoir attirer continuellement, dans le secteur, de nouvelles personnes qui n'y auraient peut-être pas songé auparavant, en particulier des femmes ou des gens de différentes origines ethniques ».

De plus, Alia Tayyeb a expliqué que le CST travaillait en partenariat avec les FAC à la « mise sur pied d'une force » dans le but de constituer « une nouvelle main-d'œuvre qui s'intéresse au domaine cybernétique ». Elle a aussi mentionné que le CST travaille en étroite collaboration avec le commandement de cyberdéfense des É.-U. afin d'échanger des informations et des leçons apprises et de discuter de stratégies en matière d'effectifs, le but étant d'« acquérir l'expertise dont nous avons besoin afin de mettre au point des outils efficaces qui nous permettront de relever les défis de demain ».

Le contre-amiral Carosielli a surtout parlé des activités de recrutement et de maintien des effectifs du MDN et des FAC, soulignant que le recrutement de cyberspécialistes va bon train depuis que la création du poste de cyberopérateur par les FAC en 2017 :

> En ce qui concerne les cyberforces […] au cours des trois dernières années, nous avons atteint tous nos objectifs de recrutement de cyberopérateurs. Nous n'avons pas eu à déployer de stratégies de recrutement de cyberopérateurs, car nous n'avons aucun problème à pourvoir ces postes. Les Forces armées canadiennes génèrent des cyberopérateurs.

Il a également déclaré que les FAC investissent « dans la croissance de la force de cybersécurité, tant du point de vue technique que du personnel », expliquant que le poste de cyberopérateur donne aux FAC « la capacité de recruter des gens qui sortent de l'école secondaire » ou « directement dans l'industrie ou dans des établissements d'enseignement d'autres niveaux, comme les universités ».

Nonobstant ces activités, les témoins ont offert des suggestions pour renforcer les efforts au niveau fédéral et ainsi améliorer sa capacité de faire concurrence dans le

recrutement de cyberpécialistes. Christyn Cianfarani, présidente-directrice générale de l'Association des industries canadiennes de défense et de sécurité, a recommandé au Canada d'envisager « l'échange de talents entre les secteurs public et privé » comme le fait le Royaume-Uni dans le cadre du programme Industry 100 du National Cyber Security Centre dans le but de « remédier aux pénuries de cybertalents qui sévissent partout, parce que le fait de se cannibaliser mutuellement ne fonctionnera pas ». Selon le National Cyber Security Centre, ce programme permet une étroite collaboration entre le Centre et le secteur privé, rassemblant des gens afin de favoriser une meilleure compréhension de la cybersécurité, de cerner les vulnérabilités systémiques, de discuter de nouvelles idées et d'atténuer les répercussions des cyberattaques. Dans le cadre du programme, des cyberspécialistes du secteur privé peuvent être détachés au Centre, qui offre divers postes à temps partiel, les détachements allant d'une journée par semaine à un jour par mois, et ce sont les organisations participantes du secteur privé qui paient le salaire de leur employé en détachement[11].

Christyn Cianfarani a avancé que le « recours aux réservistes ayant des compétences en cybernétique embauchés par des entreprises pourrait constituer un moyen attrayant de soutenir la reconstitution des Forces armées canadiennes, pour autant que le gouvernement ne réclame pas la propriété intellectuelle et les brevets des réservistes pour la période où ils étaient embauchés par le secteur privé ». Elle a aussi suggéré que le Canada fasse appel à ses anciens combattants, car beaucoup de ceux ayant une autorisation de sécurité et une expertise dans le domaine quittent la Défense nationale et les « organismes de sécurité ». Elle a mentionné une autre source : nos partenaires du Groupe des cinq.

Dans le même ordre d'idées, le brigadier-général à la retraite Turnbull a encouragé le resserrement de la collaboration entre les secteurs public et privé du Canada afin de trouver des solutions aux pénuries d'effectifs spécialisés en cybersécurité. Il a souligné que le Royaume-Uni, les États-Unis et d'autres alliés du Canada « n'hésitent pas à s'adresser à l'industrie et à s'engager dans des partenariats à long terme avec des chefs de file de l'industrie, de même qu'à investir directement dans les technologies émergentes ». Il a laissé entendre que les ministères et organismes fédéraux « semblent au contraire vouloir résoudre tous les problèmes à l'interne ». À son avis, les « véritables chefs de file de la cybersécurité au Canada ne se trouvent pas au gouvernement ni même au CST. Ils travaillent dans l'industrie des télécommunications, le secteur financier, le secteur du commerce de détail, et le secteur de la cybersécurité, où ils occupent des emplois permanents et à temps plein[12]. » Il a fait remarquer qu'il existe

11 Royaume-Uni, National Cyber Security Centre, *Industry 100* [DISPONIBLE EN ANGLAIS SEULEMENT].

12 Document soumis au NDDN par le brigadier-général à la retraite John Turnbull, 13 février 2023.

« une réticence profondément ancrée à recourir à la sous-traitance pour assurer des services de cybersécurité » pour gonfler les effectifs fédéraux dans le domaine, soulignant que la « plupart des ministères [et organismes], y compris le CST et le MDN, insistent pour constituer et tenter de maintenir leur propre effectif au sein de leurs propres systèmes de ressources humaines ». Selon lui, « [l]'efficience et l'efficacité de cette approche doivent être remises en question[13] ».

M. de Boer a aussi suggéré des façons de renforcer les cybereffectifs du Canada, proposant, par exemple, de « compenser avec des machines, avec l'IA ». Il a proposé que le gouvernement du Canada agisse « immédiatement » pour remédier au problème de pénurie de main-d'œuvre afin de veiller à ce que le MDN et les FAC, de même que d'autres partenaires fédéraux de la cybersécurité, disposent des toutes dernières technologies mues par l'AI, précisant que « ce n'est pas le cas aujourd'hui ».

Réponse aux menaces de guerre cognitive

Les témoins ont recommandé au gouvernement du Canada de redoubler d'efforts pour lutter contre l'ingérence étrangère, les campagnes de désinformation et les autres formes de guerre cognitive. M. Wark a déclaré que le Canada devrait s'« inquiéter davantage des adversaires qui envisagent de mener des campagnes de désinformation et de s'ingérer dans les pratiques démocratiques », observant que depuis 2016, les activités d'ingérence étrangère dans les élections démocratiques suscitent de vives inquiétudes. Il a aussi signalé que les campagnes étrangères de désinformation, de mésinformation et de malinformation polarisent les populations et érodent la confiance du public envers les gouvernements et d'autres institutions bien établies, tant au Canada qu'ailleurs dans le monde. De plus, à son avis, une grande attention est portée dernièrement à « la façon dont nos adversaires étatiques peuvent utiliser des cyberoutils pour tenter d'avoir un impact sur les communautés de la diaspora au Canada et chez nos alliés ».

Encourageant le gouvernement du Canada à s'attaquer aux menaces de guerre cognitive en exposant les acteurs étrangers qui se livrent à ce genre d'activités et en publiant des réponses fondées sur des faits, M. Wark a déclaré ceci :

> La première [mesure], et sans doute la plus importante, consiste à surveiller et à dénoncer publiquement ces activités. Cette dénonciation peut servir de moyen de dissuasion contre les acteurs étatiques étrangers qui tentent d'utiliser ces outils, mais

13 *Ibid*.

> elle peut aussi permettre à la population canadienne de comprendre ce qui se passe […] La sensibilisation de la population est un élément essentiel.

Marcus Kolga a soutenu que le Canada, en particulier ses forces armées, « pourrait avoir du mal à se défendre » dans des situations de cyberguerre. Reconnaissant que les FAC avaient par le passé développé des capacités de se défendre contre les opérations de guerre psychologique et de désinformation étrangères, ce témoin a affirmé que l'effort en vue de maintenir et d'accroître ces capacités a été « interrompu » en 2020 après la diffusion dans les médias de reportages qui laissaient entendre que « les Forces armées canadiennes se préparaient à utiliser la guerre psychologique et les activités d'information contre les Canadiens ». Il était d'avis que depuis, « les Forces armées canadiennes ne semblent pas avoir continué […] ces efforts pour défendre nos forces » contre les opérations de guerre psychologique et les campagnes de désinformation, ce qui fait en sorte que les FAC ne disposent pas à l'heure actuelle « des capacités nécessaires pour se défendre contre ces types d'attaques d'information ». Selon lui, il faut faire davantage pour aider les FAC à se défendre contre les menaces de guerre cognitive.

Par ailleurs, parlant du Comité des parlementaires sur la sécurité nationale et le renseignement, Marcus Kolga a recommandé la création de deux comités parlementaires multipartites : un qui se pencherait sur les cybermenaces, et l'autre qui se concentrerait sur la désinformation d'origine étrangère. Il a indiqué que ces comités non partisans devraient se réunir régulièrement pour discuter des enjeux et analyser les diverses cybermenaces et menaces de guerre cognitive, notamment les « récits de désinformation », pour ensuite en faire rapport à leur caucus respectif.

Réforme de l'approvisionnement pour la défense

D'après les témoins, il importe de réformer le processus d'approvisionnement pour la défense du Canada, car il est trop lourd et lent, limitant la capacité du pays de mettre la main sur les technologies et outils de cybersécurité de fine pointe qui sont nécessaires pour faire face aux cybermenaces en constante évolution. Christyn Cianfarani a recommandé que le Canada se procure rapidement ces technologies, en accordant des marchés au secteur grandissant de la cybersécurité au Canada. Elle a indiqué que ce secteur croît rapidement à l'échelle mondiale et que les dépenses qui y sont associées devraient dépasser celles des TI traditionnelles, le secteur ayant connu une croissance de plus de 30 % pour ce qui est de l'emploi, de la recherche et du développement et des revenus entre 2018 et 2020. Cela dit, elle a souligné que seulement 8 % des revenus du secteur de la cybersécurité sont dérivés des contrats du gouvernement du Canada, les ventes du secteur étant « trois fois plus importantes auprès de nos alliés du Groupe des

cinq qu'auprès du gouvernement du Canada ». Il en ressort, selon elle, que les alliés « voient plus de valeur dans le secteur de la cybersécurité que le Canada ». Elle a affirmé que le Canada « a besoin de faire plus d'acquisitions auprès de sa propre base industrielle, en utilisant l'approvisionnement comme levier politique pour stimuler l'innovation et pour faire croître les entreprises canadiennes » et qu'il doit « faire des acquisitions à la vitesse de la cybernétique ».

Par ailleurs, Christyn Cianfarani a souligné que les cycles d'innovation dans le domaine de la cybersécurité « se mesurent en mois et même en semaines », et qu'un processus d'acquisition lent « est le moyen parfait pour acheter des cybertechnologies désuètes, voire obsolètes », ajoutant que « le temps est le nerf de la guerre ». Selon elle, les pratiques et procédures d'approvisionnement pour la défense de notre pays sont languissantes et ne permettent pas de suivre l'évolution rapide des cybermenaces et les progrès constants en matière de technologies de cybersécurité. Elle était d'avis que ces pratiques et procédures doivent être plus souples et a proposé que l'on élargisse les possibilités de conclure avec des entreprises canadiennes des contrats à fournisseur unique :

> Il y a un lieu et un moment pour la concurrence. Habituellement, les pays ouvrent la porte à la concurrence lorsqu'il y a deux fournisseurs étrangers et aucun fournisseur titulaire canadien […] Lorsqu'il y a un fournisseur titulaire canadien — et ce dont nous parlons ici dans le domaine cyber, c'est d'avoir une entreprise canadienne déjà fiable, sélectionnée, avec qui on est prêt à faire affaire, et dans ce cas particulier, le modèle du fournisseur unique n'est pas et ne doit pas être vu comme le fait de court-circuiter le processus. Au contraire, cela doit être vu comme une solution d'agilité.

Christyn Cianfarani a soutenu que « la plupart des pays utilisent le processus du fournisseur unique ou de l'approvisionnement agile pour maintenir et faire croître les entreprises au sein même de leur pays, et assurer leur viabilité, ce qui veut dire que la sécurité nationale est la sécurité économique », ajoutant que ces pays comprennent « que, fondamentalement, en investissant dans une entreprise [nationale], et en le faisant d'une façon agile avec des sources de confiance ou des personnes de confiance, on peut investir, en fait, dans notre économie ».

Dans le but d'améliorer et d'accélérer le processus d'approvisionnement pour la défense, Christyn Cianfarani a encouragé le gouvernement du Canada a réfléchir aux trois propositions formulées par l'Association des industries canadiennes de défense et de sécurité dans son rapport de 2021 intitulé *Procurement at Cyber Speed* [DISPONIBLE EN ANGLAIS SEULEMENT] :

> [V]ous commencez par créer des projets-cadres qui viennent assurer la capacité […] vous avez des partenaires de confiance et […] il y a acquisition et perfectionnement des

> compétences ici même au pays, puis vous affectez des fonds à l'échelon du projet-cadre. L'autre chose que vous pourriez faire serait d'avoir un financement plus souple. Actuellement, il y a énormément de processus d'approbation. La demande passe par le Conseil du Trésor où il y a environ 200 étapes à franchir […] Vous devriez vous débarrasser [de toutes ces étapes] et envisager des fonds qui bénéficient de la souplesse du crédit 1 et de la possibilité d'acquérir de nouvelles capacités du crédit 5 [pour l'acquisition de technologies de pointe]. Ensuite, la dernière chose que vous pourriez faire serait d'accélérer les processus d'approbation et de conclusion de marchés […] en établissant des lignes directrices, dans lesquelles vous pouvez exiger de la technologie et des services conçus par des Canadiens possédant une autorisation de sécurité canadienne et par des entreprises canadiennes de confiance qui paient leurs impôts au Canada et dont la propriété intellectuelle reste au pays.

De même, Glenn Gulak, président-directeur général de Lorica Cybersecurity, a affirmé qu'il faut faire de la cybersécurité une priorité et, dans la mesure du possible, accélérer le processus d'approvisionnement afin « de suivre l'évolution des cybermenaces[14] ». Il a parlé d'une étude publiée récemment par Innovation, Sciences et Développement économique Canada selon laquelle, en moyenne, les entreprises de cybersécurité canadiennes tirent 69 % de leurs ventes au pays, ce qui comprend les ventes aux gouvernements fédéral, provinciaux et territoriaux, aux administrations municipales et à des clients du secteur privé, et 31 % de ventes à l'exportation[15]. À son avis, le gouvernement du Canada devrait investir dans le secteur canadien de la cybersécurité et rationaliser le processus d'approvisionnement pour accélérer l'acquisition de technologies et d'outils de cybersécurité.

De plus, Glenn Gulak a attiré l'attention du Comité sur le mécanisme d'approvisionnement en matière de cybersécurité de Services partagés Canada qui, à son avis, vise à permettre au gouvernement du Canada et au secteur privé de répondre rapidement aux cybermenaces, de même qu'à simplifier et à accélérer l'acquisition de technologies cybernétiques et d'information. Il a expliqué que ce programme crée « un écosystème des fournisseurs sûrs pouvant rapidement offrir des solutions de cybersécurité à l'échelle de l'organisation qui correspondent aux besoins précis des ministères et des organismes du gouvernement ». Selon lui, le programme est un exemple de processus d'approvisionnement agile qui facilitent l'acquisition de capacités et de technologies en matière de cybersécurité nécessaires à la protection des systèmes et des réseaux du gouvernement du Canada contre les cybermenaces[16].

---

14 Document soumis au NDDN par Glenn Gulak, président-directeur général de Lorica Cybersecurity Inc., 24 mars 2023.

15 *Ibid*.

16 *Ibid*.

Amélioration de la coopération à l'échelle globale

Les témoins ont encouragé le redoublement des efforts en vue d'améliorer la coopération en matière de cybersécurité entre le Canada et ses alliés. Parlant de ses recherches, Kristen Csenkey a expliqué que les pays du Groupe des cinq « n'ont pas tous la même compréhension de certaines menaces à la cybersécurité, » avançant que les « divergences dans l'interprétation des menaces associées à la cybersécurité ont une incidence sur les rôles et les responsabilités des différents acteurs chargés de les neutraliser ». Elle estimait que ces divergences offrent au Canada l'occasion de « prendre les devants au sein du Groupe des cinq pour aborder et favoriser la compréhension de certains enjeux de cybersécurité, comme la menace quantique ». Elle a fait remarquer que, selon ses recherches, il y a des différences « dans la manière dont cette menace [informatique quantique], ses intentions, la technologie employée, ses utilisateurs et les possibles acteurs malveillants sont pris en compte dans les politiques » parmi les pays du Groupe des cinq. À son avis, le Canada pourrait diriger « un consortium quantique » du Groupe des cinq.

Par ailleurs, les témoins ont exhorté le Canada à reproduire les mesures prises par d'autres pays en matière de cybersécurité. M. Leuprecht a indiqué que plusieurs pays ont des ambassadeurs de la cybersécurité qui font la promotion des questions de cybersécurité dans leur pays et à l'échelle internationale, précisant que le Danemark a été le premier pays à créer un tel poste et que les États-Unis ont aussi agi en ce sens. À son avis, le fait que le Canada n'ait pas d'ambassadeur de la cybersécurité « montre que notre façon de concevoir le domaine de la cybersécurité pourrait être mise à jour ». Il a déclaré que le Canada se doit de nommer un tel ambassadeur pour « établir des liens avec le secteur privé et les différentes parties prenantes de la planète, qui ne se trouvent pas forcément dans un pays à proprement parler ». Donnant des précisions sur ce rôle, il a déclaré que :

> [l]e domaine de la cybersécurité se caractérise par une très grande distribution sur le plan géographique, et l'établissement de contacts directs requiert un effort. L'objectif des ambassades et des ambassadeurs est de fournir au gouvernement des renseignements ouverts […] Le gouvernement du Canada n'a actuellement pas assez de renseignements ouverts sur les différentes parties prenantes et les acteurs privés dans ce domaine. Un ambassadeur de la cybersécurité nous permettrait de bâtir des liens avec ces importants joueurs qui, dans plusieurs cas, sont plus puissants que beaucoup de nos partenaires de puissance moyenne.

De même, M. de Boer a recommandé la nomination d'un ambassadeur canadien de la cybersécurité chargé de renforcer les efforts canadiens en matière de cybersécurité et d'assurer une plus grande collaboration entre les secteurs public et privé. Il a exposé les différents rôles que pourrait assurer un tel ambassadeur, faisant valoir que :

> [l]e rôle principal d'une telle personne […] serait, tout d'abord, de signaler à tous les Canadiens que la cybersécurité est importante. Deuxièmement, cette personne serait chargée d'assurer la cohérence des politiques et des programmes dans l'ensemble du Canada. À l'heure actuelle, cela n'existe pas […] Le rôle […] serait d'examiner l'ensemble du gouvernement du Canada afin d'assurer la cohérence et l'unité des efforts et d'unifier notre approche de défense du pays.

Élaboration de cadres juridiques internationaux régissant le cyberespace

Les témoins ont souligné qu'il n'y a pas de cadres juridiques internationaux régissant le cyberespace et la cybersécurité. Alexander Rudolph a déclaré qu'« aucune norme ou loi internationale n'est actuellement en place pour lutter contre les cyberconflits et les cyberguerres ». Du même avis, M. Leuprecht a exposé que depuis deux décennies, « la cyberdiplomatie a échoué à susciter une entente sur les normes internationales visant à limiter les comportements malveillants des acteurs étatiques ou tolérés par les États dans le cyberespace ». Il a déclaré ceci :

> Cela fait 20 ans que nous essayons d'établir des normes et de dégager un consensus à ce sujet, mais nous n'avons guère progressé au sein des Nations unies et d'autres organismes. Ce qu'il faut comprendre, c'est qu'il y a des gens qui croient en l'ordre international libéral fondé sur des règles — c'est-à-dire environ 57 pays –, puis il y a des pays qui sont agnostiques, mais il y a aussi un sous-ensemble de pays qui ne souscrivent tout simplement pas à cet ordre. Par conséquent, nous n'aurons jamais de régime international de cybergouvernance, du moins pas dans un avenir prévisible.

M. Leuprecht a fait valoir qu'en l'absence de normes et de consensus à l'échelle internationale sur le cyberespace, le meilleur moyen pour le Canada et ses alliés de « dissuader et limiter les mauvais comportements » consiste à « intervenir » contre les États et les acteurs non étatiques malveillants en recourant « à des cybermesures actives et offensives ».

Les témoins ont insisté sur le fait que le Canada devrait encourager l'élaboration de normes et de cadres internationaux pour pallier les menaces dans le cyberespace. M. Wark a noté qu'il est nécessaire d'établir en droit international que les cyberattaques constituent des crimes de guerre, commentant que, pour l'instant, il « n'est pas clair dans le droit international » si une cyberattaque contre une nation étrangère constitue un acte de guerre. Il était d'avis que le Canada pourrait prendre « les devants […] en matière de développement du droit international » à ce chapitre. De plus, il a indiqué que l'Ukraine réclame « une dénonciation claire des cyberattaques à l'encontre des infrastructures civiles essentielles comme étant des crimes de guerre » et la volonté « de demander des comptes aux auteurs de ces crimes ». Il a encouragé le gouvernement du

Canada à soutenir « la position de l'Ukraine » et à « être aux avant-postes » des efforts internationaux visant à désigner « les cyberattaques contre les infrastructures essentielles […] comme étant des crimes de guerre en droit international et aider les Ukrainiens à demander des comptes aux coupables ».

Par ailleurs, les témoins ont demandé au gouvernement de mettre en place des lois nationales concernant les cyberattaques étrangères. Aaron Shull a affirmé que le gouvernement du Canada doit « établir un cadre juridique clair et concis pour faire face aux cyberattaques, un cadre comprenant des lignes directrices en matière d'attribution, d'intervention et de responsabilité ». Il était d'avis que la « structure de gouvernance de ce cadre devrait toutefois demeurer souple et être en mesure de s'adapter à un contexte qui évolue rapidement » et que les « règlements devraient être élaborés par des experts en fonction de bonnes pratiques, et non de stratagèmes politiques », ajoutant que le gouverneur en conseil « devrait être en mesure d'approuver les normes, les codes de pratique et les programmes de certification, agissant comme un mécanisme de conformité intégré ».

Qui plus est, les témoins ont affirmé que le Canada et ses alliés devraient imposer des sanctions en guise de réponse aux cyberattaques étrangères. M. Wark a indiqué que l'Ukraine demande à la communauté internationale de recourir « à des sanctions pour miner les cybercapacités d'un agresseur ». Il a proposé que le Canada et ses alliés aient recours « à des sanctions ciblées afin de miner les cybercapacités de l'État russe et de ses mandataires » et qu'ils continuent « de documenter et de dénoncer publiquement les cyberagressions de la Russie à l'encontre de l'Ukraine et de l'OTAN ». Abondant dans le même sens, Marcus Kolga a ajouté qu'il ne faut pas seulement imposer des sanctions en cas de cybermenaces, mais aussi pour les campagnes de désinformation et d'autres opérations de guerre cognitive. Il a soutenu que le gouvernement du Canada pourrait « déployer [son] régime de sanctions de manière plus efficace pour cibler les organes de propagande russes qui répandent ce genre de discours visant à nuire aux intérêts du Canada et de l'Ukraine » au moyen de campagnes de désinformation.

RENFORCER LA CYBERRÉSILIENCE DU CANADA

Au Canada, la cybersécurité demeure une question épineuse qui exige une vigilance constante. Le contexte des cybermenaces évolue constamment : on voit tous les jours apparaître de nouvelles menaces toutes plus sophistiquées les unes que les autres, et des acteurs étatiques et non étatiques ont de plus en plus recours aux technologies nouvelles — comme l'intelligence artificielle et l'informatique quantique — à des fins malveillantes. Il est crucial que les gouvernements et les habitants des pays

comprennent la nature des cybermenaces et acquièrent les connaissances et les capacités nécessaires pour décourager ou contrecarrer ces activités.

Des témoins ont mentionné plusieurs difficultés et plusieurs moyens de renforcer la cybersécurité au Canada, de protéger le pays dans le cyberespace et d'améliorer sa résistance aux cybermenaces et aux cyberattaques. À propos de l'urgence d'agir pour préparer le Canada aux futures cybermenaces, ils ont mis l'accent sur la protection des infrastructures essentielles; la collaboration entre le gouvernement du Canada et le secteur privé; le signalement des cyberincidents; la mise en place de normes de cybersécurité pour le secteur privé; la création d'incitations pour encourager le secteur privé à investir dans la cybersécurité; l'investissement dans la recherche et le développement en matière de cybersécurité; la sensibilisation du public, l'éducation et la formation; de même que sur le respect des droits à la vie privée et des libertés civiles.

Protection des infrastructures essentielles

Comme beaucoup de services courants dépendent des infrastructures essentielles, la compromission de ces infrastructures pourrait porter un grand coup à la sécurité au Canada. Les infrastructures essentielles comprennent les ressources matérielles, les technologies de l'information, les réseaux de distribution d'électricité, les systèmes bancaires et les systèmes de fabrication, de transport et de gouvernement. La *Stratégie nationale sur les infrastructures essentielles* du Canada publiée en 2010 recense 10 secteurs d'infrastructures essentielles[17] et situe les infrastructures de défense et de sécurité dans le secteur « gouvernement ». Les gouvernements fédéral, provinciaux et territoriaux assument la responsabilité de protéger les infrastructures essentielles de concert avec le secteur privé, qui en détient ou en exploite une grande partie.

La numérisation des systèmes et des processus expose les infrastructures essentielles du Canada à des risques. Dans le *Plan d'action 2021–2023 sur les infrastructures essentielles du Forum national intersectoriel*, on dit que « [l]es infrastructures essentielles du Canada demeurent une cible fort intéressante pour l'ingérence étrangère, notamment pour la perturbation intentionnelle des services et le vol de propriété intellectuelle ». On ajoute qu'à cause de la grande interdépendance des secteurs, la perturbation d'un secteur peut se répercuter sur les autres et bouleverser des services essentiels.

17 Les 10 secteurs des infrastructures essentielles du Canada sont : l'énergie et les services publics; les finances; l'alimentation; le transport; le gouvernement; les technologies de l'information et de la communication; la santé; l'eau; la sécurité; et le secteur manufacturier. Voir Sécurité publique du Canada, *Stratégie nationale sur les infrastructures essentielles*, 2010.

Des témoins ont parlé de la nécessité de protéger les infrastructures essentielles du Canada. Tadej Nared a affirmé que les attaques contre les infrastructures essentielles « augmentent de jour en jour » dans le monde entier. Il a donné l'exemple des attaques perpétrées par la Russie ces dernières années contre des infrastructures essentielles de l'Ukraine et d'autres pays ailleurs en Europe et dans le reste du monde. Après avoir observé que les Russes « compromettent des réseaux, des centrales électriques, des centrales hydroélectriques et des infrastructures civiles allant d'hôpitaux à tout le reste », il a exprimé la crainte que « les pays occidentaux, les pays de l'OTAN, ne protègent pas leurs infrastructures comme ils le devraient » et a affirmé que c'est « un énorme problème » auquel « il faudrait [s']attaquer rapidement ».

Le brigadier général à la retraite John Turnbull a avancé l'hypothèse que, « dans une véritable cyberguerre, ce sont les infrastructures essentielles et l'économie du Canada qui seront ciblées ». Ajoutant que les FAC n'ont pas la responsabilité de protéger les infrastructures essentielles, il a remarqué que les MDN et les FAC disposent « de très peu de moyens pour intervenir sur un ["terrain de bataille" comme le cyberespace], si ce n'est pour assurer [leur] propre protection » et celle de leurs systèmes et de leurs réseaux. D'après lui, ce sont Sécurité publique Canada, les autres organismes de sécurité nationale et les entités commerciales du secteur privé qui « devront se préparer à cette bataille et la livrer[18] ».

Des témoins ont attiré l'attention du Comité sur la cybermenace que la Russie fait peser sur les infrastructures essentielles. Sami Khoury a qualifié la Russie de « cyberacteur redoutable » qui « a déployé des capacités cybernétiques destructives en Europe, ou du moins en Ukraine », en ajoutant qu'elle avait réussi à deux reprises à rendre le réseau électrique ukrainien inopérant. À propos de la sécurité des infrastructures essentielles au Canada, M. Khoury a exprimé les préoccupations du CST comme suit :

> Nous sommes très inquiets, et nous aidons les fournisseurs des infrastructures essentielles au Canada à prendre toutes les précautions et toutes les mesures nécessaires pour protéger leurs réseaux contre ce genre de cybermenaces. Les communications ponctuelles et les bulletins d'information que nous envoyons à l'intention des entreprises canadiennes servent à transmettre les enseignements que nous tirons de toute activité cybernétique, de ce qui se déroule en Ukraine et de tout ce que fait la Russie dans le monde.

Marcus Kolga a soulevé des préoccupations semblables. Il a affirmé qu'en ce moment, « [l]es secteurs les plus vulnérables aux cyberattaques russes sont évidemment les infrastructures essentielles ». Faisant ressortir la vulnérabilité des infrastructures

18 Document soumis au Comité NDDN par John Turnbull, brigadier-général à la retraite, le 13 février 2023.

essentielles canadiennes aux cyberattaques, il a mentionné qu'au cours des mois précédents, le secteur de la santé du Canada était « devenu la proie de rançongiciels ». Il a aussi précisé qu'« [u]n grand nombre d'organisations qui se livrent à des activités criminelles comme l'utilisation de rançongiciels sont établies en Russie » et mènent leurs activités avec « l'aval du Kremlin ». Selon l'*Évaluation des cybermenaces nationales 2023–2024* du Centre canadien pour la cybersécurité, depuis mars 2020, plus de 400 organismes de santé au Canada et aux États-Unis ont fait face à des attaques par rançongiciel. Par exemple, en octobre 2021, le système de santé de Terre-Neuve-et-Labrador a été la cible d'une cyberattaque qui a perturbé les services médicaux et compromis des réseaux et des renseignements sensibles. Marcus Kolga a émis l'opinion que « les autorités russes représentent […] une menace pour nos infrastructures de santé et l'ensemble de nos infrastructures essentielles » et qu'elles ont « fait la démonstration » qu'elles n'hésiteront pas « à s'en prendre aux infrastructures essentielles d'un pays ».

Des témoins ont encouragé le gouvernement du Canada à prendre davantage de mesures pour assurer la protection de ses infrastructures essentielles. Lorsqu'il a comparé ce que le Canada investit dans ses infrastructures essentielles à ce que font les États-Unis, M. Wark a souligné que « nous avons un grand pas à franchir pour décider ce que nous souhaitons faire du point de vue de nos infrastructures essentielles ». Il a affirmé que le Canada est encore « en attente d'une stratégie en matière d'infrastructures essentielles » et a décrit ainsi les étapes nécessaires pour développer cette stratégie :

> Il faudra d'abord et avant tout déterminer ce que l'on entend exactement par « infrastructures essentielles ». Une fois que cette étape […] aura été franchie, nous devrons réfléchir à la façon dont nous voulons régir le fonctionnement de ces infrastructures essentielles […] surtout aux fins des stratégies de cybersécurité.

De même, des témoins ont attiré l'attention du Comité sur la nécessité de mieux protéger l'infrastructure industrielle de défense canadienne contre les cybermenaces. Christyn Cianfarani a mentionné que, même si le Centre canadien pour la cybersécurité concentre actuellement ses efforts sur les infrastructures essentielles, il « commence à se pencher sur la base industrielle de défense, ce qui comprend le secteur manufacturier ». Au sujet de la cybersécurité et des risques auxquels l'industrie canadienne de la défense et de la sécurité est exposée, Tim Callan a indiqué que « la fabrication en matière de défense est essentielle aux infrastructures de la défense » et a observé qu'un acteur parrainé par un État peut nuire au Canada et à sa base industrielle de défense grâce à des cyberattaques visant à perturber les systèmes ou grâce au cyberespionnage visant à voler des informations et des secrets de première importance. Faisant remarquer qu'il faut prendre davantage de mesures pour atténuer ces risques,

M. Callan a proposé que le Canada construise « une forteresse de sécurité » pour protéger sa base industrielle de défense, qui revêt une importance stratégique pour la défense et la sécurité nationale du pays.

D'autres témoins, en revanche, ont mentionné qu'on accorde trop d'attention à la vulnérabilité des infrastructures essentielles du Canada. D'après Alexis Rapin, « les cyberattaques sur les infrastructures critiques représentent une menace à risque élevé, mais peu probable ». Il a expliqué qu'en raison de l'importance du risque, « il faut y penser, se préparer et se doter de plans au cas où [de telles attaques] se produiraient », mais que celles-ci « restent assez peu probables ». Il a ajouté que « très peu [de ces attaques] ne se sont véritablement matérialisées au Canada ». À son avis, il faudrait davantage se pencher sur d'autres cybermenaces « plus discrètes, moins graves, » qui « se répètent et se produisent au quotidien » et qui touchent les systèmes et les réseaux du Canada — mais pas nécessairement ses infrastructures essentielles.

Collaboration plus étroite entre le gouvernement du Canada et le secteur privé

Des témoins ont mis l'accent sur la nécessité de resserrer la collaboration entre le gouvernement du Canada et le secteur privé en matière de cybersécurité. Christyn Cianfarani a affirmé que « [l]e Canada a besoin d'un degré plus élevé de coopération, de partage de connaissances et de développement en collaboration entre le gouvernement et le secteur privé ». Elle a reconnu qu'il y a eu « des mesures concrètes en ce sens […] », ajoutant toutefois que « nous ne sommes absolument pas rendus là où nous devrions l'être ». Elle a mentionné que des organismes fédéraux comme le CST « ont les capacités voulues » en matière de cybersécurité, mais a précisé que « la recherche de l'Association des industries canadiennes de défense et de sécurité a montré que notre gouvernement est loin derrière nos alliés lorsqu'il est question de collaboration avec le secteur d'une manière institutionnalisée ». Selon elle, le secteur privé — qui détient et exploite 85 % des infrastructures essentielles du Canada — est l'un des principaux intervenants du domaine de la cybersécurité et joue un « rôle très important » pour ce qui est de sécuriser ses propres infrastructures afin de les protéger des cybermenaces.

En particulier, Christyn Cianfarani a recommandé au gouvernement du Canada d'accroître sa collaboration avec l'industrie canadienne de défense et de sécurité. Elle a mentionné qu'environ 60 % de l'industrie « a la capacité de sécuriser les réseaux et l'infrastructure des données, » ce qui peut comprendre « les réseaux situés dans des environnements menaçants, mais aussi les capteurs et les actifs, comme les avions, les navires et les chars qui opèrent dans des environnements en réseau, comme au sein des

Forces armées canadiennes, ainsi que l'infrastructure ». Elle a ajouté que l'industrie canadienne de défense et de sécurité est également « très fort[e] dans des secteurs stratégiques, comme le cryptage, les tests de pénétration et la surveillance des menaces, » ainsi que les satellites et les autres actifs spatiaux qu'elle entretient, exploite et déploie et qui « servent à la collecte de renseignements et au ciblage ».

Qui plus est, Christyn Cianfarani a souligné que l'industrie canadienne de défense et de sécurité dispose « de talents et de savoir-faire » en matière de cybersécurité et qu'elle « mis[e] constamment sur le développement et l'innovation » dans ce domaine, « afin d'apporter ces compétences aux [ministères et organismes fédéraux] et de maintenir ces derniers au courant de ce qui [se] fait de plus pointu pour protéger le Canada et la société canadienne ». À son avis, le gouvernement du Canada devrait tirer parti de ces ressources et profiterait d'un « échange collaboratif » avec l'industrie canadienne de défense et de sécurité.

D'après M. de Boer, « le renforcement de la collaboration public-privé dans le domaine de la cybersécurité doit devenir prioritaire ». M. de Boer a affirmé qu'« une collaboration proactive entre le gouvernement et le secteur privé sur le plan des opérations » serait utile pour « combler les lacunes en matière de connaissance de la situation, assurer l'uniformité des guides d'intervention en cas d'incident et favoriser une culture axée sur la collaboration proactive à grande échelle ». Il a aussi préconisé « la mise en place d'un environnement de collaboration commun ou d'une collaboration commune en matière de cyberdéfense » qui serait une voie de communication et d'échange de renseignements sur la cybersécurité entre les secteurs public et privé.

Dans le même ordre d'idée, Christyn Cianfarani a observé que « [l]e Canada doit […] créer des systèmes améliorés de partage des menaces qui conjuguent les sources de données ouvertes sur les effractions, les indicateurs et les réponses possibles à celles du gouvernement et de l'industrie ». Elle a précisé que cette approche consisterait à « rationaliser ce qui n'est pas classifié et ce qui reste classifié et qui a accès à quoi ». À son avis, il faut accroître le partage d'informations sur les cybermenaces et les brèches « de manière proactive » et au moyen d'« un mécanisme institutionnel » afin de « pouvoir profiter des technologies et des organismes pour obtenir la meilleure protection possible ».

Par ailleurs, Christyn Cianfarani a affirmé que le gouvernement du Canada devrait « établir un forum permanent pour le dialogue et la discussion sur les questions cybernétiques avec tous les principaux intervenants », c'est-à-dire le secteur privé, le CST, le Centre canadien pour la cybersécurité, le MDN, les FAC, Affaires mondiales Canada et Sécurité publique Canada. Abondant dans le même sens, Aaron Shull a

proposé que le gouvernement mette en place « une plateforme annuelle multilatérale pour assurer la participation et la collaboration des acteurs concernés par la question de la cybersécurité », et que cette plateforme rassemble « des participants de tous les ordres du gouvernement, du secteur privé, de l'industrie, des communautés autochtones, du milieu universitaire, des organismes à but non lucratif, et des chefs de file en matière de maintien de l'ordre ».

Des témoins ont désapprouvé la « rigidité » du système de classification de sécurité actuel au Canada et ont prôné un allègement des exigences en la matière pour faire croître la collaboration et l'échange d'informations entre le gouvernement du Canada et le secteur privé. Christyn Cianfarani a mentionné qu'au Canada, nous avons tendance à classifier à outrance, et qu'au sein des ministères et organismes fédéraux, « nous craignons également ce que les gens feront de ces renseignements et le fait que ces derniers pourraient être utilisés contre nous ». D'après elle, « les Canadiens, de même que nos institutions gouvernementales, sont par nature un peu plus réticents à prendre des risques que nos alliés », et la rigidité du système de cotes de sécurité nuit au partage d'informations cruciales sur les cybermenaces entre le gouvernement et le secteur privé. À cet égard, elle a fourni l'explication qui suit :

> L'idée au pays est qu'il y ait le moins de cotes de sécurité possible. On pense que moins il y en aura, plus on sera en sécurité, moins il y aura de gens qui auront accès à ce genre d'information et de connaissances, plus le pays sera en sécurité, car il y aura sans doute moins de fuites ou choses du genre.

À titre de comparaison, M^{me} Cianfarani a mentionné que des pays comme le Royaume-Uni ou les États-Unis « ont adopté une approche très différente » et « déclassifient de l'information en temps réel […] pour rendre la population plus consciente de ce qui se passe ». À son avis, « il faut que notre optique change » sur l'attribution des cotes de sécurité au Canada, et « l'idée voulant qu'il faille tenir les gens à l'écart, au lieu de les inclure et de mieux les informer, doit changer ».

M. Leuprecht a lui aussi affirmé que le Canada pousse la classification à l'excès, ajoutant que beaucoup de documents devraient être déclassifiés et publiés. Selon lui,

> [a]u Canada, nous avons tendance à surclassifier constamment et abondamment les documents : 90 % des documents que nous classifions n'ont probablement pas besoin de l'être. Les 10 % restants doivent être protégés à tout prix. À l'heure actuelle, nous effectuons une classification beaucoup trop vaste, au lieu de cibler notre protection, nos ressources pour nous assurer que les éléments qui ne doivent jamais être divulgués sont bel et bien protégés. Les discussions récentes sur les fuites montrent que nous avons certes encore beaucoup de travail à faire.

Sami Khoury a fait remarquer que « chaque ministère [fédéral] est doté d'un agent de sécurité organisationnel » et qu'un « groupe » de ces agents se rencontre régulièrement pour discuter des problèmes concernant la classification de sécurité. Il a affirmé que le Conseil du Trésor du Canada est la « branche stratégique » de ce groupe et que le CST ne mène pas de vérification auprès des ministères pour évaluer la manière dont ils traitent les renseignements classifiés. Selon ses dires,

> [n]ous déterminons les différentes normes de sécurité de l'information qui sont en vigueur : protégé A, protégé B, protégé C. Nous communiquons ces normes. Elles sont en quelque sorte instaurées par l'entremise du Conseil du Trésor. Grâce à chacun de ces niveaux de classification, les ministères savent quels renseignements sont classés dans la catégorie « protégé B » ou « protégé C », ou ce qui est secret et ce qui est très secret. Les ministères eux-mêmes doivent respecter ces normes. Nous n'en faisons pas une vérification proprement dite.

Pour améliorer le partage d'informations avec le secteur privé, des témoins ont encouragé le gouvernement du Canada à cesser de travailler en vase clos et à adopter une approche plus uniforme à l'égard de la cybersécurité. En particulier, Christyn Cianfarani a soutenu que le travail en vase clos « nuit beaucoup à nos efforts de coopération » et que « les organismes gouvernementaux provinciaux et municipaux, et en fait, l'ensemble du gouvernement fédéral [ne sont] pas coordonnés dans leurs stratégies ou l'échange d'information face aux menaces ». Elle a aussi attiré l'attention sur le travail en vase clos dans le secteur privé, qui « nuit au pays », surtout dans le domaine de la cybersécurité. Elle a avancé que si le gouvernement faisait tomber les cloisons, il aiderait le secteur privé à « se soucier davantage de la cybernétique » et à mieux se protéger dans le cyberespace, en précisant ceci :

> Notre approche cloisonnée signifie que nous nous occupons de nous-mêmes. Les organismes s'occupent du gouvernement. Les FAC s'occupent des FAC, et l'industrie s'occupe d'elle-même. Ce que nous constatons, c'est que l'approche que nous utilisons ne fonctionne pas.

Signalement des cyberincidents

Des témoins ont indiqué qu'il devrait être obligatoire pour les entreprises du secteur privé de déclarer les cyberincidents au gouvernement du Canada, plus précisément au Centre canadien pour la cybersécurité. Selon Sami Khoury, les rançongiciels sont une « menace sérieuse » pour le secteur privé et sont utilisés contre de nombreuses organisations, mais celles-ci signalent rarement qu'elles en ont été victimes. Lorsqu'il a mentionné que le CST travaille avec le secteur privé pour atténuer ou contrer la menace des rançongiciels, M. Khoury a souligné que le Centre canadien pour la cybersécurité « publi[e] constamment des alertes et des bulletins cybernétiques pour attirer

l'attention sur ce qui pourrait être de nouveaux vecteurs de rançongiciels ou de nouvelles techniques que les cybercriminels utilisent avec des rançongiciels ». Il a ajouté que, « [c]haque fois que l'occasion se présente de parler à une communauté d'affaires, [le CST traite] de la menace des rançongiciels », et que, lorsque des partenaires de cybersécurité alertent le CST qu'ils ont détecté des signes précurseurs d'une cyberattaque contre une organisation du secteur privé, le CST prévient « l'organisation visée » pour qu'elle puisse prendre des mesures de protection.

Sami Khoury a cependant précisé que « [l]e secteur privé n'est pas tenu de signaler des incidents de rançongiciel [au CST ou à son Centre canadien pour la cybersécurité], et bien des entreprises ne les signalent pas ». Il a indiqué qu'en 2021, seulement 300 incidents de rançongiciels avaient été signalés au Centre canadien pour la cybersécurité, et que d'autres « ne sont probablement pas signalés ». Au sujet de l'aide que le CST propose aux organisations du secteur privé qui ont été victimes d'une cyberattaque, M. Khoury a mentionné que, « [p]arfois, elle est acceptée, mais elle est plus souvent rejetée », un état de fait qui doit changer.

Christyn Cianfarani a soutenu l'idée que le gouvernement du Canada emploie la technique « du bâton et de la carotte » pour obliger le secteur privé à signaler les cyberattaques et les brèches dans les systèmes de cybersécurité, dans le but « de nous améliorer et de rendre l'écosystème en général plus sûr ». À son avis, bon nombre d'organisations du secteur privé ne divulguent pas leurs cyberincidents de façon volontaire ou proactive parce qu'ils craignent « que leur marque ou leur entreprise n'en souffre », mais « le bâton pourrait pousser certaines entreprises à divulguer leurs brèches ». Pour ce qui est de la « carotte », M^{me} Cianfarani a recommandé que l'on s'applique à sensibiliser et à renseigner les entreprises pour les amener à se soucier de la cybernétique et de la cybersécurité en leur montrant les avantages qu'il y a à déclarer les cyberincidents, par exemple gagner l'accès à de l'information sur les cybermenaces, les vulnérabilités des autres organisations et les leçons que certaines ont tirées des cyberattaques qu'elles ont subies. D'après elle, si le gouvernement veut pousser les organisations du secteur privé à signaler les cyberincidents, il devra les inviter à le faire d'« une façon efficace » qui ne nuira pas à leur image de marque ou à leurs activités et qui leur rapportera de l'information utile pour renforcer leur sécurité dans le cyberespace.

Kristen Csenkey, qui avait la même opinion, a déclaré que les organisations du secteur privé devraient être tenues de signaler les cyberincidents et a décrit certains des avantages qui en découleraient :

> Si les [petites et moyennes entreprises], ou les entreprises dans cette catégorie, avaient l'obligation de signaler les cyberattaques, cela nous aiderait à évaluer l'ampleur de la

> situation. Cela nous fournirait également davantage de renseignements nous permettant de mieux évaluer la menace et les risques et d'élaborer un cadre visant à mieux protéger certaines industries et des entreprises du secteur privé.

Alex Rapin a abondé dans son sens et affirmé que les organisations du secteur privé devraient être tenues de déclarer les cyberincidents, à titre de « bonne pratique ». Marcus Kolga a lui aussi indiqué que les cyberincidents devraient être déclarés, en précisant que « nous [n']aurions [pas] avantage à les balayer sous le tapis. De cette manière, nous allons acquérir une meilleure compréhension de l'origine des menaces. »

Mise en place de normes de cybersécurité pour le secteur privé

Des témoins ont affirmé que le gouvernement du Canada devrait encourager la mise au point de normes sur la cybersécurité pour le secteur privé. En particulier, Aaron Shull a proposé que le gouvernement « incit[e] les entreprises à adopter [les normes et] les mesures de sécurité les plus récentes » et a attiré l'attention du Comité sur le programme de certification CyberSécuritaire Canada mis sur pied par le CST et par Innovation, Sciences et Développement économique Canada pour les petites et les moyennes entreprises. M. Shull a décrit le programme comme une mesure positive et a encouragé le gouvernement à prendre des mesures supplémentaires, car, même si le programme « offre un niveau de protection élevé […] son adoption demeure limitée ».

Étant donné que l'infrastructure industrielle de défense du Canada est étroitement liée à celle des États-Unis, Christyn Cianfarani a proposé que les deux secteurs collaborent davantage et uniformisent leurs normes de cybersécurité. Selon elle,

> [l]es Américains sont, sans surprise, en avance sur nous. Une norme contraignante et obligatoire sera bientôt appliquée à tous les contrats de défense du Pentagone. Il s'agit du Cybersecurity Maturity Model Certification, la CMCC […] le Canada devrait adopter cette norme comme référence. La CMMC deviendra fort probablement de fait la norme de référence du Groupe des cinq, voire une norme mondiale, des entreprises de défense.

M^{me} Cianfarani a ajouté que « la moitié [des exportations de la base industrielle de défense canadienne] sont destinées aux États-Unis. Si nous voulons être un partenaire fiable dans la chaîne d'approvisionnement aux États-Unis, nous allons devoir avancer de pair avec eux pour nous assurer de pouvoir être des partenaires de confiance et qu'ils pourront s'approvisionner chez nous. »

D'après Christyn Cianfarani, le Canada étudie la CMMC « en ce moment même » et l'ambassade du Canada aux États-Unis, Sécurité publique Canada, le MDN et Services publics et approvisionnement Canada « essaient d'établir si la norme doit être

“canadianisée” de quelque façon ». C’est une chose qu’elle déconseille, car, si on développait des parties canadianisées de la norme, « les entreprises canadiennes se retrouveraient […] avec deux normes, ce qui augmenterait leur coût ». M^{me} Cianfarani a également émis l’hypothèse que, « [s]i nous ne faisons pas les choses correctement, les Américains pourraient aller de l’avant pendant que les entreprises canadiennes attendent la norme nationale et seraient donc laissées en plan en matière d’approvisionnement », car ces entreprises seraient incapable de soumissionner pour des projets d’approvisionnement militaire américains. Elle a ajouté que « le fait de prendre le temps d’envisager d’adopter une autre norme au Canada pourrait s’avérer être un désavantage pour les entreprises canadiennes et un obstacle au commerce libre de tarifs douaniers ».

Création d’incitations pour encourager le secteur privé à investir dans la cybersécurité

Des témoins ont exhorté le gouvernement du Canada à offrir des incitations aux organisations du secteur privé, en particulier aux petites et moyennes entreprises, pour les encourager à investir dans la cybersécurité. M. de Boer a observé que 47 % des petites et moyennes entreprises qui ont répondu à un sondage de 2021 commandé par le Bureau d’assurance du Canada[19] avaient déclaré n’avoir absolument rien investi dans la cybersécurité. Il a indiqué que ces entreprises sont très vulnérables aux cyberattaques et sont souvent la cible de tentatives de cyberespionnage ou de vol de propriété intellectuelle. À son avis, puisque le coût élevé des mesures de cybersécurité freine les investissements des petites et moyennes entreprises canadiennes dans ce domaine, le gouvernement du Canada devrait « inciter [ces entreprises] à protéger leur propriété intellectuelle » ainsi que leurs systèmes et leurs réseaux.

Dans le même ordre d’idée, Aaron Shull a recommandé la création d’un crédit d’impôt fédéral qui inciterait le secteur privé à investir dans la cybersécurité en vue d’« accroître le niveau général de cybersécurité au pays et [de] réduire le risque de cyberattaques visant nos entreprises ». Il a souligné que les cyberattaques commises contre le secteur privé entraînent des pertes financières importantes, perturbent les opérations et portent atteinte à la réputation.

19 Voir Bureau d’assurance du Canada (BAC), « Beaucoup de petites entreprises sont vulnérables aux cyberattaques », 2021; et Léger, *IBC Small Business Cyber Security Survey Report*, 17 août 2021 [DISPONIBLE EN ANGLAIS SEULEMENT].

Investissement dans la recherche et le développement en matière de cybersécurité

Des témoins ont fait ressortir la nécessité pour le Canada d'investir dans la recherche et le développement (R-D) en matière de cybersécurité afin de donner au pays des moyens de réagir aux nouvelles cybermenaces. M. de Boer a affirmé que « nous devons investir continuellement dans la R-D […] pour ne pas être dépassés par nos rivaux ». Il a aussi dit que « [n]ous sommes à la traîne en matière d'investissement dans la R-D » et a expliqué que, pour le moment, les entreprises canadiennes — notamment les multinationales — gagnent bien plus à développer la R-D à l'étranger « parce qu'il y a beaucoup plus de systèmes de soutien collaboratifs en place ». D'après lui, il faut « un partenariat concerté entre le gouvernement [du Canada] et le secteur privé » en matière de R-D, concentré sur « certains créneaux où le Canada jouit d'un avantage comparatif ».

M. de Boer a proposé que le gouvernement du Canada donne un élan à la R-D en matière de cybersécurité en aidant le secteur privé à « commercialiser » les technologies pertinentes conçues au pays. Il a fourni l'explication suivante :

> Il y a beaucoup de ce que nous appelons un niveau de maturité technologique inférieur. Autrement dit, le tout début de la R-D se déroule au Canada, mais ensuite, passée cette étape initiale, la R-D traverse ce qu'on appelle la vallée de la mort, ce qui veut dire qu'il est très difficile de productiser cette R-D ici, au Canada. Par exemple, très peu de programmes soutiennent les entreprises canadiennes pour les aider à lancer des produits initiaux afin de les essayer et de commercialiser […]

M. de Boer a comparé la situation du Canada à celle de son voisin, en faisant remarquer que les États-Unis « ont mis en place des systèmes pour aider les entreprises à franchir cette vallée de la mort afin qu'elles puissent commercialiser leurs produits ». Il a proposé que le gouvernement du Canada « cré[e] un fonds de commercialisation canadien qui aiderait des entreprises canadiennes à passer l'étape de la productisation ».

D'après Glenn Gulak, le gouvernement du Canada doit trouver des moyens de resserrer sa collaboration avec les chefs de file du secteur privé canadien et d'encourager les innovations en matière de cybersécurité. Par exemple, dit-il, le gouvernement pourrait « organiser des vitrines plus régulières (qui mettent généralement en évidence les secteurs d'intérêt du gouvernement) et lancer un plus grand nombre de défis d'innovation et de projets pilotes rémunérés. Il pourrait également simplifier le processus d'approvisionnement […] afin que des solutions de pointe "fabriquées au Canada" soient intégrées rapidement dans ses systèmes opérationnels. » M. Gulak a ajouté que « [l]es investissements de ce genre sont essentiels sur le plan de l'économie

et de la sécurité afin de protéger la prospérité, les valeurs et le bien-être du Canada dans un avenir de plus en plus incertain[20] ».

Sensibilisation du public, éducation et formation

Selon des témoins, il faudrait bonifier les programmes publics de sensibilisation, d'éducation et de formation concernant les cybermenaces et les menaces de guerre cognitive. Tim Callan a affirmé que « l'être humain est toujours un maillon faible dans tout système numérique » et a souligné que, même si « on peut très facilement mettre au point des solutions cryptographiques mathématiquement pures qui sont sans failles […] [i]l est plus difficile d'enseigner aux gens à ne pas tomber dans les pièges ». Il a recommandé qu'on offre une formation sur « l'ingénierie sociale » axée sur la cyberhygiène, et aussi qu'on sensibilise davantage les gens aux cybermenaces et aux menaces de guerre cognitive.

M. Wark a suggéré que le gouvernement du Canada rehausse ses programmes de sensibilisation, d'éducation et de formation concernant la cybersécurité. Il a fait remarquer qu'à l'avenir, on pourrait « transposer » les « systèmes de formation » du CST dans d'autres ministères et organismes fédéraux et dans le secteur privé.

Marcus Kolga a lui aussi soutenu qu'il faut renseigner les Canadiennes et les Canadiens sur les cybermenaces et s'assurer que les personnes qui travaillent au sein du gouvernement, des autres organisations du secteur public et des organisations du secteur privé « possèdent de solides compétences en matière de cyberhygiène, notamment l'utilisation de mots de passe robustes ». Selon lui, « c'est par là que nous devons commencer pour protéger [les] infrastructures essentielles et [les] institutions [du Canada] ».

Marcus Kolga a également attiré l'attention du Comité sur l'importance d'intégrer la sensibilisation du public, l'éducation et la formation « non partisanes » — au moyen d'une approche « pansociétale » — à tout effort national visant à combattre les activités d'influence étrangère et les campagnes de désinformation. Il a mentionné plusieurs pays qui intègrent ces mesures publiques à leur lutte contre les activités d'ingérence étrangère et les campagnes de désinformation, y compris des « pays qui partagent une frontière avec un voisin qui mène des activités de désinformation », notamment l'Estonie, la Lettonie et la Lituanie, qui bordent toutes la Russie et qui sont visées depuis longtemps par les activités d'influence et les campagnes de désinformation de celle-ci.

20 Document soumis au Comité NDDN par Glenn Gulak, président-directeur général de Lorica Cybersecurity Inc., 24 mars 2023.

M. Kolga a aussi fait remarquer que Taïwan « fait un travail exceptionnel dans la lutte contre la désinformation chinoise » et que la Finlande et la Suède « ont intégré des activités de sensibilisation […] dans les programmes d'éducation de la petite enfance » pour veiller à ce que « toutes les prochaines générations de Suédois et de Finlandais disposent des ressources cognitives nécessaires pour évaluer de manière critique les informations auxquelles ils sont exposés ».

Qui plus est, Marcus Kolga a encouragé le Canada à adopter les pratiques exemplaires que d'autres pays ont mises en place pour sensibiliser, renseigner et former leur population concernant les cybermenaces, y compris les menaces de guerre cognitive. D'après lui, « il faut une sensibilisation plus exhaustive en général pour tous les Canadiens afin qu'ils puissent reconnaître les activités d'information et se défendre contre elles ». M. Kolga a aussi fait ressortir la nécessité de « créer [une] capacité à gérer directement [les messages de désinformation], à les contester et à les repousser » publiquement.

Protection du droit à la vie privée des particuliers et des libertés civiles

Un des témoins a soulevé des préoccupations au sujet du droit à la vie privée des particuliers et des libertés civiles dans le contexte de la cybersécurité. Tim McSorley était d'avis « qu'il est vital pour le Canada de moderniser ses lois en matière de cybersécurité afin de mieux protéger les renseignements confidentiels des Canadiens et les infrastructures d'information dont nous dépendons ». Reconnaissant « que le nombre et la complexité des cyberattaques augmentent, et que le Canada n'a pas le choix de prendre des mesures pour se défendre », il a toutefois insisté sur le fait que « rien ne doit être fait au détriment de la responsabilité et de la transparence des activités du gouvernement, y compris celles du CST ».

Tim McSorley a également soutenu que les « pouvoirs trop larges » conférés au CST et à d'autres organismes fédéraux responsables de la sécurité nationale, de même que la « culture du secret trop poussée » dans l'esprit de laquelle ils mènent généralement leurs activités, pourraient mener à la violation des droits individuels des Canadiens. Selon lui, de telles violations peuvent avoir de « réelles » conséquences, surtout si des renseignements au sujet de Canadiens sont transmis à des gouvernements étrangers. Conscient qu'en vertu de la *Loi sur le Centre de la sécurité des télécommunications*, le CST ne peut pas cibler des Canadiens, il a néanmoins fait remarquer que le CST fait la collecte de renseignements SIGINT et de toutes sortes d'informations, dont une partie « peut se rapporter à des Canadiens » en particulier dans le cadre de ses activités de cybersécurité. Il a mentionné que dans ces situations, le CST « ne cible pas des

Canadiens ». Or, selon lui, le CST « recueille accessoirement ces renseignements et les conserve, et ils sont encore utilisés par ailleurs ». Il a affirmé que les pays du Groupe des cinq et d'autres encore ont accès à des renseignements concernant certains Canadiens, ajoutant que « le Canada [peut perdre] le contrôle sur ce qu'on en fait et laisse le champ libre à des utilisations qui peuvent mener à des atteintes aux droits, à des abus et même à la torture ».

Par ailleurs, Tim McSorley s'est dit inquiet du double mandat du SCT (renseignement électromagnétique et cybersécurité), signalant que l'exécution de ces deux volets « ne se fait pas en vase clos ». Il a recommandé que l'on modifie la *Loi sur le Centre de la sécurité des télécommunications* et le projet de loi C-26 afin d'établir des « séparations strictes » entre ces deux types d'activités, notamment en établissant des restrictions relatives à l'échange d'information. Il a aussi suggéré que « des restrictions plus importantes soient imposées à la collecte, à la conservation et à l'utilisation des métadonnées et des "informations accessibles au public" » par le CST et que des exigences plus strictes soient mises en place relativement « aux autorisations en matière de renseignement étranger et de cybersécurité, ainsi qu'aux approbations de cyberopérations actives et défensives, afin de garantir le respect par le CST de ses obligations à l'égard des organes de contrôle et d'examen ». Proposant que le CST « mette immédiatement en place un système permettant à l'[Office de surveillance des activités en matière de sécurité nationale et de renseignement] d'accéder à ses dossiers », il a aussi exigé qu'« un examen complet des cyberactivités actives et défensives du CST soit effectué, en particulier en ce qui concerne le respect du droit international et le rôle du Canada dans l'intensification des activités de cyberguerre », de même qu'un examen des « activités de surveillance de masse internationale du CST » afin d'en restreindre la portée[21].

Au sujet de la surveillance, Tim McSorley a préconisé un contrôle plus étroit du CST et des autres ministères et organismes fédéraux responsables de la cybersécurité dans le but de stimuler la confiance du public à l'égard de leurs activités. Il a fait valoir que le « contrôle et l'examen ne consistent pas seulement à mettre les organisations sur la défensive et à les dénoncer, mais aussi à voir comment nous pouvons tirer des leçons de nos erreurs et améliorer les opérations ». À son avis, il « faut de l'ouverture et de la transparence pour que nous comprenions ce que font les agences canadiennes, y compris le CST, lorsqu'elles s'engagent à protéger la cybersécurité du Canada, à mener des cyberopérations actives et défensives et à faire du renseignement d'origine

21 Document soumis au NDDN par la Coalition pour la surveillance internationale des libertés civiles, le 6 avril 2023.

électromagnétique », et le moyen de s'en assurer est « d'imposer davantage de déclarations obligatoires sur les activités qu'elles mènent ».

Alexander Rudolph a exprimé un point de vue similaire et a affirmé qu'une plus grande transparence était nécessaire dans le domaine de la cybersécurité au Canada. Comme il l'a indiqué :

> Je suis tout à fait d'accord pour dire qu'il faut plus de transparence, de façon générale, sur la politique de cyberdéfense canadienne. J'effectue principalement mes recherches en examinant les rapports de vérification et les résultats ministériels. […] Je connais les grands thèmes, mais mes connaissances comportent beaucoup de lacunes, et c'est tout simplement parce que les Forces armées canadiennes ne disent pas tout et qu'on les empêche de le faire.

En outre, Tim McSorley a attiré l'attention du Comité sur le fait qu'il n'y a pas d'organe de surveillance fédéral chargé d'examiner les activités de cybersécurité au Canada. Mentionnant le contrôle exercé par le commissaire au renseignement du Canada et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, il a observé qu'il « n'est pas évident qu'ils aient un rôle à jouer dans l'examen des opérations de cybersécurité du Canada, parce qu'elles touchent à la sécurité nationale, mais pas forcément de la manière dont ces organismes l'examinent toujours ». D'après lui, il faudrait soit modifier le mandat de ces organisations pour « bien préciser » qu'elles sont responsables de l'examen des activités de cybersécurité, soit créer un nouveau poste qui aurait cette responsabilité.

OBSERVATIONS ET RECOMMANDATIONS DU COMITÉ

Le contexte des cybermenaces est en constante évolution. Chaque jour, de nouvelles menaces de plus en plus sophistiquées sont conjurées et utilisées par des États et des acteurs non étatiques malveillants à diverses fins. Les Canadiens vivent dans l'un des pays les plus interconnectés de la planète et dépendent de plus en plus des technologies, des systèmes et des réseaux numériques. Ils utilisent entre autres Internet pour le travail, les études, les soins de santé, les services bancaires, les achats, les divertissements et les interactions sociales. En plus de faire ressortir l'importance d'une connectivité Internet fiable et abordable, la pandémie de COVID-19 a accéléré l'adoption de technologies numériques facilitant le télétravail, les études à distance et la recherche des contacts en ce qui concerne l'exposition au virus de la COVID-19. De nos jours, les Canadiens sont beaucoup plus exposés aux cybermenaces qu'il y a à peine cinq ans.

L'évolution rapide du contexte de sécurité mondiale ces dernières années a amené un grand nombre de pays à réaliser des investissements sans précédent dans la sécurité et

la défense, y compris leurs forces armées. La résurgence de la concurrence entre les puissances mondiales et les actions de plus en plus agressives de certains États autoritaires, révisionnistes et expansionnistes, comme la Chine et la Russie, ont fait croître les tensions entre des pays, de même qu'à l'intérieur de certains, déstabilisant plusieurs régions du monde et y faisant éclater des conflits. Dans le cadre de leurs investissements dans la sécurité et la défense, le Canada et ses alliés s'efforcent non seulement de protéger leurs systèmes et réseaux numériques contre les cybermenaces étrangères, mais aussi de préparer leurs forces militaires et de sécurité à mener des activités et à triompher dans le cyberespace moderne.

Le Comité convient certes que la cybercriminalité est la menace qui touche le plus les Canadiens en tant qu'individu, mais les programmes cybernétiques parrainés par des États, comme la Russie, la Chine, l'Iran et la Corée du Nord, demeurent la plus grande cybermenace stratégique pour notre pays. Les cyberattaques et les opérations militaires cinétiques menées par la Russie contre l'Ukraine au cours de la dernière année illustrent à quel point le cyberespace est devenu un nouveau théâtre de guerre et font ressortir que la cyberguerre est une nouvelle réalité du 21^{e} siècle. Qui plus est, les menaces de guerre cognitive sont de plus en plus préoccupantes.

Comme d'autres, le Comité croit que l'ensemble de la société doit participer aux efforts visant à protéger le Canada contre les cybermenaces et les menaces de guerre cognitive. Les ordres du gouvernement, les différentes entités du secteur public, le secteur privé et les Canadiens doivent tous contribuer à la cybersécurité. Le gouvernement du Canada joue un rôle important, et une douzaine de ministères et organismes fédéraux — dont le CST, le MDN et les FAC — se livrent à des efforts visant à assurer la cybersécurité sous la direction de Sécurité publique Canada. À ces efforts nationaux s'ajoutent la collaboration et la coopération internationale, qui sont essentielles pour protéger notre pays contre les cybermenaces et les menaces de guerre cognitive.

Le Comité croit aussi que des efforts soutenus au niveau fédéral sont nécessaires pour veiller à ce que le Canada soit dans le peloton de tête des nouvelles technologies numériques et qu'il mette l'accent sur la cybersécurité. Le Canada doit agir en ce sens pour lui permettre de connaître du succès dans des contextes de cyberguerre non seulement aujourd'hui, mais dans les années à venir, ce qui est important. Entre autres, le Canada doit porter une attention soutenue à la cyberguerre, à la coordination des efforts en matière de cybersécurité, aux effectifs spécialisés dans le domaine, aux menaces de guerre cognitive, à l'approvisionnement pour la cyberdéfense, à la coopération mondiale sur les questions de cybersécurité et à l'établissement de cadres internationaux relatifs au cyberespace.

Par ailleurs, le Comité se joint à d'autres pour signaler que, pour renforcer la cyberrésilience à l'échelle nationale, des activités devront être menées dans différents domaines, notamment la protection des infrastructures essentielles, le resserrement de la collaboration entre les secteurs public et privé sur les questions de cybersécurité, le signalement des cyberincidents dès qu'ils se produisent, l'élaboration de normes connexes, la mise en place d'incitations à l'investissement, l'investissement dans la recherche et le développement sur la cybersécurité, la sensibilisation du public et la formation, et le respect des droits à la vie privée et des libertés civiles.

Il est clair pour le Comité que tout le Canada — c'est-à-dire les gouvernements, le secteur privé et les particuliers — doit agir non seulement pour aider le pays à se défendre contre les cybermenaces, mais aussi pour veiller à ce que les systèmes et réseaux numériques soient protégés contre les cybermenaces et les menaces de guerre cognitives qui évoluent rapidement. La cybersécurité — qui doit être un objectif partout au sein de notre société — est essentielle à sécurité et à la prospérité du Canada dans les années à venir.

Compte tenu de ce qui précède, le Comité recommande :

Recommandation 1

Que le gouvernement du Canada mette en place une plateforme multilatérale permanente pour susciter la collaboration et l'engagement des divers intervenants en matière de cybersécurité. La plateforme devrait avoir des objectifs fondés sur ceux du programme Industry 100 du Royaume Uni. Elle devrait aussi former un espace collaboratif dans lequel les responsables de l'industrie et de la cybersécurité pourront se réunir pour échanger des informations et des pratiques exemplaires et établir des moyens de signaler les cyberattaques commises contre le secteur privé en vue d'améliorer le partage d'informations et de prévenir d'autres attaques.

Recommandation 2

Que le gouvernement du Canada investisse dans la cybersécurité de sa propre infrastructure réseau et évalue de façon exhaustive les mesures supplémentaires nécessaires pour renforcer les systèmes du gouvernement et l'infrastructure réseau des tierces parties qui hébergent ses données, afin d'assurer la sécurité de ses données critiques.

Recommandation 3

Que le gouvernement du Canada collabore avec ses partenaires du Groupe des cinq pour adopter une norme CMMC (Cybersecurity Maturity Model Certification) compatible avec celles de ses partenaires et reconnue par ces derniers afin d'éviter que l'utilisation d'une norme distincte au Canada ne défavorise les entreprises de l'industrie de défense canadienne par rapport à celles des autres pays membres du Groupe des cinq.

Recommandation 4

Que le gouvernement du Canada offre des incitations (p. ex. des crédits d'impôt) aux entreprises pour les encourager à adopter des mesures de cybersécurité, comme le programme de certification « CyberSécuritaire Canada » créé par ISED et le CST pour les petites et moyennes entreprises.

Recommandation 5

Que le gouvernement du Canada accélère le renouvellement de la stratégie nationale de cybersécurité du pays et qu'il soumette cette stratégie à un examen périodique pour pouvoir la mettre à jour au rythme de l'évolution des cybermenaces.

Recommandation 6

Que le gouvernement du Canada maintienne son dialogue avec les propriétaires et les exploitants d'infrastructures essentielles tels que les municipalités; les gouvernements provinciaux, territoriaux et autochtones; et les exploitants du secteur privé comme les sociétés de service public, et que ces efforts soient officialisés afin qu'il y ait un dialogue constant sur les menaces éventuelles et sur les bonnes pratiques.

Recommandation 7

Que le gouvernement du Canada examine la Loi sur le Service canadien du renseignement de sécurité pour s'assurer que le Service dispose des outils juridiques dont il a besoin pour s'adapter aux réalités modernes de l'ère numérique et pour suivre le rythme des progrès technologiques et de la perpétuelle évolution des menaces qui planent sur la cybersécurité au Canada.

Recommandation 8

Que le gouvernement du Canada collabore avec les provinces et l'industrie pour créer des exigences obligeant les exploitants d'infrastructures critiques du secteur privé à signaler les attaques par rançongiciel et les atteintes à la cybersécurité au Centre

canadien pour la cybersécurité dans un délai donné; qu'il mette en place des mécanismes appropriés pour protéger les victimes de cyberattaques et, ainsi, atténuer ou éliminer les facteurs qui les dissuadent de signaler ces attaques; et que le gouvernement incite les propriétaires et les exploitants d'infrastructures critiques à coopérer avec les autorités compétentes pour déceler, signaler et éliminer les vulnérabilités.

Recommandation 9

Que le gouvernement du Canada collabore avec ses partenaires de l'industrie pour améliorer la cybersécurité au stade de la conception du matériel informatique et des logiciels afin de délester les utilisateurs d'une partie du fardeau d'assurer la cybersécurité.

Recommandation 10

Que le gouvernement du Canada prenne des mesures pour maintenir au pays la propriété intellectuelle des technologies de l'information conçues au Canada, y compris des mesures de commercialisation pour préserver la propriété canadienne des cybertechnologies.

Recommandation 11

Que le gouvernement du Canada, en collaboration avec la société civile, l'industrie et les pays alliés, développe davantage de ressources pour faire face aux opérations étrangères de guerre cognitive — dont la mésinformation, la désinformation et la malinformation — afin de mieux protéger les Canadiens et de veiller à ce que le public ait accès à de l'information exacte.

Recommandation 12

Que le gouvernement du Canada veille à ce que les ministères et les contrats fédéraux fassent l'objet d'une vérification afin de confirmer que les normes de sécurité de l'information sont bien respectées par le gouvernement et les sous-traitants.

Recommandation 13

Que le gouvernement du Canada collabore avec les provinces en vue d'établir des normes de cybersécurité de base pour les petites et moyennes entreprises, et qu'il offre des incitations aux entreprises pour les encourager à adopter les mesures de sécurité les plus récentes qui les protégeront contre les attaques à risque élevé, mais peu probables, ainsi que contre les attaques à faible risque, mais fréquentes.

Recommandation 14

Qu'il y ait une plus grande collaboration entre le gouvernement du Canada et l'industrie canadienne de la défense et de la sécurité pour renforcer l'infrastructure de cyberopérations offensives et défensives du Canada à un moment où des États malveillants manifestent une audace croissante.

Recommandation 15

Que le gouvernement du Canada entreprenne une analyse approfondie de la cybersécurité pour cerner les vulnérabilités du Canada en la matière, y compris au sein de ses infrastructures essentielles, et pour déterminer la priorité à accorder à la suppression de ces vulnérabilités et des intrusions commises par des acteurs malveillants.

Recommandation 16

Que le gouvernement du Canada désigne les plateformes spatiales comme des infrastructures essentielles et qu'il veille à ce qu'elles soient sécurisées.

Recommandation 17

Que le gouvernement du Canada précise les rôles et les responsabilités de chacun des ministères chargés d'exploiter des cybercapacités au Canada, d'en faire la surveillance ou d'intervenir en cas de cyberattaque.

Recommandation 18

Que le gouvernement du Canada procède à un examen de toutes les cyberinfrastructures qui soutiennent les fonctions opérationnelles du ministère de la Défense nationale et des Forces armées canadiennes afin de s'assurer qu'elles ne contiennent aucune technologie critique conçue, assemblée ou exploitée, de façon directe ou indirecte, par des États malveillants, et susceptible de présenter un risque pour la cybersécurité ou de compromettre des informations protégées.

Recommandation 19

Que le gouvernement du Canada oblige tous les ministères fédéraux à fournir au Conseil du Trésor et au Centre de la sécurité des télécommunications une liste détaillée de leurs infrastructures essentielles et à mettre cette liste à jour chaque année, et qu'il demande à tous les gouvernements provinciaux, territoriaux, municipaux et autochtones et à toutes les administrations municipales d'en faire de même.

Recommandation 20

Que le gouvernement du Canada augmente le financement accordé au Centre canadien pour la cybersécurité pour améliorer la coordination entre les systèmes de cybersécurité fédéraux et provinciaux en vue de mieux réagir aux incidents.

Recommandation 21

Que le Parlement du Canada crée un comité mixte spécial sur la cybersécurité, la guerre de l'information et l'intelligence artificielle.

Recommandation 22

Que le gouvernement du Canada entreprenne immédiatement un examen complet et une réforme expéditive des processus d'approvisionnement en équipement militaire, y compris l'équipement de cyberguerre — et que l'examen et la réforme visent aussi les lignes directrices du Conseil du Trésor sur les processus d'appel à la concurrence et d'attribution de contrats à fournisseur unique —, afin que la durée des projets puisse se compter en semaines ou en mois plutôt qu'en années.

Recommandation 23

Que le gouvernement du Canada s'adapte et mette au point un plan détaillé de recrutement et de conservation des cyberopérateurs qui puisse soutenir la concurrence du secteur privé pour aider les Forces armées canadiennes et le Centre de la sécurité des télécommunications à recruter les personnes qui possèdent les compétences dont ils ont besoin.

Recommandation 24

Que le gouvernement du Canada, en collaboration avec les Forces armées canadiennes, se dote d'une capacité de mobilisation continue et qu'il en fasse usage.

Recommandation 25

Que le gouvernement du Canada mette sur pied un système permettant aux anciens combattants qui réintègrent la vie civile de conserver une autorisation de sécurité équivalente à celle qu'ils possédaient dans les Forces armées canadiennes, afin que leur habilitation de sécurité soit maintenue et que leur embauche au sein du ministère de la Défense nationale soit facilitée. Le gouvernement devrait également envisager un système permettant d'accélérer la délivrance d'habilitations de sécurité aux anciens combattants qui recherchent un emploi dans d'autres ministères fédéraux.

Recommandation 26

Que le gouvernement du Canada prenne des mesures pour bien définir les rôles et les responsabilités des Forces armées canadiennes et du Centre de la sécurité des télécommunications en matière de cybersécurité au Canada et à l'étranger.

Recommandation 27

Que le gouvernement du Canada prenne immédiatement des mesures pour remédier aux problèmes de soutien logistique au sein des Forces armées canadiennes et de leurs cyberforces.

Recommandation 28

Que le gouvernement du Canada assure la viabilité à long terme des cyberforces des FAC grâce à la création d'un programme de maintien en poste des cyberopérateurs et à la mise en place des cyberinfrastructures nécessaires.

Recommandation 29

Que le gouvernement du Canada tienne à jour le cadre juridique sur les interventions en cas de cyberattaques, qui comprend des lignes directrices en matière d'attribution, de réponse et de responsabilité.

Recommandation 30

Que le gouvernement du Canada collabore avec ses alliés pour actualiser les lois internationales, dont le Statut de Rome et la Convention de Genève, afin que la guerre cybernétique commanditée par l'État y soit considérée comme un crime de guerre.

Recommandation 31

Que le gouvernement du Canada adopte immédiatement toutes les recommandations qui n'ont pas encore été mises en œuvre parmi celles énoncées dans le Rapport 7 de la vérificatrice générale du Canada intitulé La cybersécurité des renseignements personnels dans le nuage, déposé au Parlement le 15 novembre 2022.

Recommandation 32

Que le gouvernement du Canada soumette à ses régimes de sanctions les particuliers et entités qui se livrent à la mésinformation, à la désinformation ou à la malinformation des Canadiennes et des Canadiens.

Recommandation 33

Que le gouvernement du Canada prenne des sanctions dissuasives contre les pays qui ont recours à des cybercriminels pour voler les fonds ou la propriété intellectuelle d'autrui, pour se livrer à la guerre de l'information ou pour mener d'autres activités malveillantes, ou qui tolèrent ces délits.

Recommandation 34

Que le gouvernement du Canada entreprenne un examen de sa politique de cyberdéfense et qu'il tienne des discussions bilatérales avec des pays alliés, comme les États-Unis, pour veiller à ce que les politiques en vigueur soient cohérentes et uniformes.

Recommandation 35

Que le gouvernement du Canada communique aux provinces le matériel pédagogique de la Finlande et de la Suède pour les civils au sujet de la guerre cognitive.

Recommandation 36

Que le gouvernement du Canada établisse des démarcations claires entre les activités du Centre de la sécurité des télécommunications se rapportant au renseignement électromagnétique et celles se rapportant à la cybersécurité, y compris les processus d'autorisation ministérielle et les mécanismes de déclaration.

Recommandation 37

Que le gouvernement du Canada se dote d'un ambassadeur en matière de cybersécurité.

ANNEXE A
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
Centre for International Governance Innovation	2023/02/07	48
Aaron Schull, directeur général et avocat général		
Wesley Wark, agrégé supérieur		
Centre de la sécurité des télécommunications	2023/02/07	48
Sami Khoury, dirigeant principal, Centre canadien pour la cybersécurité		
Alia Tayyeb, chef adjointe des renseignements électromagnétiques (SIGINT)		
À titre personnel	2023/02/10	49
Kristen Csenkey, doctorante, Balsillie School of International Affairs, Wilfrid Laurier University		
Thomas Keenan, professeur, University of Calgary		
Alexander Rudolph, doctorant, Department of Political Science, Carleton University		
Université du Québec à Montréal	2023/02/10	49
Alexis Rapin, chercheur en residence, Chaire Raoul-Dandurand en études stratégiques et diplomatiques		
À titre personnel	2023/02/14	50
Marcus Kolga, agrégé supérieur, Institut Macdonald-Laurier		
Ministère de la Défense nationale	2023/02/14	50
Cam Lou Carosielli, commandant de la Force cybernétique, Forces armées canadiennes		
Jonathan Quinn, directeur général, Politique de défense continentale		

Organismes et individus	Date	Réunion
À titre personnel Christian Leuprecht, professeur, Collège militaire royal du Canada	2023/03/10	53
Association des industries canadiennes de défense et de sécurité Christyn Cianfarani, présidente-directrice générale	2023/03/10	53
Sectigo Tim Callan, directeur de l'expérience client	2023/03/10	53
À titre personnel Tadej Nared, président du conseil d'administration, Slovenian Certified Ethical Hackers Foundation	2023/03/31	55
BlackBerry John de Boer, directeur principal, Affaires gouvernementales et politiques publiques, Canada	2023/03/31	55
Coalition pour la surveillance internationale des libertés civiles Tim McSorley, coordinateur national	2023/03/31	55

ANNEXE B
LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

Turnbull, John

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions nos 48, 49, 50, 53, 55, 63, et 64) est déposé.

Respectueusement soumis,

Le président,
L'hon. John McKay

Le Nouveau Parti démocratique soutient l'intention qui sous-tend le rapport du Comité permanent de la défense nationale sur la cybersécurité et la menace de cyberguerre. Les Canadiens s'inquiètent à juste titre de la menace que représentent les progrès de la cybertechnologie dans un contexte d'escalade des tensions mondiales. L'intelligence artificielle, la désinformation, les pirates informatiques parrainés par des États et les progrès en matière de stockage infonuagique entraînent des menaces uniques pour les Canadiens et nos infrastructures essentielles. C'est en tenant compte de ces menaces émergentes que le Comité permanent de la défense nationale a entamé notre étude, dans le but d'éclairer des réformes significatives qui protégeront les Canadiens.

Les néo-démocrates abordent la cybersécurité dans l'optique de protéger d'abord les Canadiens. Nous devons moderniser nos lois sur la cybersécurité afin de protéger les renseignements privés des Canadiens et les infrastructures essentielles dont nous dépendons. Nous devons veiller à ce que la Charte des droits à la vie privée des Canadiens soit protégée contre les acteurs hostiles et à ce que nos infrastructures essentielles soient efficacement défendues contre les attaques.

Plusieurs des recommandations que nous avons adoptées devraient être mises en œuvre immédiatement, notamment celles qui concernent l'élaboration d'une politique de cybersécurité plus souple et plus solide pour le gouvernement fédéral, les infrastructures essentielles et les réponses à la désinformation.

Cependant, le rapport du comité ne reflète pas adéquatement deux défis majeurs à notre politique de cybersécurité : le rôle croissant des monopoles sur nos infrastructures essentielles, et le manque de responsabilité des organismes de renseignement du Canada.

Le rôle des monopoles dans les infrastructures essentielles du Canada

En juillet dernier, plus de 12 millions de Canadiens ont perdu l'accès à l'internet et aux réseaux cellulaires. Le service *Interac* a été mis hors ligne, de nombreux organismes de transport public ont connu des pannes et de nombreux sites Web gouvernementaux n'étaient pas disponibles. Les Canadiens ont pris conscience de l'impact que pourrait avoir une attaque sur nos infrastructures essentielles.

Mais cette menace n'était pas posée par un acteur d'un État étranger; il s'agissait d'une défaillance interne des systèmes du géant des télécommunications Rogers. Si le Canada veut sérieusement se préoccuper de ses vulnérabilités en matière de cybersécurité, il doit aborder la question des monopoles croissants sur les infrastructures essentielles dans l'optique de la sécurité nationale. Le comité aurait pu bénéficier d'une remise en question de cette vulnérabilité.

En outre, tout au long des travaux du comité, nous avons longuement discuté du domaine des médias sociaux en ce qui concerne la désinformation provenant de l'étranger. Marcus Kolga, de l'Institut Macdonald-Laurier, nous a expliqué que la guerre cognitive est « un outil extrêmement important dans la trousse d'outils » de nos adversaires et qu'elle se fait souvent par la diffusion de la désinformation dans les médias sociaux.

Alors que nous avons longuement discuté de l'utilisation des médias sociaux comme domaine de guerre cognitive, le rapport du comité n'a pas abordé le rôle dangereux des géants des médias sociaux eux-mêmes. Wesley Wark, de l'Institut canadien pour l'innovation dans la gouvernance, a déclaré que « nous avons certainement besoin de restrictions qui encouragent davantage les entreprises de médias sociaux à utiliser le consentement. Je pense que le gouvernement du Canada a un rôle à jouer à cet égard en établissant des lignes directrices — aussi difficile que cela puisse être, car les plateformes géantes de médias sociaux n'aimeront pas cela. »

Les médias sociaux, en tant qu'espace où la désinformation provenant de l'étranger survient, sont entre les mains de quelques milliardaires qui poursuivent un capitalisme de surveillance. La volonté de ces milliardaires de monétiser les données des Canadiens produit des algorithmes avancés qui posent des menaces majeures pour la sécurité nationale, et le comité aurait bénéficié d'un examen plus approfondi de cette question.

Enfin, les néo-démocrates soutiennent l'intention derrière les recommandations 3 et 12, qui visent à renforcer les mesures de cybersécurité prises par les entrepreneurs avec le gouvernement fédéral. Alors que nos fonctionnaires travaillent avec diligence pour protéger la vie privée des Canadiens au quotidien, le gouvernement fait trop souvent appel à des entreprises privées qui ne respectent pas les mêmes normes. Deloitte, le principal bénéficiaire de l'externalisation des services du gouvernement, a connu de multiples atteintes aux données des consommateurs et des citoyens.

Les néo-démocrates ont évoqué l'exemple d'un incident survenu en 2017, lorsque Deloitte a subi une importante atteinte aux données qui a entraîné la fuite de mots de passe, d'adresses IP et de données identifiables dans le cadre d'un contrat avec le département américain de la Défense, le département de la Sécurité intérieure, le département d'État et l'Institut national de la santé. Les entreprises comme Deloitte doivent être tenues responsables lorsqu'elles ne respectent pas les pratiques exemplaires en matière de cybersécurité, et la sécurité des données canadiennes doit être prise en compte lors de l'externalisation.

La communauté du renseignement au Canada

À mi-chemin de cette étude, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement a publié une lettre adressée au commissaire de l'Agence du revenu du Canada (ARC), dans laquelle il lui demande d'ouvrir une enquête sur la Division de la revue et de l'analyse de l'ARC concernant l'islamophobie systémique dans les vérifications des organismes de bienfaisance musulmans.

Cette enquête a été déclenchée à la suite de révélations d'organisations telles que la Coalition pour la surveillance internationale des libertés civiles, selon lesquelles 75 % des organisations dont le statut d'organisme de bienfaisance a été révoqué à la suite de vérifications effectuées par la Division de la revue et de l'analyse étaient des organismes de bienfaisance musulmans.

Interrogé à ce sujet, Tim McSorley, de la Coalition pour la surveillance internationale des libertés civiles, a déclaré :

« L'Association des libertés civiles de la Colombie-Britannique a constaté dans ses recherches que le CST partageait des renseignements avec l'ARC afin de soutenir ses efforts de lutte contre le financement des activités terroristes. Cependant, nos recherches nous ont permis de constater que l'ARC, dans le cadre de ses efforts pour lutter contre le financement des activités terroristes, a adopté une approche préjudiciable à l'égard des organismes de bienfaisance musulmans au Canada. Elle est partie de l'idée qu'en raison des menaces terroristes émanant d'organismes liés aux musulmans, la communauté musulmane devait être davantage soupçonnée. Cela se traduit par une plus grande surveillance, une plus grande collecte et un plus grand partage de renseignements ainsi que des répercussions plus importantes par rapport à d'autres communautés au Canada ».

À la lumière de ce qui précède, le Nouveau Parti démocratique est préoccupé par les recommandations formulées par le comité en vue d'intégrer davantage la collaboration du Centre de la sécurité des télécommunications avec d'autres organismes gouvernementaux dans le cadre d'une surveillance significative.

Bien que nous soyons conscients qu'une approche pangouvernementale est nécessaire pour répondre aux besoins du Canada en matière de cybersécurité, les néo-démocrates se souviennent que le Canada a rejeté l'élargissement des pouvoirs des organismes de renseignement dans le cadre du projet de loi C-51 du gouvernement Harper. Nous sommes déçus de la décision du gouvernement libéral de maintenir ou d'élargir bon nombre de ces pouvoirs dans le cadre du projet de loi C-59. Comme nous l'avons vu avec le partage de renseignements entre les organismes de renseignement et l'Agence du revenu du Canada, le racisme systémique peut se manifester dans le maintien de l'ordre au sein des communautés marginalisées.

Comme nous l'ont expliqué Sami Khoury et Alia Tayyeb, du Centre de la sécurité des télécommunications, le CST a un double mandat : Établir et maintenir la cybersécurité pour le gouvernement fédéral et ses partenaires industriels, ainsi que le renseignement d'origine électromagnétique. Leur rôle dans la protection de la cybersécurité est essentiel au fonctionnement de notre gouvernement fédéral, mais nous sommes préoccupés par le fait que les limites entre ce rôle défensif et leur mandat en matière de renseignement d'origine électromagnétique sont floues.

Tim McSorley nous a dit que le CST ne « délimite pas adéquatement les deux types d'activités, bien que chacune d'entre elles nécessite un processus d'approbation différent ». Les néo-démocrates sont fermement convaincus qu'avant d'élargir le mandat du CST, nous devons délimiter clairement la frontière entre le renseignement d'origine électromagnétique et les opérations de cybersécurité.