CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

PRÊT À RELEVER LE DÉFI : RENFORCER LA POSTURE DE SÉCURITÉ DU CANADA PAR RAPPORT À LA RUSSIE

Rapport du Comité permanent de la sécurité publique et nationale

Ron McKinnon, président

MARS 2023
44e LÉGISLATURE, 1re SESSION

PRÊT À RELEVER LE DÉFI : RENFORCER LA POSTURE DE SÉCURITÉ DU CANADA PAR RAPPORT À LA RUSSIE

Rapport du Comité permanent de la sécurité publique et nationale

Le président
Ron McKinnon

MARS 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 DE LA SÉCURITÉ PUBLIQUE ET NATIONALE

PRÉSIDENT

Ron McKinnon

VICE-PRÉSIDENTES

Raquel Dancho

Kristina Michaud

MEMBRES

Paul Chiang

Pam Damoff

Iqwinder Gaheer

Peter Julian

Dane Lloyd

Glen Motz

Taleeb Noormohamed

Peter Schiefke

Doug Shipley

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Jim Carr

Kody Blois

Scot Davidson

Stephen Ellis

Michael Kram

Viviane Lapointe

Alistair MacGregor

Robert J. Morrissey

Kyle Seeback

Jake Stewart

Tako Van Popta

Karen Vecchio
Len Webber
Sameer Zuberi

GREFFIER DU COMITÉ

Simon Larouche

BIBLIOTHÈQUE DU PARLEMENT

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

Lyne Casavant
Allison Goody

LE COMITÉ PERMANENT
DE LA SÉCURITÉ PUBLIQUE ET NATIONALE

a l’honneur de présenter son

SEPTIÈME RAPPORT

Conformément au mandat que lui confère l’article 108(2) du Règlement, le Comité a étudié l'évaluation de la posture de sécurité du Canada par rapport à la Russie et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

AVANT PROPOS DU PRÉSIDENT

Comme le Comité regroupe des députés de partis différents, il arrive inévitablement que nous ne nous entendions pas sur les questions politiques dont nous sommes saisis. Toutefois, le rapport qui suit reflète nos inquiétudes et notre détermination, qui sont communes à tous les membres du Comité. Après des mois de travail, l'étude de la menace que représente la Russie pour la sécurité a fait ressortir la nature complexe et les nombreuses facettes des questions de sécurité nationale. Le Comité estime que ses recommandations peuvent renforcer la posture de sécurité du Canada pour répondre aux menaces.

Notre travail n'aurait pas été possible sans les précieuses observations de ceux qui ont comparu en tant que témoins devant le Comité ou qui ont soumis de la documentation. Le Comité tient à leur exprimer sa gratitude.

La majeure partie de cette étude a été réalisée sous la direction de l'honorable Jim Carr, qui est malheureusement décédé le 12 décembre 2022. Il a été notre président de décembre 2021 à septembre 2022. En tant qu'ancien ministre fédéral, parlementaire engagé et personnalité publique notable, il a guidé le Comité dans le cadre de cette étude importante et vaste. Il a su instaurer un climat à la fois sympathique et sérieux que le Comité est déterminé à conserver.

Le Comité aimerait dédier le présent rapport, qui est le fruit d'un travail collectif, à la mémoire de l'honorable Jim Carr.

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 continue :

- **d'imposer à la Russie des coûts élevés pour son agression contre l'Ukraine;**
- **d'appuyer la souveraineté, l'indépendance et l'intégrité territoriale de l'Ukraine;**
- **de collaborer avec ses alliés et ses partenaires pour défendre l'ordre international fondé sur des règles;**
- **d'accélérer les efforts de dissuasion et de défense pour combattre toute menace conventionnelle ou non conventionnelle à la sécurité nationale du Canada. 15**

Recommandation 2

Que le gouvernement du Canada travaille avec ses partenaires provinciaux et territoriaux pour créer et promouvoir des programmes de formation postsecondaire agréés dans le domaine de la cyberdéfense. 25

Recommandation 3

Que le gouvernement du Canada, en consultation avec les parties concernées, mise sur la Stratégie nationale de cybersécurité afin :

- **de faire en sorte que les propriétaires et exploitants d'infrastructures essentielles de toute taille disposent des spécialistes, de l'expertise et des ressources dont ils ont besoin en matière de cybersécurité pour faire face à une cyberattaque et s'en remettre;**

PRÊT À RELEVER LE DÉFI : RENFORCER LA POSTURE DE SÉCURITÉ DU CANADA PAR RAPPORT À LA RUSSIE

APERÇU

Introduction

Le 3 mars 2022, le Comité permanent de la sécurité publique et nationale de la Chambre des communes (le Comité) a adopté la motion ci-dessous :

> Que, conformément à l'article 108(2) du *Règlement*, le Comité commence immédiatement une étude des préparatifs d'urgence du Canada relativement aux diverses menaces que pose la Russie, y compris les menaces à la sécurité publique et la sécurité nationale du Canada et aux infrastructures essentielles du Canada (infrastructure physique et cyber infrastructure), à la prévalence et aux répercussions de la désinformation ainsi que la menace d'un recours à des activités d'espionnage ou de sabotage et d'un recours à des armes de destruction massive par la Russie[1].

Pour réaliser cette étude, le Comité a tenu huit réunions entre le 5 avril et le 6 octobre 2022 au cours desquelles il a reçu les témoignages d'un large éventail d'intervenants, y compris des universitaires et d'autres spécialistes, le ministre de la Protection civile, le ministre de la Sécurité publique, le chef d'état-major de la défense et la chef du Centre de la sécurité des télécommunications.

Le présent rapport contient les principales conclusions et les recommandations du Comité relativement à la posture de sécurité du Canada par rapport à la Russie. Il offre d'abord un aperçu du contexte dans lequel les travaux du Comité s'inscrivent. Il présente ensuite les principales préoccupations soulevées au sujet de la Russie pendant l'étude, à savoir : les cyberactivités malveillantes ciblant les infrastructures essentielles; les campagnes visant à propager de fausses informations et à perturber les systèmes démocratiques; la corruption à l'appui de l'agression; et les armes qui menacent la

1 Chambre des communes, Comité permanent de la sécurité publique et nationale (SECU), *Procès-verbal*, 3 mars 2022.

défense continentale. Il conclut par une analyse des vastes répercussions stratégiques d'un contexte de menace de plus en plus complexe.

Contexte

Guerre de la Russie contre l'Ukraine

Le 24 février 2022, la Russie a lancé une invasion à grande échelle de l'Ukraine. Le rassemblement de chars, de soldats, d'aéronefs et de missiles aux frontières de l'Ukraine, puis leur déploiement le long de multiples vecteurs d'attaque, témoignaient de l'intention manifeste de la Russie d'utiliser la force pour atteindre ses objectifs géopolitiques et de sa disposition à violer le droit international, ce qui a laissé planer des questions quant à la véritable portée des objectifs de la Russie.

Les longs mois de combat ont exposé les faiblesses des forces militaires conventionnelles de la Russie, notamment sur les plans de l'instruction, de la logistique et de l'intégration interarmes[2]. En septembre 2022, après la retraite forcée des unités russes face à la contre-offensive de l'Ukraine dans la région de Kharkiv, et alors qu'il annonçait la tenue de soi-disant « référendums » dans le territoire ukrainien occupé, le président Vladimir Poutine a déclaré que la Russie était prête à recourir à tous les systèmes d'armes à sa disposition si son intégrité territoriale était menacée[3]. Après avoir tenu cette rhétorique – largement interprétée comme faisant allusion à l'arsenal nucléaire de la Russie – Poutine a annoncé l'annexion des quatre régions ukrainiennes visées[4], une action dénoncée comme étant illégale par la communauté internationale[5]. D'ailleurs, la Russie ne détient pas tout le territoire ukrainien qu'elle revendique. Par exemple,

2 SECU, *Témoignages*, 6 octobre 2022, 1135 (Gén Wayne D. Eyre, chef d'état-major de la défense, Forces armées canadiennes, ministère de la Défense nationale). Au sujet des échecs observés sur le plan stratégique, le général Eyre a noté que « Leurs moyens et leurs ressources militaires ne sont pas à la hauteur de leurs objectifs politiques » [en parlant de la Russie]. Néanmoins, tout en soulignant qu'une très grande partie des forces terrestres de la Russie avaient été déployées aux fins de la guerre contre l'Ukraine, le général Eyre a indiqué que « il lui reste beaucoup d'autres forces ». Le général Eyre a rappelé que les forces aériennes, navales et stratégiques continuent de poser une menace.

3 « Read Putin's national address on a partial military mobilization », *The Washington Post*, 21 septembre 2022. Voir aussi Anton Troianovski, « With Annexation Plans, Putin Escalates Battle of Wills With the West », *The New York Times*, 29 septembre 2022.

4 Ann M. Simmons et Yuliya Chernova, « Russia Announces Annexation of Four Regions of Ukraine », *The Wall Street Journal,* 30 septembre 2022; et David E. Sanger, Anton Troianovski et Julian E. Barnes, « In Washington, Putin's Nuclear Threats Stir Growing Alarm », *The New York Times*, 1er octobre 2022.

5 Nations Unies, ONU Info, *Ukraine : L'Assemblée générale de l'ONU demande à la Russie de revenir sur sa « tentative d'annexion illégale » de quatre régions d'Ukraine*, 12 octobre 2022.

immédiatement après le discours de Poutine, les forces russes à Lyman, dans la région de Donestk, ont battu en retraite alors que la ville leur servait de centre logistique[6].

Au-delà du champ de bataille, la guerre menée par la Russie et les tactiques employées par celle-ci pour faire pression ont eu des ramifications à l'échelle mondiale. William Browder, président-directeur général d'Hermitage Capital Management Ltd, a expliqué au Comité que le régime de Poutine en Russie « militaris[e] tout ce qu'il peut militariser[7] ».

Au début de la guerre, les forces russes ont saisi la centrale nucléaire de Zaporijia en Ukraine, la plus grande en Europe. Les activités militaires près de la centrale suscitent d'importantes inquiétudes au sujet de la sûreté nucléaire[8]. Par ailleurs, la Russie a fait pression sur les marchés énergétiques, d'abord en réduisant les exportations de gaz vers les pays d'Europe, puis en fermant carrément le gazoduc Nord Stream 1[9]. La Russie a également utilisé la nourriture comme une arme. Bien qu'elle ait finalement accepté, en juillet 2022, un accord négocié par la Turquie et les Nations Unies en vue de l'établissement d'un corridor maritime[10], la Russie a empêché l'exportation de millions de tonnes de céréales en provenance de ports ukrainiens[11], ce qui a eu pour effet de faire grimper les prix déjà élevés de denrées alimentaires partout dans le monde.

Schéma de comportement

Bien que ces événements servent de toile de fond à la présente étude, le comportement et les intentions de la Russie suscitent des inquiétudes grandissantes depuis des années. En 2008, la Russie a fait la guerre à la Géorgie, puis, en 2014, elle a occupé la région de la Crimée en Ukraine et a entrepris de l'annexer, déstabilisant l'est de ce pays. Durant cette même période, la Russie mettait en œuvre un programme pluriannuel de modernisation de ses forces militaires. Or, la menace ne s'est pas limitée au contexte de

6 Voir Mary Ilyushina, Emily Rauhala et Isabelle Khurshudyan, « Ukraine hammers Russian forces into retreat on east and south fronts », *The Washington Post*,4 octobre 2022.

7 SECU, *Témoignages*, 17 mai 2022, 1200 (William Browder, président-directeur général, Hermitage Capital Management Ltd, à titre personnel).

8 Agence internationale de l'énergie atomique (AIEA), *Nuclear Safety, Security and Safeguards in Ukraine : 2nd Summary Report by the Director Genera, 28 avril – 5 septembre*; et AIEA, *Update 112 – IAEA Director General Statement on Situation in Ukraine*, 5 octobre 2022 [DISPONIBLES EN ANGLAIS SEULEMENT].

9 Max Seddon, David Sheppard et Henry Foy, « Russia switches off Europe's main gas pipeline until sanctions are lifted », *Financial Times*, 5 septembre 2022.

10 Nations Unies, ONU Info, *On vous explique pourquoi l'Initiative céréalière de la mer Noire est importante pour le monde*, 16 septembre 2022.

11 Matina Stevis-Gridneff, « Russia Agrees to Let Ukraine Ship Grain, Easing World Food Shortage », *The New York Times*, 23 juillet 2022.

politique étrangère. La Russie a aussi mené des campagnes hybrides conçues, semble-t-il, pour porter atteinte aux normes et aux systèmes démocratiques.

De multiples incidents ont mis en lumière ces campagnes. Aux États-Unis, la Central Intelligence Agency, le Federal Bureau of Investigation et la National Security Agency ont déterminé que le « président russe Vladimir Poutine avait ordonné en 2016 une campagne visant à influencer les élections présidentielles[12] », notamment des opérations sur les médias sociaux et du piratage informatique[13]. Ailleurs, le Canada et ses alliés ont déterminé en octobre 2019 que les unités cybernétiques du service de renseignement militaire russe avaient perpétré une vaste cyberattaque qui faisait « partie d'un effort prémédité du gouvernement russe visant à semer la discorde en prévision des élections parlementaires de la Géorgie[14] » prévues en 2020.

Il y a eu d'autres cibles et d'autres formes de perturbation dans le domaine cybernétique. En 2015 et en 2016, des acteurs parrainés par la Russie ont désactivé une partie du réseau de distribution d'électricité ukrainien[15]. En outre, le Canada et ses alliés ont déterminé que « des auteurs de menaces de la Russie sont responsables du développement de NotPetya », un maliciel qui s'est attaqué sans distinction à « des entités des secteurs financier, énergétique et gouvernemental et du secteur des infrastructures partout dans le monde en juin 2017[16] ».

D'autres cyberactivités malveillantes continuent d'être signalées. De concert avec des partenaires américains et autres, les ministres canadiens des Affaires étrangères, de la Défense nationale, de la Sécurité publique et de la Protection civile ont publié une déclaration en avril 2021 au sujet d'une « campagne de cyberespionnage russe qui a infiltré la plateforme Orion de SolarWinds[17] ». La chaîne d'approvisionnement de l'entreprise a été compromise par une porte dérobée insérée lors d'une mise à jour logicielle. La porte dérobée a permis l'installation d'autres logiciels malveillants dans les

12 États-Unis, Bureau du directeur du renseignement national, *Assessing Russian Activities and Intentions in Recent US Elections: Intelligence Community Assessment*, 6 janvier 2017, p. ii [TRADUCTION].

13 Le procureur spécial Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I of II*, département de Justice des États-Unis, mars 2019, p. 1.

14 Centre de la sécurité des télécommunications (CST), *Déclaration du CST sur les cyberactivités malveillantes menées par la Russie et ciblant la Géorgie*.

15 Centre canadien pour la cybersécurité, *Bulletin sur les cybermenaces : Les cyberattaques visant le secteur canadien de l'électricité*, fondée sur des informations en date du 29 septembre 2020.

16 CST, *Déclaration du CST concernant l'affaire du maliciel NotPetya*.

17 Affaires mondiales Canada, *Déclaration sur la cybercompromission de SolarWinds*, déclaration, 15 avril 2021.

réseaux d'un sous-groupe de clients de l'entreprise[18]. Les réseaux de plus d'une centaine d'entités canadiennes ont ainsi été compromis, ce qui a nécessité « des activités d'atténuation coûteuses et pourrait avoir sapé la confiance du public à l'égard du téléchargement de mises à jour logicielles[19] ». Selon le Canada, le groupe APT29, alias « The Dukes » ou « Cozy Bear », était à l'origine de cette activité malveillante[20]. La déclaration précisait que le groupe opérait très certainement « dans le cadre d'activités des services de renseignements russes[21] », qui avaient aussi ciblé des installations canadiennes de recherche et développement du vaccin contre la COVID-19 en 2020[22].

Au début de 2022, le Centre canadien pour la cybersécurité, qui fait partie du Centre de la sécurité des télécommunications Canada (CST), a publié deux bulletins, exhortant les exploitants d'infrastructures essentielles du pays à mieux prendre conscience des menaces, à surveiller activement leurs réseaux et à mettre en place des mesures d'atténuation pour contrer les cyberactivités malveillantes parrainées par la Russie[23]. En avril 2022, à la suite de l'invasion de l'Ukraine par la Russie, les autorités responsables de la cybersécurité au Canada, aux États-Unis, en Australie, au Royaume-Uni et en Nouvelle-Zélande ont publié un bulletin de sécurité conjoint indiquant que « les organisations responsables des infrastructures essentielles partout dans le monde sont plus susceptibles d'être ciblées par des auteurs de menaces persistantes avancées (MPA) parrainés par la Russie, par leurs mandataires et par des groupes cybercriminels indépendants[24] ». Ce bulletin faisant état de diverses menaces, comme le déploiement d'attaques par rançongiciel ou par déni de service distribué visant à perturber ou à

18 Affaires mondiales Canada, *Cybercompromission de la plateforme de SolarWinds*, document d'information.

19 Affaires mondiales Canada, *Déclaration sur la cybercompromission de SolarWinds*, déclaration, 15 avril 2021.

20 *Ibid*.

21 *Ibid*.

22 Affaires mondiales Canada, *Déclaration sur les cyberactivités malveillantes de la Russie qui touchent l'Europe et l'Ukraine*, Déclaration, 10 mai 2022.

23 Centre canadien pour la cybersécurité, *Bulletin sur les cybermenaces : Le CCC exhorte les exploitants des infrastructures essentielles du Canada à prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et à prendre des mesures d'atténuation contre celles-ci*, 26 janvier 2022; et Centre canadien pour la cybersécurité, *Bulletin sur les cybermenaces, le CCC rappelle aux exploitants des infrastructures essentielles du Canada de prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et de prendre des mesures d'atténuation contre celles-ci*, 13 février 2022.

24 Centre canadien pour la cybersécurité, *Bulletin de cybersécurité conjoint sur les cybermenaces criminelles et parrainées par la Russie qui planent sur les infrastructures essentielles*, 20 avril 2022.

endommager des fonctions de technologies opérationnelles ou de systèmes de contrôle industriels essentiels[25].

Dans l'ensemble, la Russie suscite de plus grandes inquiétudes parce qu'elle n'a montré aucune hésitation à violer les règles internationales reconnues. L'attentat à l'agent neurotoxique perpétré en 2018 contre un ancien agent double et sa fille à Salisbury, au Royaume-Uni, a été attribué à des agents des services du renseignement russes, et on estime que cette opération a « très certainement été approuvée à un niveau élevé de décision gouvernementale[26] ». Jeffrey Mankoff, chercheur émérite de la National Defense University, a indiqué au Comité que cette opération et la tentative précédente d'empoisonnement au polonium d'un transfuge des services de sécurité russes, elle aussi perpétrée en sol britannique, « témoignent d'une volonté manifeste de recourir non seulement à la violence, mais aussi de franchir les limites internationalement reconnues concernant l'utilisation d'armes chimiques et radiologiques[27] ».

MENACES ASSOCIÉES À LA RUSSIE

Évaluation de la menace globale à la sécurité nationale du Canada

Le comportement perturbateur de la Russie est désormais bien établi, surtout dans le cyberespace, et il préoccupe surtout les pays européens à proximité. Le Comité a entendu différents points de vue en ce qui concerne la nature et la gravité de la menace que fait peser directement la Russie sur le Canada, plus particulièrement la sécurité publique et nationale de notre pays. Certains intervenants estiment que la Russie présente manifestement un danger, mais d'autres ont laissé entendre qu'il s'agit d'un danger à long terme qu'il faut situer dans le contexte de menace et le cadre géopolitique en général.

Robert Huebert, professeur associé du Département de sciences politiques à l'Université de Calgary, a déclaré que « la Russie est une menace existentielle pour le Canada et que cette menace s'accroît ». Il a fait remarquer que Poutine s'efforce de « reconstituer l'empire russe » et de protéger son régime depuis le début de sa présidence à la fin de 1999. Selon M. Huebert, le fait que la Russie soit prête à recourir à ses propres méthodes de guerre (ou « processus de guerre multidomaines ») pour atteindre ses

25 *Ibid*.

26 Premier ministre du Canada, Justin Trudeau, *Déclaration commune entre les dirigeants français, allemand, américain, canadien et britannique sur l'attaque à Salisbury*, 6 septembre 2018.

27 SECU, *Témoignages*, 17 mai 2022, 1205 (Jeffrey Mankoff, chercheur universitaire émérite, National Defense University, à titre personnel).

objectifs « la place sur une trajectoire de collision directe avec l'OTAN [Organisation du Traité de l'Atlantique Nord][28] ».

Charles Burton, agrégé supérieur du Centre for Advancing Canada's Interests Abroad à l'Institut Macdonald-Laurier, estime que la menace que représente la Russie pour la sécurité publique et nationale du Canada a « considérablement augmenté » depuis que les pays occidentaux ont réagi à l'invasion de l'Ukraine en imposant des sanctions à la Russie et en fournissant des armes à l'Ukraine. Amer et en colère, Poutine a la capacité de lancer de « dangereuses attaques contre le Canada en représailles » et, de l'avis de M. Burton, il est « fort possible qu'il fasse front commun avec la Chine, ce qui aggravera la menace[29] » à laquelle fait face le Canada.

David Perry, président de l'Institut canadien des affaires mondiales, estime que la Russie « défie les intérêts canadiens et occidentaux en de nombreux endroits du monde et avec de nombreux moyens différents, y compris les cyberattaques et la désinformation ». Il est d'avis que la guerre contre l'Ukraine montre que « la Russie est prête à utiliser son armée modernisée sans provocation, d'une manière fondamentalement contraire aux intérêts et aux valeurs du Canada et que nous avons du mal à comprendre au Canada[30] ».

Jonathan Paquin, professeur titulaire du Département des sciences politiques à l'Université Laval, a également fait référence à des données qui laissent entendre que la Russie « est une menace à la sécurité de notre pays », entre autres les cyberattaques répétées de la Russie contre les infrastructures essentielles de pays qu'elle juge hostile. Puisque « le Canada est actuellement très hostile aux intérêts de Moscou », notre pays est « potentiellement une cible de choix pour le Kremlin », a indiqué M. Paquin, qui a aussi mentionné le financement par la Russie de campagne de désinformation et les menaces nucléaires qu'elle a proférées depuis son invasion de l'Ukraine. Il a conseillé au Canada et à ses alliés de redoubler de vigilance « maintenant que les pays occidentaux ont revu à la hausse leurs objectifs dans le conflit ukrainien et qu'ils cherchent

28 SECU, *Témoignages*, 5 avril 2022, 1110 (Robert Huebert, professeur associé, Département de sciences politiques, Université de Calgary, à titre personnel).

29 SECU, *Témoignages*, 3 mai 2022, 1135 (Charles Burton, agrégé supérieur, Centre for Advancing Canada's Interests Abroad, Institut Macdonald-Laurier, à titre personnel).

30 SECU, *Témoignages*, 5 avril 2022, 1220 (David Perry, président, Institut canadien des affaires mondiales, à titre personnel).

ouvertement à affaiblir les capacités de la Russie[31] ». M. Paquin a recommandé que le Canada utilise une double stratégie pour accroître sa sécurité : la dissuasion fondée sur la possibilité de représailles (par sa participation à l'OTAN) et la dissuasion par le déni (c.-à-d. cyberrésilience, éducation et « défense continentale renouvelée[32] »).

Malgré les menaces du recours à la force nucléaire proférées par la Russie, comme moyen de dissuasion, Jeffrey Mankoff a noté que la Russie préférera sans doute utiliser des outils de perturbation et des armes non conventionnelles à sa disposition en raison de la « faiblesse relative » de ses forces militaires conventionnelles. Il estime que le danger de telles attaques « ne fera que croître à mesure que les relations avec Moscou se détérioreront et que Poutine sera de plus en plus désespéré par les pertes russes en Ukraine ». Selon lui, tout en continuant à appuyer l'Ukraine, le Canada et ses alliés au sein de l'OTAN « doivent tous rester attentifs à la possibilité que la Russie franchisse des limites que l'on croyait jusque-là infranchissables ». D'après cette analyse, les pays doivent adopter une posture sans « timidité », qui est axée sur « la préparation et la prudence[33] ».

Pour sa part, James Fergusson, directeur adjoint du Centre d'étude sur la défense et la sécurité à l'Université du Manitoba, estime que la menace ne date pas du 24 février 2022 et ne devrait pas nécessairement déclencher un sentiment de panique au Canada. Bien que la guerre de la Russie contre l'Ukraine ait certainement « aiguisé l'attention », il a affirmé que « ces vulnérabilités existent depuis longtemps ». Nonobstant l'adversité entre la Russie et l'Occident, M. Fergusson est d'avis que la situation actuelle n'est pas « une nouvelle guerre froide » et qu'il y a « d'autres problèmes et d'autres menaces qui doivent être pris en compte pour tenter de répondre à la partie russe de cette équation[34] ».

Décrivant la réponse du Canada à l'agression russe, l'honorable Bill Blair, ministre de la Protection civile, a informé le Comité que le gouvernement travaille sans relâche pour imposer des coûts élevés à la Russie, tout en demeurant « à l'affût de toutes les menaces russes potentielles à l'intérieur du Canada et concernant les intérêts des

31 SECU, *Témoignages*, 3 mai 2022, 1250 (Jonathan Paquin, professeur titulaire, Département de science politique, Université Laval, à titre personnel). M. Paquin a plus tard observé que « [s]i la Russie […] devait perdre la guerre ou si la Russie ne devait pas être en mesure de gagner dans l'Est et dans le Sud du pays, il y a fort à parier qu'il y aura des mesures de représailles, et que, essentiellement, les Russes ne maintiendront pas le statu quo ». Voir *ibid*., 1310.

32 SECU, *Témoignages*, 3 mai 2022, 1250 (Jonathan Paquin).

33 SECU, *Témoignages*, 17 mai 2022, 1205 (Jeffrey Mankoff).

34 SECU, *Témoignages*, 5 avril 2022, 1105 (James Fergusson, directeur adjoint, Centre d'étude sur la défense et la sécurité, Université du Manitoba, à titre personnel).

Canadiens partout dans le monde[35] ». Il a souligné que les organismes de sécurité nationale du Canada exercent une « vigilance accrue » à l'égard de « toute forme d'ingérence, y compris en matière de cybersécurité, qui pourrait avoir lieu au pays[36] ».

Bien qu'elles soient au cœur de la présente étude, les menaces émanant de la Russie ne sont pas la seule source de préoccupation du point de vue stratégique. Andrea Charron, directrice et professeure agrégée du Centre d'études pour la défense et la sécurité à l'Université du Manitoba, a souligné que la Russie représente « une grave menace pour l'Amérique du Nord », mais a rappelé que « la Chine est le concurrent à long terme des États-Unis, dont l'hégémonie est décroissante[37] ».

Dans son témoignage, le général Wayne D. Eyre, chef d'état-major de la défense des Forces armées canadiennes, a offert un point de vue géopolitique plus large :

> Nous nous trouvons de nouveau dans un monde chaotique et dangereux où de grandes puissances, notamment la Russie et la Chine, sont déterminées à refaire l'ordre mondial pour parvenir à leurs fins et où les droits et libertés des États plus petits et moins puissants sont éliminés[38].

Ce qu'il faut tirer de cette affirmation, c'est qu'il s'agit d'une confrontation entre l'idée d'un ordre international fondé sur des règles et celle d'un ordre fondé sur la puissance, et qu'il faut donc réagir en conséquence[39]. Or, le général Eyre a déclaré que l'ordre fondé sur les règles « qui sous-tend depuis des générations la stabilité mondiale et, en effet, notre prospérité nationale, est maintenant incertain ». Notre tâche, a-t-il déclaré, est de défendre cet ordre[40].

Compte tenu de ce qui précède, le Comité recommande :

Recommandation 1

Que le gouvernement du Canada continue :

35 SECU, *Témoignages*, 2 juin 2022, 1100 (L'hon. Bill Blair, ministre de la Protection civile).

36 *Ibid*., 1155.

37 SECU, *Témoignages*, 7 avril 2022, 1205 (Andrea Charron, directrice et professeure agrégée, Centre d'études pour la défense et la sécurité, Université du Manitoba, à titre personnel).

38 SECU, *Témoignages*, 6 octobre 2022, 1100 (Gén Wayne D. Eyre).

39 *Ibid*.

40 *Ibid*., 1105.

- **d'imposer à la Russie des coûts élevés pour son agression contre l'Ukraine;**
- **d'appuyer la souveraineté, l'indépendance et l'intégrité territoriale de l'Ukraine;**
- **de collaborer avec ses alliés et ses partenaires pour défendre l'ordre international fondé sur des règles;**
- **d'accélérer les efforts de dissuasion et de défense pour combattre toute menace conventionnelle ou non conventionnelle à la sécurité nationale du Canada.**

Cyberactivités malveillantes et infrastructures essentielles

Enjeux

Il est ressorti des témoignages que les cybermenaces provenant de la Russie sont celles qui risquent le plus de porter atteinte à la sécurité publique et nationale du Canada, en particulier dans le contexte des infrastructures essentielles. Le terme infrastructure essentielle, qui désigne « l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que l'efficacité du gouvernement[41] », souligne en soi à quel point ces infrastructures sont importantes, sans compter que la plupart sont facilitées par la technologie informatique. Les infrastructures essentielles sont présentes dans de multiples secteurs : énergie, services publics, alimentation, etc. D'ailleurs, dans la Stratégie nationale sur les infrastructures essentielles, le gouvernement du Canada reconnaît que leur perturbation « pourrait se traduire en pertes de vie et en effets économiques néfastes[42] ».

D'ailleurs, Errol Mendes, professeur de droit constitutionnel et international à l'Université d'Ottawa, estime que les alliés doivent travailler ensemble pour produire des cyberavertissements, comme les bulletins publiés par le CST avant l'invasion de l'Ukraine par la Russie concernant la protection des infrastructures essentielles, et les présenter comme de graves violations du droit international. On pourrait aussi faire mention du

41 Sécurité publique Canada, *Stratégie nationale sur les infrastructures essentielles*.

42 *Ibid*.

droit humanitaire international si les cyberattaques mettent un grand nombre de vies en danger, par exemple celles ciblant les hôpitaux ou les réserves d'eau[43].

Cyberacteurs et cibles multiples

Dans le cyberespace, les dimensions liées à la sécurité nationale sont complexes, car les menaces ne proviennent pas seulement d'État et ne se limitent pas à des cibles gouvernementales. Jennifer Quaid, directrice exécutive d'Échange canadien de menaces cybernétiques, a rappelé au Comité que ce sont à la fois « les États-nations qui utilisent Internet pour se livrer à des activités d'espionnage et d'action politique, et les criminels qui utilisent la cybercriminalité à des fins lucratives[44] ». Caroline Xavier, chef du CST, a signalé que la cybercriminalité « est la menace la plus courante et la plus répandue contre les Canadiens et les entreprises canadiennes », ajoutant que « les programmes de cyberopérations parrainés par des États, notamment la Chine, la Corée du Nord, l'Iran et la Russie, représentent les menaces stratégiques les plus importantes pour le Canada[45] ». Parmi les cybermenaces étrangères, mentionnons les tentatives ciblant des exploitants d'infrastructures essentielles ainsi que leurs technologies opérationnelles et d'information[46].

Plusieurs facteurs font en sorte qu'il est difficile de protéger les infrastructures essentielles contre les cyberattaques et de renforcer la cyberrésilience. James Fergusson a rappelé que contrairement au secteur de la défense, qui est dominé par le gouvernement, l'infrastructure essentielle du Canada « est en grande partie entre les mains du secteur privé[47] ». En fait, David A. Etkin, professeur de gestion des catastrophes et des urgences à l'Université York, a indiqué que « 85 % des infrastructures essentielles du Canada appartiennent au secteur privé[48] ».

Il faut aussi tenir compte de facteurs structurels lorsque l'on compare les domaines de la défense et de l'informatique. En ce qui concerne les menaces touchant l'aérospatiale et

43 SECU, *Témoignages*, 17 mai 2022, 1210 (Errol Mendes, professeur, Droit constitutionnel et international, Université d'Ottawa, à titre personnel).

44 SECU, *Témoignages*, 3 mai 2022, 1140 (Jennifer Quaid, directrice exécutive, Échange canadien de menaces cybernétiques).

45 SECU, *Témoignages*, 6 octobre 2022, 1110 (Caroline Xavier, chef, Centre de la sécurité des télécommunications).

46 *Ibid*.

47 SECU, *Témoignages*, 5 avril 2022, 1105 (James Fergusson).

48 SECU, *Témoignages*, 7 avril 2022, 1100 (David A. Etkin, professeur, Disaster and Emergency Management, Université York, à titre personnel).

le domaine maritime, le partenariat de défense entre le Canada et les États-Unis repose sur le Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD)[49]. M. Fergusson a fait remarquer qu'il n'existe aucune structure équivalente « pour coordonner les réponses à d'éventuelles cyberattaques russes, que ce soit pour des motifs d'espionnage ou pour tenter de saper ou de saboter des infrastructures essentielles[50] ». Les témoins ont aussi fait valoir qu'il serait important de renforcer la capacité transfrontalière de gestion des urgences. Donnant l'exemple d'une cyberattaque contre l'industrie automobile à Detroit, Juliette Kayyem, maître de conférences en sécurité internationale, chaire d'enseignement Belfer à la Kennedy School of Government de l'Université Harvard, a noté qu'il faudrait essentiellement traiter la situation comme une intervention « sans frontières[51] ».

Il est difficile de bien se préparer en raison de l'éventail de cibles pouvant faire l'objet de cyberactivités malveillantes. Caroline Xavier a mentionné au Comité que les exploitants d'infrastructures essentielles et les grandes entreprises sont les « cibles les plus profitables » pour les cybercriminels[52]. Le Comité a toutefois également entendu que les petites et moyennes entreprises sont vulnérables, car elles ont moins de ressources à leur disposition et une moins grande expertise en matière de cybersécurité pour relever les menaces et se remettre d'un incident. Jennifer Quaid a signalé que 44 % des petites entreprises membres de son organisation n'ont « aucune forme de cyberdéfense » et que 60 % n'ont pas d'assurance[53]. Au sujet de la menace liée aux cyberacteurs russes, Ken Barker, professeur de l'Institute for Security, Privacy, and Information Assurance à l'Université de Calgary, a observé qu'il est peu probable que les petites et moyennes entreprises « soient une cible spécifique de la Russie, à moins qu'elles fassent partie de certains secteurs de cybersécurité ou qu'elles soient des fournisseurs d'infrastructures essentielles[54] ».

---

49 Défense nationale, *Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD)*, document d'information.

50 SECU, *Témoignages*, 5 avril 2022, 1105 (James Fergusson).

51 SECU, *Témoignages*, 7 juin 2022, 1240 (Juliette Kayyem, maître de conférences en sécurité internationale, chaire d'enseignement Belfer, Kennedy School of Government, Université Harvard, à titre personnel).

52 SECU, *Témoignages*, 6 octobre 2022 (Caroline Xavier).

53 SECU, *Témoignages*, 3 mai 2022, 1155 (Jennifer Quaid).

54 SECU, *Témoignages*, 7 juin 2022, 1205 (Ken Barker, professeur, Institute for Security, Privacy, and Information Assurance, Université de Calgary, à titre personnel).

Capacités bien établies

Les témoins ont parlé des cybercapacités de la Russie, tant celles associées à l'État que celles d'acteurs non étatiques, et des activités malveillantes attribuées à la Russie, comme on le résume au début du présent rapport.

Selon Christian Leuprecht, professeur au Collège militaire royal du Canada de l'Université Queen, l'attaque SolarWinds montre que la Russie, la Chine et une poignée d'autres ont les moyens de se livrer délibérément à des exploits ciblés[55]. De même, David Shipley, directeur général de Beauceron Security, a fait savoir au Comité que la capacité de la Russie de recourir à la technologie et de contrôler les dommages est « bien documentée » et que la menace n'est pas seulement théorique. « Les cyberattaques des gangs criminels russes ont porté préjudice aux municipalités canadiennes, aux organismes de soins de santé et plus, et ont coûté des dizaines de millions de dollars[56] », a-t-il déclaré.

Or, d'après les témoignages, les cyberactivités de la Russie depuis l'invasion de l'Ukraine n'ont pas été aussi destructrices que certains observateurs le craignaient, et il n'y a pas eu non plus de montée de ces activités. D'importantes cyberopérations ont eu lieu, ciblant le gouvernement, les forces militaires, les fonctions économiques et les infrastructures de l'Ukraine[57]. Or, comme l'a fait remarquer M. Barker, il n'y a pas eu, depuis le début de la guerre, de hausse du nombre d'« attaques du jour zéro », c'est-à-dire d'attaques d'origine inconnue ou d'attaques ciblant des vulnérabilités qui n'étaient pas connues[58].

Selon Nora Cuppens, professeure à Polytechnique Montréal, peut-être que la Russie était mal préparée ou encore peut-être qu'elle attend le « bon moment » pour amorcer une cyberguerre[59]. Autre hypothèse : « [L]e déclenchement d'une cyberattaque massive par l'un des deux camps serait sans doute vu comme un franchissement de la fameuse

---

55 SECU, *Témoignages*, 17 mai 2022, 1120 (Dr. Christian Leuprecht, professeur, Collège militaire royal du Canada, Université Queen, à titre personnel).

56 SECU, *Témoignages*, 7 juin 2022, 1215 (David Shipley, directeur général, Beauceron Security).

57 Il y a eu des cyberincidents ailleurs qu'en Ukraine, y compris une opération ayant perturbé une grande partie du réseau européen de communications par satellite KA-SAT de Viasat. Voir Centre canadien pour la cybersécurité, *Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie*, fondé sur les informations disponibles au 22 juin 2022. Le bulletin précise également que dès « janvier 2022, du renseignement en pleine évolution indiquait que des auteurs de cybermenace de la Russie exploraient les possibilités de contre-attaques visant les États-Unis, le Canada et d'autres pays de l'OTAN et de la collectivité des cinq, y compris leurs infrastructures essentielles ».

58 SECU, *Témoignages*, 7 juin 2022, 1205 (Ken Barker).

59 SECU, *Témoignages*, 3 mai 2022, 1240 (Nora Cuppens, professeure, Polytechnique Montréal, à titre personnel).

ligne rouge, ce qui conduirait inévitablement à une escalade conflictuelle[60]. » De l'avis de Juliette Kayyem, la meilleure explication à ce jour pourrait être la suivante : « [T]out comme la capacité militaire, nous avons surestimé la cybercapacité de destruction de la Russie par rapport à sa capacité de créer des perturbations, des perturbations que nous pouvons gérer[61]. » Il se pourrait aussi que l'invocation de l'article relatif à la sécurité collective par l'OTAN en ce qui concerne tout attaque contre des infrastructures essentielles qui a des répercussions sur des civils, ait « apporté de la discipline[62] ».

Accroître la résilience et renforcer l'expertise

L'honorable Marco Mendicino, ministre de la Sécurité publique, a dit au Comité que les cyberattaques ciblant des systèmes qui assurent le bon fonctionnement des infrastructures essentielles du Canada « sont […] une préoccupation de tous les instants[63] ». Sécurité publique Canada travaille avec d'autres organismes au sein du gouvernement et à l'échelle internationale « afin de dénoncer les États ou les acteurs parrainés par un État lorsqu'il est possible de leur attribuer en toute confiance la responsabilité d'une cyberactivité malveillante[64] ». Au sujet des efforts déployés au Canada, le ministre Mendicino a mentionné le cadre établi par la Stratégie nationale de cybersécurité, qui fait l'objet d'un examen en vue de son renouvellement[65], et a souligné le rôle du Centre canadien pour la cybersécurité, qui fournit des conseils techniques. Il a également indiqué que la Gendarmerie royale du Canada (GRC) dispose maintenant d'une unité qui dirige les opérations policières contre les cybercriminels[66].

Tout en reconnaissant les mesures prises à ce jour par le gouvernement, les témoins ont mentionné ce que le Canada peut faire davantage, selon eux, pour renforcer la cyberrésilience et mieux se préparer à la gestion des urgences en général.

Certains témoins ont abordé la question des compétences, des connaissances et de la recherche. M. Etkin était d'avis que le Canada gagnerait à avoir « un centre national

60 *Ibid*.

61 SECU, *Témoignages*, 7 juin 2022, 1210 (Juliette Kayyem).

62 *Ibid*.

63 SECU, *Témoignages*, 9 juin 2022, 1105 (L'hon. Marco Mendicino, ministre de la Sécurité publique).

64 *Ibid*.

65 Voir Sécurité publique Canada, *Un Canada numérique sûr et prospère : Consultation concernant l'approche adoptée par le Canada en matière de cybersécurité*.

66 Voir Gendarmerie royale du Canada (GRC), *Le Groupe national de coordination contre la cybercriminalité (GNC3)*.

interdisciplinaire d'excellence spécialisé dans l'étude des catastrophes ». Il a informé le Comité que les « interconnexions » entre les infrastructures essentielles ne sont pas bien comprises. Il a d'ailleurs recommandé le financement d'une étude à long terme visant à examiner « les interconnexions et les vulnérabilités des infrastructures essentielles du Canada[67] ».

En ce qui a trait à la cybersécurité, M. Barker a déclaré que la « grave pénurie » de spécialistes constitue l'un des principaux enjeux[68]. Frédéric Cuppens, professeur à Polytechnique Montréal, a insisté sur l'importance de mettre sur pied non seulement des programmes menant au baccalauréat et à la maîtrise, mais aussi à des certificats, ainsi que des microprogrammes et des programmes de perfectionnement professionnel continu. Du point de vue de la recherche, il estimait qu'il devrait y avoir plus de travaux sur « l'arme cybernétique comme arme de dissuasion[69] ». La recherche devrait aborder des questions comme l'attribution des cyberattaques, la surveillance des menaces internes dans le contexte des infrastructures ciblées, la mesure de l'effet réel d'une cyberattaque et la cyberrésilience[70].

D'autres thèmes importants sont ressortis de l'étude, notamment le signalement des cyberincidents et la mise en œuvre de normes sur la cybersécurité. Outre les obligations découlant de la *Loi sur la protection des renseignements personnels et les documents électroniques*, BlackBerry a souligné dans son mémoire qu'il n'existe au Canada aucun règlement « exigeant – et encore moins obligeant – les propriétaires et exploitants d'éléments d'infrastructure critique à signaler les incidents relatifs à la cybersécurité, à s'y préparer ou à les prévenir[71] ». Alors que les administrations portuaires et les exploitants d'installations maritimes ou de services de traversiers sont tenus par la réglementation de signaler tout cyberincident aux organismes d'application de la loi et à Transports Canada, ces obligations « ne sont pas assorties de périodes de référence précises, et ne contiennent aucune ligne directrice sur les mesures de sécurité devant être mises en place[72] ».

---

67 SECU, *Témoignages*, 7 avril 2022, 1100 (David A. Etkin).

68 SECU, *Témoignages*, 7 juin 2022, 1205 (Ken Barker).

69 SECU, *Témoignages*, 3 mai 2022, 1245 (Frédéric Cuppens, professeur, Polytechnique Montréal, à titre personnel).

70 *Ibid*.

71 BlackBerry, mémoire, 15 juin 2022, p. 1.

72 *Ibid*.

En réponse à une question à ce sujet, la chef du CST, Caroline Xavier, a expliqué la pratique actuelle :

> Nous travaillons également de façon étroite avec des organisations qui nous rapportent avoir été victimes de cyberattaques. Cependant, comme vous l'avez dit, plusieurs organisations ne le signalent pas. Nous continuons tout de même à en discuter ouvertement avec les industries.
>
> Nous organisons beaucoup de séances d'information et de sensibilisation visant à les informer du fait que nous sommes là pour leur offrir le soutien nécessaire. Nous publions aussi beaucoup de bulletins d'information pour leur expliquer les risques, afin qu'elles se protègent et qu'elles préviennent les attaques possibles.
>
> Cela nous inquiète, évidemment[73].

Elle a précisé que bien des pays éprouvent ce problème[74].

Dans son mémoire, BlackBerry signale que le gouvernement américain avait pris des mesures à la suite de cyberincidents ayant ciblé des infrastructures essentielles aux États-Unis, y compris un décret présidentiel exigeant « des mesures de prévention comme la mise en œuvre du modèle à vérification systématique dans toutes les agences gouvernementales américaines, et le renforcement de la sécurité de la chaîne d'approvisionnement du pays et des logiciels du gouvernement[75] ». De plus, conformément à la *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (Loi de 2022 sur le signalement des cyberincidents touchant les infrastructures essentielles), les exploitants d'infrastructures essentielles aux États-Unis seront tenus de « signaler aux autorités tout cyberincident les touchant dans les 72 heures, et dans les 24 heures s'il s'agit d'une attaque par rançongiciel[76] ». Toujours d'après BlackBerry, l'Union européenne a imposé des exigences semblables aux propriétaires et exploitants d'infrastructures essentielles. La directive en question « prévoit des amendes allant

---

73 SECU, *Témoignages*, 6 octobre 2022, 1125 (Caroline Xavier).

74 *Ibid*.

75 BlackBerry, mémoire, 15 juin 2022, p. 2. Pour plus de contexte, voir États-Unis, Maison-Blanche, *Executive Order on Improving the Nation's Cybersecurity*, 12 mai 2021; et Executive Office of the President, Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies*, 26 janvier 2022. Le modèle « zéro confiance » représente un changement d'approche, qui est passé de la vérification du périmètre à une vérification systématique de chaque utilisateur, appareil, application et transaction.

76 BlackBerry, mémoire, 15 juin 2022, p. 2. Les règles obligatoires doivent être élaborées avant l'entrée en vigueur des exigences en matière de signalement prévues dans la loi. Voir États-Unis, Cybersecurity & Infrastructure Security Agency, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*.

jusqu'à 10 millions d'euros ou 2 % du revenu annuel (selon le plus élevé de ces montants) en cas de non-conformité[77] ».

Frédéric Cuppens a parlé des obligations mises en place en France. Dans ce pays, les entreprises menant des activités dans un secteur essentiel sont désignées des « opérateurs d'importance vitale », et ont « l'obligation […] de mettre en place un certain nombre d'obligations pour être en conformité avec [la] loi de programmation militaire » du pays. Il précisé que cette exigence s'applique non seulement aux grandes entreprises, mais « aussi [aux] petites ou moyennes entreprises à partir du moment où l'une de ces entreprises exerce des activités en lien avec un secteur d'activités critique[78] ».

Sur ce point, David Shipley était d'avis que le Canada est « en retard par rapport aux États-Unis et à l'Europe[79] ». Il a recommandé fortement que l'on rende obligatoire le signalement des cyberincidents, non seulement dans le cas des industries sous réglementation fédérale, mais aussi pour « les soins de santé ainsi que les chaînes d'approvisionnement vitales, y compris les secteurs manufacturiers et alimentaires ». M. Shipley a expliqué que la plupart des organisations ne communiquent pas volontairement au gouvernement fédéral ces incidents, car leurs services juridiques et de gestion du risque ou leur assureur leur disent que ce genre de collaboration offre des « gains limités » et peut entraîner « beaucoup de pertes[80] ».

Michael Doucet, directeur exécutif du Bureau du chef de la sécurité de l'information chez Optiv Canada, a préconisé une approche s'appliquant à « certains intervenants des infrastructures critiques ». Après avoir fait remarquer la vaste portée des dix secteurs d'infrastructures essentielles au Canada, il a expliqué pourquoi il préférait une approche nuancée : « Allons-nous exiger une déclaration obligatoire de la part d'un producteur laitier possédant un troupeau de 60 bêtes[81]? »

De l'avis de M. Doucet, si l'on décide d'imposer cette obligation, il sera important de protéger les informations communiquées et les mesures prises, et ce tout en trouvant

77 BlackBerry, mémoire, 15 juin 2022, p. 2. Pour plus de contexte, voir la Commission européenne, *La Commission se félicite de l'accord politique relatif à de nouvelles règles en matière de cybersécurité des réseaux et des systèmes d'information*, communiqué, 13 mai 2022.

78 SECU, *Témoignages*, 3 mai 2022, 1320 (Frédéric Cuppens).

79 SECU, *Témoignages*, 7 juin 2022, 1215 (David Shipley).

80 *Ibid*.

81 SECU, *Témoignages*, 3 mai 2022, 1225 (Michael Doucet, directeur exécutif, Bureau du chef de la sécurité de l'information, Optiv Canada Federal).

un moyen de partager les connaissances à l'échelle du pays. « Nous voulons tout d'abord éviter que l'information communiquée par les organisations qui signalent des bris de sécurité soit réacheminée là où il ne faut pas », a-t-il indiqué, soulignant qu'une « fois ces renseignements regroupés, cela fait beaucoup d'information[82] ».

Jennifer Quaid, quant à elle, estime que le gouvernement pourrait faciliter la communication d'information en adoptant des lois « d'exonération » conçues pour encourager les entreprises et les organisations à partager volontairement des renseignements au-delà des exigences législatives « en les protégeant contre les répercussions juridiques[83] ».

Un autre point a été soulevé, celui de la nature volontaire des normes de cybersécurité. David Shipley aimerait que l'on impose des pratiques exemplaires en matière de cybersécurité à l'échelle nationale. Qualifiant d'« excellent début » Cybersécuritaire Canada – le programme de certification à l'intention des petites et moyennes organisations – il a soutenu que « la participation volontaire sera toujours faible ». Selon lui, il y a des leçons à tirer de programmes britanniques en vertu desquels les marchés publics ne sont ouverts qu'à ceux qui respectent des normes de bases en matière de cybersécurité[84].

Donnant l'exemple de l'Agence nationale de la sécurité des systèmes d'information en France, Nora Cuppens a recommandé la création d'une « institution semblable » au Canada, qui opérationnaliserait « la protection de nos systèmes et de nos infrastructures ». En plus d'assurer une cybersurveillance, une telle institution, selon la vision de M^{me} Cuppens, « pousserait la réglementation et […] vérifierait que les règles sont appliquées[85] ».

Enfin, concernant la résilience et l'expertise, il importe de tenir compte de la capacité en matière de cybersécurité des autres intervenants, non seulement celle du gouvernement fédéral et des grandes entreprises, comme on l'a déjà mentionné. Selon David Shipley, les entités du secteur subnational au Canada ont besoin de « fonds dédiés du gouvernement fédéral pour améliorer leur sécurité le plus rapidement possible ». Il a ajouté que dans le secteur privé, les petites et moyennes entreprises « ont désespérément besoin d'aide

82 *Ibid*.

83 SECU, *Témoignages*, 3 mai 2022, 1140 (Jennifer Quaid).

84 SECU, *Témoignages*, 7 juin 2022, 1215 (David Shipley).

85 SECU, *Témoignages*, 3 mai 2022, 1305 (Nora Cuppens).

pour se procurer les outils de sécurité dont elles ont besoin dans un environnement de plus en plus hostile[86] ».

Aaron Shull, directeur général, Centre pour l'innovation dans la gouvernance internationale, a noté que le CST a déjà établi des contrôles de base en cybersécurité pour les petites et moyennes organisations[87]. Il a suggéré que, si les entreprises appliquaient ces contrôles de base, « il y a de fortes chances qu'elles n'aient pas de problèmes, parce qu'aucun auteur de menaces au niveau de l'État ne s'en prendrait à une petite entreprise, surtout si elle est difficile à infiltrer. Cela n'en vaut tout simplement pas la peine[88] ». Malgré tout, M. Shull a déclaré au Comité que la plupart des entreprises ne l'ont pas encore fait. Pour les encourager, il a suggéré d'envisager « la possibilité d'offrir un genre de crédit d'impôt[89] ».

Compte tenu de la menace que font peser les cyberactivités malveillantes sur les intérêts nationaux du Canada, y compris les services sur lesquels les Canadiens comptent pour assurer leur sécurité et leur bien-être, le Comité convient qu'il est temps d'imposer le signalement des cyberincidents graves touchant les infrastructures essentielles et qu'il faudra porter une attention particulière à la gestion de cette obligation. Après un examen attentif de tous les témoignages reçus concernant les problèmes que représentent les cyberactivités malveillantes et la protection de l'infrastructure essentielle, le Comité recommande :

Recommandation 2

Que le gouvernement du Canada travaille avec ses partenaires provinciaux et territoriaux pour créer et promouvoir des programmes de formation postsecondaire agréés dans le domaine de la cyberdéfense.

Recommandation 3

Que le gouvernement du Canada, en consultation avec les parties concernées, mise sur la Stratégie nationale de cybersécurité afin :

86 SECU, *Témoignages*, 7 juin 2022, 1215 (David Shipley).

87 Pour obtenir plus d'information, voir Centre canadien pour la cybersécurité, *Introduction aux contrôles de base*.

88 SECU, *Témoignages*, 17 mai 2022, 1120 (Aaron Shull, directeur général, Centre pour l'innovation dans la gouvernance internationale).

89 *Ibid*.

- **de faire en sorte que les propriétaires et exploitants d'infrastructures essentielles de toute taille disposent des spécialistes, de l'expertise et des ressources dont ils ont besoin en matière de cybersécurité pour faire face à une cyberattaque et s'en remettre;**

- **de s'assurer que les normes de cybersécurité sont respectées et font l'objet de rapports.**

Recommandation 4

Que le gouvernement du Canada ordonne au Centre de la sécurité des télécommunications d'élargir l'éventail d'outils utilisés pour sensibiliser les petites et moyennes entreprises à la nécessité d'adopter des normes de cybersécurité.

Recommandation 5

Que le gouvernement du Canada instaure des mesures incitatives – entre autres choses une déduction pour amortissement accéléré ou d'autres mesures fiscales – destinées aux petites et moyennes entreprises pour les encourager à procéder aux investissements nécessaires pour appliquer les contrôles de cybersécurité de base établis par le Centre de la sécurité des télécommunications.

Recommandation 6

Que le gouvernement du Canada exige que les exploitants d'infrastructures essentielles de secteurs désignés se préparent à faire face à des cyberincidents, les préviennent et les signalent, qu'il mette en place des délais pour le signalement des incidents graves, des services d'assistance technique et des mesures de protection de l'information signalée au Centre de la sécurité des télécommunications, qui aurait pour mandat de partager les leçons apprises avec l'industrie, et qu'il soumette au Parlement des rapports annuels sur ces efforts.

Assurer une réponse coordonnée, cohérente et efficace

Dans son évaluation de la posture de sécurité du Canada en général, Wesley Wark, agrégé supérieur au Centre pour l'innovation dans la gouvernance internationale, a indiqué que la capacité de notre pays de se défendre contre les cyberattaques ou les tentatives qui menacent nos infrastructures constitue une « menace de haut niveau[90] ».

90 SECU, *Témoignages*, 17 mai 2022, 1105 (Wesley Wark, agrégé supérieur, Centre pour l'innovation dans la gouvernance internationale).

Le Comité a également appris qu'une douzaine de ministères et organismes ont des responsabilités en matière de cybersécurité[91]. Par exemple, le CST, qui a notamment pour mandat d'agir à titre d'« autorité technique nationale du Canada en matière de cybersécurité[92] », rend compte au ministre de la Défense nationale, alors que le « dirigeant principal pour la cybersécurité » est Sécurité publique Canada[93].

Outre ce que prévoient les instruments stratégiques en place, le ministre Mendicino a indiqué que le sous-ministre de la Sécurité publique joue le « rôle de président d'une tribune qui réunit différents fonctionnaires de tout le gouvernement », le but étant « de mettre en commun l'information, de coordonner les efforts, de repérer les menaces et de déterminer la meilleure façon d'instaurer des stratégies d'atténuation[94] ». Il a reconnu qu'il est important de poursuivre ces efforts afin « d'éviter une forme de cloisonnement, qui peut mener à la fragmentation d'une réponse coordonnée[95] ». Soulignant que les États-Unis ont créé le poste de directeur de la cybersécurité nationale à la Maison-Blanche, BlackBerry a proposé dans son mémoire que le Canada « réfléchi[sse] à l'établissement d'un poste, au sein du Cabinet, de responsable de la coordination et des mesures gouvernementales en matière de cybersécurité[96] ».

Le Comité estime qu'il faudrait, en guise de premier pas, procéder à un examen de l'appareil gouvernemental et des responsabilités en matière de cybersécurité afin de s'assurer qu'il n'y a pas de failles ou lacunes dans la préparation ou la défense du Canada.

Compte tenu de ce qui précède, le Comité recommande :

Recommandation 7

Que le gouvernement du Canada veille à ce que les rôles, responsabilités et structures en matière de cybersécurité à l'échelle du gouvernement fédéral optimisent la cohérence, la

91 BlackBerry, mémoire, 15 juin 2022, p. 7.

92 SECU, *Témoignages*, 6 octobre 2022, 1105 (Caroline Xavier). Le CST, soit l'organisme national du renseignement électromagnétique, exerce conformément à la loi un mandat comportant cinq volets : le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives, les cyberopérations actives et l'assistance technique et opérationnelle.

93 Sécurité publique Canada, *Cybersécurité au gouvernement fédéral du Canada*.

94 SECU, *Témoignages*, 9 juin 2022, 1130 (L'hon. Marco Mendicino).

95 *Ibid*.

96 BlackBerry, mémoire, 15 juin 2022, p. 7.

coordination et la prise de mesures en temps opportun dans le domaine de la cybersécurité, et qu'il soumette au Parlement des rapports annuels sur ces efforts.

Recommandation 8

Que le gouvernement du Canada insiste sur l'importance et la modernisation de la cybersécurité dans les mandats de ses ministères.

Recommandation 9

Que le gouvernement du Canada explore les options pour la création d'une structure canado-américaine de commandement de la cyberdéfense.

Désinformation

Plusieurs témoins ont parlé des opérations d'information de la Russie et plus particulièrement de la propagation de désinformation. Ils ont exprimé des vues semblables au sujet des méthodes utilisées et des objectifs de ces opérations, mais ont offert des perspectives différentes quant aux conséquences et aux mesures de lutte à prendre.

Tactiques et intentions de la Russie

Marcus Kolga, agrégé supérieur à l'Institut MacDonald-Laurier, a expliqué que les méthodes de guerre de l'information employée par la Russie sont le fruit de l'expertise acquise par l'Union soviétique durant la Guerre froide. Il a affirmé que le président Poutine, un ancien agent du renseignement, « a rétabli la guerre cognitive il y a 20 ans, comme principal outil pour réprimer son propre peuple, miner les démocraties occidentales et venir à bout de la cohésion au sein de l'alliance de l'OTAN[97] ».

Selon M. Kolga, les objectifs de Poutine en ce qui concerne la guerre cognitive sont « pour la plupart indépendants de toute idéologie générale, mais ils concordent avec son appui aux groupes d'extrême gauche et d'extrême droite[98] ». Pour polariser les sociétés, des questions sensibles sont ciblées et amplifiées dans le cadre d'un « processus complexe de blanchissage de l'information par la Russie », notamment par les médias

97 SECU, *Témoignages*, 7 avril 2022, 1210 (Marcus Kolga, agrégé supérieur, Institut MacDonald-Laurier, à titre personnel).

98 *Ibid*.

d'État russes et une « constellation de groupes et de plateformes qui agissent de façon interposée, y compris ici même au Canada, et régurgitent cette information[99] ».

D'après Ahmed Al-Rawi, professeur adjoint à l'Université Simon Fraser, le gouvernement russe « a un intérêt constant à s'ingérer dans la politique canadienne en utilisant une gamme d'opérations d'information, de propagande et de désinformation[100] ». Après avoir examiné des ensembles de données rendues publiques par Facebook et Twitter il y a quelques années, M. Al-Rawi a déterminé que « les trolls russes étaient les plus investis dans le ciblage du Canada, bien plus que les trolls iraniens et les autres trolls d'État de la Chine et de l'Arabie saoudite[101] ». Il estime que ces opérations d'information ont non seulement pour but de semer la discorde et de créer des tensions, mais aussi de « confondre les gens sur le vrai ou le faux[102] ».

L'éventail des plateformes et des méthodes de communication utilisées est très problématique. Anciennement connu sous le nom « Russia Today », RT, qui est le bureau de presse appuyé par l'État, a été rayé de la liste des services de programmation et des stations autorisés à distribuer des services de radiodiffusion au Canada[103]. Or, Veronica Kitchen, professeure agrégée du Département des sciences politiques à l'Université de Waterloo, a affirmé que, malgré cette décision, la campagne de désinformation de la Russie est « toujours présente sur les médias sociaux et dans les forums fréquentés par les adeptes d'autres genres de complots populistes[104] ».

M. Al-Rawi a souligné l'activité sur les médias sociaux des missions diplomatiques russes, précisant que celles-ci sont le « principal vecteur de diffusion de la propagande » sur les plateformes des médias sociaux[105]. À son avis, la présence diplomatique russe en ligne sert à militariser les pratiques de vérification des faits. Il a ajouté que l'ambassade de la Russie « tente de créer avec le public canadien un lien direct que le [Conseil de la

99 *Ibid*.

100 SECU, *Témoignages*, 5 avril 2022, 1210 (Ahmed Al-Rawi, professeur adjoint, Université Simon Fraser, à titre personnel). Le gouvernement définit la désinformation comme suit : « une information délibérément fausse ». Voir gouvernement du Canada, *Les efforts du Canada pour contrer la désinformation - Invasion russe de l'Ukraine*.

101 SECU, *Témoignages*, 5 avril 2022, 1210 (Ahmed Al-Rawi).

102 *Ibid*.

103 Conseil de la radiodiffusion et des télécommunications canadiennes, *Décision de radiodiffusion CRTC 2022-68*, 16 mars 2022.

104 SECU, *Témoignages*, 5 avril 2022, 1115 (Veronica Kitchen, professeure agrégée, Département des sciences politiques, Université de Waterloo, à titre personnel).

105 SECU, *Témoignages*, 5 avril 2022, 1210 (Ahmed Al-Rawi).

radiodiffusion et des télécommunications canadiennes] ne peut bloquer », notamment sous la forme de messages directs[106].

Établissant un contraste entre les mesures prises par des alliés de l'OTAN et des partenaires de l'Union européenne, qui ont expulsé plus de 500 fonctionnaires russes de leur territoire depuis l'invasion de l'Ukraine, Wesley Wark a fait remarquer le gouvernement canadien « n'a encore pris aucune mesure » pour chasser les agents du renseignement russes du pays. Il est d'avis que le « [l]e Canada doit prendre des mesures fermes pour contrer les activités d'espionnage et d'ingérence de la Russie[107] ».

Conséquences de la désinformation

Les témoins n'étaient pas tous du même avis au sujet de l'incidence des opérations de désinformation russes et de la menace qu'elles représentent pour la sécurité nationale et publique du pays. James Fergusson n'est « pas de ceux qui croient que la désinformation russe, la désinformation chinoise ou les campagnes de désinformation de quiconque ont vraiment un effet » et estime que la menace est « beaucoup monté[e] en épingle et exagéré[e][108] ». En revanche, M. Al-Rawi a indiqué que l'on ne comprend pas encore l'influence de la désinformation russe sur la population canadienne et qu'on ne l'a pas encore quantifié[109].

Selon Veronica Kitchen, « [l]es campagnes de désinformation russes relient l'invasion de l'Ukraine à QAnon et à d'autres théories de complot de l'État profond qui alimentent les crimes haineux et la méfiance à l'égard du gouvernement canadien[110] ». Soulignant que « les adeptes de ces théories du complot sont susceptibles de commettre des actes violents », elle a rappelé au Comité que « l'action politique des partisans de l'extrémisme populiste peut aussi avoir des effets néfastes qui ne se transforment pas en menace pour la sécurité ou en crime[111] ». Selon elle, « seul un petit nombre de Canadiens sera attiré par ces idées et influencé par la désinformation russe[112] ». Elle a toutefois signalé que ces idées sont « facilement amplifiées par les robots » (soit les programmes qui

106 *Ibid*.

107 SECU, *Témoignages*, 17 mai 2022, 1105 (Wesley Wark).

108 SECU, *Témoignages*, 5 avril 2022, 1105 (James Fergusson).

109 SECU, *Témoignages*, 5 avril 2022, 1235 (Ahmed Al-Rawi).

110 SECU, *Témoignages*, 5 avril 2022, 1115 (Veronica Kitchen).

111 *Ibid*.

112 *Ibid*.

agissent automatiquement sur les plateformes Internet), un problème qui nécessite sans doute la mise en place de solutions à long terme[113].

Christian Leuprecht a affirmé que l'« information erronée et la désinformation diffusées par les Russes sur les plateformes de médias sociaux de source ouverte compromettent les forces de police et le gouvernement au pouvoir[114] ».

Compte tenu de ces témoignages, le Comité recommande :

Recommandation 10

Que le gouvernement du Canada cherche à déterminer la pleine étendue des activités de désinformation russes – et des campagnes parrainées par d'autres États – qui ciblent le Canada, ainsi que les intervenants, les méthodes, les messages et les plateformes en jeu, de même que les répercussions de la désinformation sur la population canadienne et la sécurité nationale du pays, et qu'il rende compte chaque année de ses constatations au Parlement.

Comment réagir

Si l'objectif général des opérations de désinformation russes est clair, on ne peut en dire autant sur la manière la plus efficace de les combattre.

D'après M. Al-Rawi, « la meilleure façon de protéger les Canadiens est de discréditer la désinformation et de vérifier les faits pour tout ce qui touche au Canada, aux Canadiens et à la guerre en Ukraine[115] ». Paul Goode, titulaire de la chaire d'études russes McMillan à l'Université Carleton, a également insisté sur l'importance de l'éducation et de la formation. Étant donné que la désinformation « joue généralement sur des caractéristiques ou des thèmes émotifs », il estime que « le fait d'y répondre de façon objective, de façon réfléchie, est peut-être la façon la plus efficace de la contrer, parce

113 *Ibid*.

114 SECU, *Témoignages*, 17 mai 2022, 1100 (Christian Leuprecht).

115 SECU, *Témoignages*, 5 avril 2022, 1240 (Ahmed Al-Rawi). Le gouvernement du Canada publie « un échantillon » de désinformation russe au sujet de l'Ukraine, les fausses déclarations étant comparées avec les faits. Voir gouvernement du Canada, *Contrer la désinformation par des faits - L'invasion russe de l'Ukraine*.

que la répression généralisée n'est pas une réaction démocratique à ce genre de menace[116] ».

Reconnaissant que la connaissance des médias puisse aider dans certains cas, M[me] Kitchen jugeait essentiel que l'on travaille avec les entreprises privées et les alliés du Canada « pour améliorer nos réponses technologiques à la désinformation[117] ». À titre de pas dans la bonne direction, elle a mentionné la création récente par le gouvernement d'un groupe consultatif sur la sécurité en ligne[118] et la formation du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections[119]. Selon elle, la réglementation « devient utile » pour se débarrasser des robots, et il serait bien de collaborer avec les entreprises qui sont ouvertes à l'idée d'« essayer de freiner l'extrémisme » sur leur plateforme[120].

Aaron Shull a fait écho à ces commentaires dans ses conseils au Comité, qui étaient de mettre l'accent sur l'« amplification ». Étant donné que « 39 % du trafic Internet provient de robots malveillants[121] », il a suggéré que l'on s'efforce de couper les fonds qui servent à alimenter ce trafic automatisé (autrement dit de faire en sorte qu'il soit plus difficile pour les trolls qui contrôlent les « robots malveillants » d'être payés[122]). Sur ce point, il a donné l'exemple des sanctions imposées à la Russie depuis l'invasion de l'Ukraine. M. Shull a également parlé de l'architecture technique de l'Internet, soulignant qu'il est possible de s'attaquer aux « grandes fermes de robots » à l'aide du système de noms de domaine. On pourrait également définir ce que sont des « robots malveillants » à l'échelle internationale et prendre des mesures pour en restreindre le flux[123].

D'autres témoins ont insisté sur les responsabilités des plateformes de services numériques. Conscient des questions de liberté d'expression risquant d'être soulevées,

---

116 SECU, *Témoignages*, 7 avril 2022, 1135 (Paul Goode, titulaire de la chaire d'études russes McMillan, Université Carleton, à titre personnel).

117 SECU, *Témoignages*, 5 avril 2022, 1115 (Veronica Kitchen).

118 Voir Patrimoine canadien, « Groupe consultatif d'experts », *L'engagement du gouvernement en faveur de la sécurité en ligne*.

119 Voir gouvernement du Canada, *Protection de la démocratie*. Le ministre Blair a informé le Comité qu'il n'avait reçu aucune information indiquant que la Russie était impliquée dans un quelconque effort d'ingérence étrangère dans les élections fédérales de 2021. Voir SECU, *Témoignages*, 2 juin 2022, 1110 (L'hon. Bill Blair).

120 SECU, *Témoignages*, 5 avril 2022, 1155 (Veronica Kitchen).

121 SECU, *Témoignages*, 17 mai 2022, 1100 (Aaron Shull).

122 *Ibid*., 1130.

123 *Ibid*., 1100.

Errol Mendes a encouragé le Canada à examiner ce que propose l'Union européenne, qui envisage d'imposer à ces plateformes la responsabilité de « procéder à des évaluations annuelles et à des vérifications indépendantes et, en fin de compte, d'étayer ces mesures par un cadre réglementaire pouvant donner lieu à des amendes massives[124] ».

En plus de réitérer les recommandations relatives à la sécurité numérique contenues dans son rapport sur l'extrémisme violent à caractère idéologique[125], le Comité recommande ce qui suit :

Recommandation 11

Que le gouvernement du Canada, en collaboration avec ses alliés et ses partenaires canadiens, continue à exposer et à contrecarrer les campagnes de désinformation russes et celles soutenues par des États étrangers ciblant les Canadiens.

Recommandation 12

Que le gouvernement du Canada travaille avec des experts, des fournisseurs de services Internet, des plateformes de médias sociaux et des partenaires internationaux pour lutter contre les robots en ligne qui amplifient la désinformation parrainée par des États, et qu'il présente dans un rapport au Parlement ses observations et les mesures qui ont été prises.

Un autre outil a été proposé : appuyer les voix indépendantes. Paul Goode a encouragé le Canada à « accueillir des universitaires, des journalistes et des militants qui sont la cible de persécutions en raison de leur opposition à la guerre russe ». À son avis, la diaspora russe doit être « une alliée et non seulement une spectatrice », et il s'agit d'une cause qui peut être avancée « en offrant un refuge aux chefs de file moraux et intellectuels de la Russie[126] ».

Alexander Cooley, professeur de science politique, lauréat du prix Claire Tow au Barnard College, et membre auxiliaire du corps professoral de Chatham House, a également attiré l'attention du Comité sur les personnes qui ont quitté la Russie par suite de la guerre contre l'Ukraine. Il a mentionné que les bureaux de presse russes indépendants s'efforcent de mener leurs activités à partir des États baltiques ou sur Telegram, que les travailleurs du domaine de la technologie de l'information se sont réfugiés entre autres

124 SECU, *Témoignages*, 17 mai 2022, 1210 (Errol Mendes).

125 SECU, *La montée de l'extrémisme violent à caractère idéologique au Canada*, Sixième rapport, juin 2022.

126 SECU, *Témoignages*, 7 avril 2022, 1105 (Paul Goode).

en Géorgie, en Arménie et en Ouzbékistan, et que des chercheurs et des analystes « cherchent […] de nouveaux types d'affiliations et de ports d'attache universitaires ». Selon lui, il est possible d'améliorer et de renforcer ces nouveaux réseaux « qui tentent de promouvoir une pensée indépendante et d'influer, dans la mesure où ils peuvent le faire depuis l'extérieur, sur la propagande de désinformation à l'intérieur » de la Russie. Les politiques à l'appui de ces efforts auraient pour but de « faire de nous un multiplicateur de forces au moment où le Kremlin tente de se dissocier de l'Ouest, pour faire en sorte que ces voix indépendantes et critiques puissent être encouragées depuis l'extérieur du pays[127] ».

Compte tenu de ce qui précède, le Comité recommande :

Recommandation 13

Que le gouvernement du Canada soutienne les journalistes et les universitaires russes indépendants et les aide à exposer la propagande et la désinformation diffusée par le régime.

Richesse tirée de la répression

Quelques témoins ont discuté de la recherche accumulée par les personnes aux échelons supérieurs du régime de Poutine, plus particulièrement du point de vue de la mise en œuvre des sanctions.

Depuis 2014, en réponse à l'agression de la Russie contre l'Ukraine, le gouvernement du Canada a imposé des sanctions à plus de 370 entités et plus de 1 600 personnes conformément à la *Loi sur les mesures économiques spéciales*[128]. D'autres mesures ont été prises de concert avec les alliés du Canada afin d'imposer des restrictions relatives à des biens et des technologies de pointe, ainsi que sur les services[129]. Le gouvernement fédéral a également déposé un projet de loi visant à modifier la *Loi sur l'immigration et*

127 SECU, *Témoignages*, 5 avril 2022, 1215 (Alexander Cooley, professeur de science politique lauréat du prix Claire Tow, Barnard College, et membre auxiliaire du corps professoral, Chatham House, à titre personnel).

128 Gouvernement du Canada, *Sanctions – Invasion russe de l'Ukraine*, consulté le 7 février 2023.

129 *Ibid*.

la protection des réfugiés afin d'interdire l'entrée au Canada à tout étranger visé par des sanctions en vertu de la *Loi sur les mesures économiques spéciale*[130].

Aux termes de la *Loi sur les mesures économiques spéciales*, le commissaire de la GRC peut fournir son assistance en matière de saisie ou de blocage d'un bien se trouvant au Canada – qui appartient à un État étranger, à une personne qui s'y trouve ou à un de ses ressortissants qui ne réside pas habituellement au Canada ou qui est détenu ou contrôlé, même indirectement, par lui – lorsqu'un décret a été émis à cet effet par le gouverneur en conseil[131]. De plus, toute personne au Canada et tout Canadien à l'étranger est tenu de communiquer à la GRC « l'existence des biens qui sont en sa possession ou sous son contrôle et qu'il soupçonne d'être la propriété ou sous le contrôle d'une personne désignée[132] ». Dans le cadre de son rôle en matière de collecte d'information, la GRC a déclaré le 23 décembre 2022 que, depuis le 24 février 2022, des avoirs au Canada d'une valeur approximative de 122 millions de dollars avaient été efficacement gelés et que des transactions financières équivalent à environ 291 millions de dollars avaient été bloqués conformément au règlement sur la Russie pris en application de la *Loi*[133].

William Browder, qui a fait campagne à l'échelle internationale en faveur de l'imposition de sanctions ciblées (lois « Magnitsky ») contre les auteurs de violations des droits de la personne, a qualifié d'« impressionnantes » les sanctions variées imposées à la suite de l'invasion de l'Ukraine par la Russie dans le but « de paralyser l'effort de guerre de Vladimir Poutine[134] ». Malgré ces résultats, il estime que le montant gelé n'est pas suffisant. Selon lui, depuis 2000, Poutine et les autres membres de l'élite russe « ont volé 1 billion de dollars à la Russie et cet argent les attend à l'Ouest ». Les montants bloqués

---

130 SECU, *Témoignages*, 9 juin 2022, 1105 (L'hon. Marco Mendicino); Agence des services frontaliers du Canada, *Le gouvernement interdira aux Russes sanctionnés d'entrer au Canada*, communiqué de presse, 17 mai 2022; et Projet de loi S-8, Loi modifiant la Loi sur l'immigration et la protection des réfugiés, apportant des modifications corrélatives à d'autres lois et modifiant le Règlement sur l'immigration et la protection des réfugiés, 44e législature, 1re session. Au moment où le Comité mettait la dernière main au présent rapport, le projet de loi S-8 avait été étudié par le Sénat et était à l'étape de la deuxième lecture à la Chambre des communes.

131 *Loi sur les mesures économiques spéciales (L.C. 1992, ch. 17)*, paragraphes 4(1) et 6.2(1).

132 GRC, *Mise à jour de la déclaration des avoirs gelés en vertu de la Loi sur les mesures économiques spéciales visant la Russie*, déclaration, 23 décembre 2022. Dans ce contexte, le terme « personne désignée » signifie une personne ou une entité assujettis à un gel des actifs ou à des interdictions de mener des opérations (sanctions) aux termes de la *Loi sur les mesures économiques spéciales, L.C. 1992, ch. 17* et du *Règlement sur les mesures économiques spéciales visant la Russie (DORS/2014-58)*.

133 GRC, *Mise à jour de la déclaration des avoirs gelés en vertu de la Loi sur les mesures économiques spéciales visant la Russie*, déclaration, 23 décembre 2022.

134 SECU, *Témoignages*, 17 mai 2022, 1200 (William Browder).

grâce aux sanctions ne représentent qu'« une partie minuscule, de minimis, de l'argent qui a été siphonné hors de Russie[135] ». La différence s'explique par les tactiques utilisées pour contourner les sanctions. M. Browder a expliqué que les individus visés par des sanctions ont employé différentes méthodes et structures – telles que des sociétés portefeuille, des membres de leur famille et des dépositaires – pour bien cacher leur argent[136].

Dans son témoignage, Alexander Cooley a également abordé la question de ces oligarques russes, soulignant qu'ils forment des réseaux transnationaux qui « trouvent des échos dans les sociétés occidentales[137] ». En plus de traiter des difficultés liées au gel des actifs, il a laissé entendre qu'il serait bon de se pencher sur les réputations. À ce sujet, M. Cooley a attiré l'attention du Comité sur les « professionnels des services » des pays occidentaux qui acceptent l'argent des oligarques et « le placent dans des biens immobiliers de luxe, achètent des sociétés-écrans et cachent l'argent dans des réseaux complexes de comptes bancaires[138] », ajoutant qu'il y a également des agences de relations publiques, des cabinets de gestion de la réputation et des lobbyistes « qui tentent de les faire passer non pas pour des personnes politiquement exposées ayant des liens avec le Kremlin, mais pour des philanthropes mondiaux[139] ».

De l'avis de M. Cooley, « [l]a mise en place d'un registre fédéral de la propriété bénéficiaire est absolument essentielle sur le plan de la sécurité nationale[140] ». Ces registres ont pour but de consigner des informations sur les personnes physiques qui, dans les faits, possèdent ou contrôlent une société (c'est-à-dire les personnes qui en sont véritablement les propriétaires bénéficiaires) plutôt que sur la propriété légale, qui peut être rattachée à une fiducie ou à une autre société[141]. M. Cooley a soulevé ce point, car il estime que « [t]out les pays doivent savoir qui sont ces sociétés fictives anonymes et qui se cache derrière pour acquérir des biens immobiliers de luxe et d'autres biens[142] ».

---

135 *Ibid*.

136 *Ibid*.

137 SECU, *Témoignages*, 5 avril 2022, 1215 (Alexander Cooley).

138 *Ibid*.

139 *Ibid*.

140 *Ibid*., 1300.

141 Innovation, Sciences et Développement économique Canada, *Consultations publiques sur le renforcement de la transparence de la propriété effective des sociétés au Canada : Ce que nous avons entendu*, 6 avril 2021.

142 SECU, *Témoignages*, 5 avril 2022, 1300 (Alexander Cooley).

M. Browder a proposé une approche spécifiquement axée sur le rôle joué par les professionnels des services dont il a été question plus haut. Il a suggéré que l'on modifie les dispositions législatives relatives aux sanctions afin de préciser que toute firme de services professionnels « qui ont fourni de l'information, donné des conseils ou qui ont été consultés relativement à une société de portefeuille et à la structuration des avoirs d'un oligarque qui a été sanctionné par le gouvernement canadien à dévoiler et à expliquer tout renseignement en leur possession relativement à cette personne ». Cette obligation aurait pour effet de transformer ces professionnels en « lanceurs d'alerte[143] ».

Le Comité est conscient de la complexité des questions juridiques, stratégiques et d'application de la loi entourant les sanctions. Il reconnaît par ailleurs les répercussions que peut avoir la richesse tirée de la corruption au sein de régimes répressifs sur la sécurité nationale lorsque ces fonds atteignent le Canada. Tout en estimant qu'une étude plus approfondie de ces questions est justifiée, le Comité recommande :

Recommandation 14

Que le gouvernement du Canada travaille de toute urgence en collaboration avec ses partenaires internationaux et nationaux afin de lutter contre le contournement des sanctions, notamment en prenant les mesures qui s'imposent pour recenser et bloquer les biens qui se trouvent au Canada et appartiennent à des individus et des entités russes visées par des sanctions.

Menaces militaires

Bien qu'une grande partie de l'étude ait porté sur les menaces non conventionnelles à la sécurité du Canada, y compris les méthodes de perturbation de la Russie, quelques témoins ont mis l'accent sur la défense. Ils ont souligné que le Canada doit investir dans les moyens de surveillance et de dissuasion compte tenu des armes de longue portée à la fine pointe qui pourraient être lancées contre des cibles en Amérique du Nord. Le général Eyre a décrit cette réalité de manière très claire : « [L]a distance et l'isolement géographique dont le Canada bénéficie depuis longtemps ne constituent plus une stratégie défensive viable[144]. »

143 SECU, *Témoignages*, 17 mai 2022, 1235 (William Browder).

144 SECU, *Témoignages*, 6 octobre 2022, 1105 (Gén Wayne D. Eyre).

Armement perfectionné et dissuasion par le déni

Parlant du soutien que le Canada a apporté à l'Ukraine et à ses alliés en Europe de l'Est, David Perry était d'avis que le Canada devrait « agir avec la même urgence et la même ingéniosité pour garantir que le Canada et l'Amérique du Nord soient mieux défendus contre une éventuelle agression russe plus près de chez eux ». Pour faire valoir ce point, il a signalé qu'après 20 années de modernisation militaire « [l]es aéronefs, les navires et les sous-marins russes peuvent désormais transporter des missiles de croisière avancés capables d'atteindre avec précision des cibles en Amérique du Nord à grande distance, comme d'autres missiles russes à longue portée peuvent le faire, y compris des planeurs hypersoniques[145] ». James Fergusson a expliqué que les missiles à longue portée que possède la Russie et ceux en cours de développement sont dotés d'une « capacité nucléaire et conventionnelle[146] », ajoutant qu'il y a « des lacunes et des vulnérabilités importantes qui existent depuis plus de dix ans en ce qui concerne la capacité du NORAD, et par conséquent du Canada, à détecter ces menaces, à les suivre, à les distinguer, puis à déclencher des capacités d'interception[147] ».

Ces lacunes et vulnérabilités ont des conséquences sur le plan stratégique. Selon Andrea Charron, « [l]a Russie en est venue à penser qu'elle peut exploiter nos vulnérabilités en matière de défense continentale, ce qui l'encourage à entreprendre des actions menaçantes à l'échelle régionale, afin de décourager les interventions outre-mer ». À son avis, le fait que l'Amérique du Nord compte depuis des décennies sur la « dissuasion par sanctions », qui « repose sur l'idée que le coût sera si élevé pour nos adversaires qu'ils n'oseront pas nous attaquer », n'a fait qu'enhardir la Russie. Compter uniquement sur cette approche « peut entraîner une escalade incontrôlable et réduire considérablement nos options d'intervention », a ajouté M^me^ Charron. Cette dernière a préconisé l'adoption d'une approche de dissuasion par déni ou interdiction. Pour effectuer ce virage, il faut s'assurer que les pays de l'Amérique du Nord « sont résilients à une variété d'attaques, surtout en deçà du seuil de recours à la force » et veiller à ce que « qu'ils repèrent les attaques et les contrent rapidement pour empêcher l'escalade ». En d'autres mots, M^me^ Charron estime qu'il faut « modifier les calculs de la Russie pour éliminer les avantages que comporteraient des attaques contre l'Amérique du Nord, plutôt que de nous concentrer uniquement sur l'augmentation des coûts[148] ».

145 SECU, *Témoignages*, 5 avril 2022, 1220 (David Perry).

146 SECU, *Témoignages*, 5 avril 2022, 1105 (James Fergusson).

147 *Ibid*.

148 SECU, *Témoignages*, 7 avril 2022, 1205 (Andrea Charron).

La protection des infrastructures essentielles et la cyberrésilience sont également une forme de dissuasion par déni. Jonathan Paquin a expliqué que cette forme de dissuasion a pour but de « décourager le Kremlin de mener de telles attaques, sachant que leurs succès sont probablement faibles ou peu probables[149] ». Comme l'a résumé le général Eyre, l'idée est d'éviter de donner aux adversaires du Canada des « cibles faciles[150] ».

Selon M[me] Charron, pour assurer la dissuasion par le déni dans le contexte de la défense, il ne doit pas y avoir en Amérique du Nord « de failles de commandement » qui peuvent être exploitées ou qui peuvent limiter l'action du Canada et des États-Unis[151]. Des capacités supplémentaires seront également nécessaires, notamment de nouveaux « capteurs pour la transformation numérique des radars » et des moyens de « créer des images opérationnelles communes, qui peuvent être partagées de façon efficace et appropriée ». M[me] Charron a aussi parlé de la nécessité d'intégrer les données et l'information « de tous les domaines, en travaillant avec un éventail d'alliés et de partenaires, y compris des organismes civils et des entreprises privées ». D'après son analyse, le but de la modernisation de la défense continentale et de la dissuasion par déni est de modifier « les perceptions antagonistes, afin que l'Amérique du Nord ne soit pas prise en otage[152] ».

En outre, Adam Lajeunesse de l'Université St. Francis Xavier a indiqué que la capacité actuelle de surveillance de l'ensemble des menaces dans l'Arctique est une source de préoccupations particulières, précisant qu'il s'agit d'une des approches que la Russie peut utiliser pour démontrer sa puissance. Il estime qu'il est prioritaire de renforcer les capacités de détection aérospatiales et maritimes du NORAD, car il faut « améliorer notre connaissance de la situation dans tous les domaines », y compris les capacités de détection sous la glace et au-dessus de celle-ci. Cette capacité permettrait de surveiller non seulement les systèmes d'armement russes, mais aussi les menaces hybrides provenant d'autres acteurs, tels que les navires de pêche illégale. M. Lajeunesse a

149 SECU, *Témoignages*, 3 mai 2022, 1250 (Jonathan Paquin).

150 SECU, *Témoignages*, 6 octobre 2022, 1145 (Gén Wayne D. Eyre).

151 SECU, *Témoignages*, 7 avril 2022, 1205 (Andrea Charron). Plus tard durant la réunion, en réponse à une question, M[me] Charron a donné en exemple le cyberespace, où « [n]ous avons des mandats très particuliers pour les différentes entités, mais aucune organisation responsable de faire un portrait global des cyberopérations », ce qui fait en sorte, selon elle, que « nous ne savons donc pas vraiment par où nous sommes touchés par les cyberattaques ». Au sujet de la situation au Canada, elle a fait remarquer que « [n]ous n'avons tout simplement pas de cybercommandement, contrairement aux États-Unis ». Dans une réponse plus générale à une autre question, elle a souligné la « tendance à penser qu'il y a le domaine de la défense et celui de la sécurité » et qu'il faut, à son avis, « les considérer ensemble. Nous ne pouvons plus travailler en vase clos. » Voir SECU, *Témoignages*, 7 avril 2022, 1230 et 1240 (Andrea Charron).

152 SECU, *Témoignages*, 7 avril 2022, 1205 (Andrea Charron).

d'ailleurs fait remarquer que l'Arctique « est en train de s'ouvrir à la navigation; un avenir sans glace ou partiellement libre de glace signifie que nous devrons surveiller et réglementer une activité accrue ». À son avis, des éléments d'un système de surveillance de tous les domaines – notamment des satellites et des navires de patrouille dans l'Arctique – ont été mis en place, mais d'autres sont en voie de développement depuis des années. M. Lajeunesse a toutefois laissé entendre qu'il « n'y a jamais eu un effort concerté de construire un système englobant tous les systèmes[153] ».

Dans une déclaration commune publiée en 2021, le Canada et les États-Unis ont convenu de moderniser, d'améliorer et de mieux intégrer les capacités nécessaires au NORAD pour maintenir une connaissance et une compréhension permanentes des menaces potentielles pour l'Amérique du Nord dans les domaines aérospatial et maritime, pour dissuader les actes d'agression contre l'Amérique du Nord, pour répondre aux menaces de manière rapide et décisive lorsque cela est nécessaire[154]. Pour éviter toute lacune pouvant être exploitée dans le contexte de la défense de l'Amérique du Nord à court et à long terme, le Comité recommande :

Recommandation 15

Que le gouvernement du Canada accélère la modernisation du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD).

Capacité de défense et état de préparation

Outre les menaces militaires touchant l'Amérique du Nord, certains témoins ont abordé la question générale de la capacité de défense et de l'état de préparation du Canada.

M. Perry a fait remarquer que même si le gouvernement du Canada cherche depuis longtemps à améliorer la défense continentale :

> [L]e rythme de mise en œuvre a été en deçà des attentes. Des fonds n'ont pas été dépensés année après année et les projets d'équipement nécessaires ont été retardés. La guerre en Ukraine illustre l'importance de disposer d'une armée moderne compétente au moment où la Russie ou toute autre puissance militaire précipite une crise internationale, et non pas lorsque nous, au Canada, décidons de le faire[155].

153 SECU, *Témoignages*, 7 avril 2022, 1110 (Adam Lajeunesse, titulaire de la chaire Irving Shipbuilding sur la sécurité maritime de l'Arctique canadien, Brian Mulroney Institute of Government, Université St. Francis Xavier, à titre personnel).

154 Défense nationale, *Déclaration conjointe sur la modernisation du NORAD*, 14 août 2021.

155 SECU, *Témoignages*, 5 avril 2022, 1220 (David Perry).

Allant plus loin, M. Perry a affirmé que « nous avons besoin d'un budget de défense plus important dès maintenant » et que « [l]es plans actuels de dépenses pour la défense du Canada sont insuffisants pour faire face aux menaces que la Russie et d'autres puissances comme la Chine représentent[156] ». Les alliés de l'OTAN se sont donné pour cible de consacrer à la défense 2 % de leur produit intérieur brut (PIB) d'ici 2024[157] ce qui, selon M. Perry, constitue une mesure « imparfaite » des contributions, mais une formule que « tous les alliés, y compris le Canada, ont convenu de respecter[158] ».

M. Lajeunesse était d'avis que le Canada devrait avoir pour « cible minimale » de consacrer 2 % de son PIB à la défense du pays. Il souhaiterait par ailleurs que ces fonds soient répartis de manière à tenir compte des adversaires stratégiques actuels[159]. Selon l'OTAN, le Canada avait affecté environ 1,27 % de son PIB à des dépenses pour la défense en 2022, ce qui le place au 24e rang parmi les 29 alliés lorsque ce paramètre est utilisé pour calculer les dépenses[160].

Pour sa part, Mme Charron a suggéré qu'au lieu de mettre l'accent sur les chiffres, il faudrait examiner « si nous avons la capacité de dépenser cet argent », faisant remarquer que les Forces armées canadiennes avaient perdu environ 10 000 militaires[161]. M. Perry a abordé la même question. Pour moderniser rapidement les capacités aériennes et navales remontant la plupart aux années 1980, il faut, selon lui, accroître la capacité du système d'approvisionnement pour la défense du Canada. M. Perry a fait remarquer que le Canada cherche à rattraper les années de retard accumulées après la Guerre froide, « lorsque nous n'avons pas suffisamment investi dans nos forces », alors que la main-d'œuvre chargée de l'approvisionnement « a été réduite de moitié dans les années 1990 et […] n'a jamais été entièrement reconstituée[162] ».

---

156 *Ibid.*

157 En 2014, les Alliés de l'Organisation du traité de l'Atlantique Nord (OTAN) ont convenu que tous les Alliés dont la proportion du produit intérieur brut consacrée à la défense était inférieure à la ligne directrice de 2 % s'efforceraient de se rapprocher de ce seuil dans les dix prochaines années. Voir OTAN, *Le financement de l'OTAN*.

158 SECU, *Témoignages*, 5 avril 2022, 1220 (David Perry).

159 SECU, *Témoignages*, 7 avril 2022, 1115 (Adam Lajeunesse).

160 Nota : trente pays sont membres de l'Alliance de l'OTAN, mais l'Islande n'a pas de forces armées. OTAN, Division diplomatie publique, « Graphique 3 : Dépenses de défense en part du PIB (%) », *Les dépenses de défense des pays de l'OTAN (2014-2022)*, 27 juin 2022.

161 SECU, *Témoignages*, 7 avril 2022, 1220 (Andrea Charron).

162 SECU, *Témoignages*, 5 avril 2022, 1220 (David Perry).

Les problèmes de capacité ne se limitent pas aux effectifs d'approvisionnement pour la défense. Le chef d'état-major de la défense, général Wayne Eyre, a laissé savoir au Comité qu'il était « très inquiet » au sujet des chiffres liés aux Forces armées canadiennes (FAC), et que c'est pour cette raison qu'il a fait de leur reconstitution (rétablissement, reconstruction et renouvellement de l'équipement) un « effort prioritaire[163] ». Le jour de sa comparution, le général Eyre a publié une directive sur la reconstitution des Forces armées canadiennes, laquelle définit le problème comme suit :

> En raison des problèmes de personnel et de dotation qui ont été aggravés par le fort engagement des FAC envers les opérations, les effets négatifs de la pandémie de la COVID-19, et une crise culturelle, la Défense nationale continue de perdre sa capacité à fournir et à maintenir des opérations simultanées à la portée et à l'échelle nécessaires pour atteindre les effets stratégiques demandés par le [gouvernement du Canada][164].

Le général Eyre a expliqué pourquoi il fallait prioriser la reconstitution des forces, exprimant ainsi ses inquiétudes : « [A]u fur et à mesure que les menaces à la sécurité mondiale augmentent et que les menaces au pays augmentent, notre état de préparation diminue au sein des Forces armées canadiennes[165]. »

Le Comité a pour mandat la sécurité publique et nationale. Il est conscient des travaux menés par le Comité permanent de la défense au sujet de la posture de défense du Canada et du recrutement du personnel. Or, vu le rôle essentiel que jouent les Forces armées canadiennes à l'égard de la sécurité du Canada, le Comité recommande :

Recommandation 16

Que le gouvernement du Canada s'assure d'avoir la capacité et les fonds nécessaires pour atteindre ses objectifs en matière d'approvisionnement pour la défense du pays, qu'il prenne toutes les mesures qui s'imposent pour faciliter la reconstitution des Forces armées canadiennes et qu'il rende compte périodiquement au Parlement des efforts déployés en vue d'atteindre ces deux objectifs.

Recommandation 17

Que le gouvernement du Canada respecte ses engagements envers ses alliés de l'OTAN et atteigne la cible de 2 % des dépenses pour la défense de l'Alliance.

---

163 SECU, *Témoignages*, 6 octobre 2022, 1115 (Gén. Wayne D. Eyre).

164 Défense nationale, *Directive du CEMD/du SM pour la Reconstitution des FAC*, 6 octobre 2022.

165 SECU, *Témoignages*, 6 octobre 2022, 1115 (Gén Wayne D. Eyre).

CONCLUSION : GÉRER UN CONTEXTE DE MENACE DE PLUS EN PLUS COMPLEXE

Bien que son étude porte sur la posture de sécurité du Canada par rapport à la Russie, le Comité a aussi entendu des témoignages concernant les préoccupations que suscite l'architecture de sécurité nationale du Canada. Ces considérations stratégiques et structurelles ont commencé à peser plus lourd dans un contexte de menace de plus en plus complexe et multidimensionnel.

Une approche intégrée en matière de sécurité nationale

Wesley Wark a mis en garde le Comité, lui conseillant d'éviter une approche en vase clos dans le cadre de son étude étant donné que les menaces auxquelles « le Canada est exposé vont bien au-delà de celles qui sont actuellement posées par la Russie[166] ». Après avoir observé que « tout est lié » en parlant de la défense, de la sécurité nationale et de la politique pour l'innovation, Aaron Shull a souligné que « les États adverses s'immiscent dans toutes les failles qu'ils peuvent exploiter avec leur puissance étatique », car ils considèrent que « tout est stratégiquement lié ». Pour ces raisons, il affirme que « nous devons faire de même[167] ».

Le général Eyre a également souligné ces liens, faisant remarquer que « [l]a Russie et la Chine ne font pas la distinction entre la paix et la guerre » et qu'ils « utiliseront tous les éléments de leur puissance nationale, agissant souvent juste sous le seuil d'un conflit violent à grande échelle ». Néanmoins, comme cela a été montré avec la guerre de la Russie contre l'Ukraine, il a ajouté que ces nations sont « bien disposées à franchir ce seuil[168] ». Selon le général, pour se préparer à « la possibilité d'un conflit ouvert dans les domaines traditionnels », il faut « développer notre capacité de gérer des affrontements dans les domaines cybernétique, spatial et cognitif ». Ce qu'il faut, a-t-il insisté, c'est « élaborer une approche intégrée combinant des interventions militaires, des actions diplomatiques, ainsi que des mesures économiques et d'information à l'échelle locale, régionale, nationale et multinationale[169] ».

166 SECU, *Témoignages*, 17 mai 2022, 1105 (Wesley Wark).

167 SECU, *Témoignages*, 17 mai 2022, 1150 (Aaron Shull).

168 SECU, *Témoignages*, 6 octobre 2022, 1100 (Gén Wayne D. Eyre).

169 *Ibid.*, 1105.

Adaptation aux nouvelles menaces

Compte tenu de l'évolution du contexte de la menace, certains témoins ont laissé entendre qu'il faut changer et renforcer l'architecture de sécurité nationale du Canada là où des fissures risquent d'apparaître. Plus précisément, Christian Leuprecht estime que « l'architecture de la sécurité régionale et nationale sous-estime depuis un certain temps[170] » l'extrémisme violent à caractère idéologique (EVCI), l'activité séditieuse et l'ingérence étrangère. Il a fait remarquer que « [l]es critères que doivent respecter les organismes fédéraux d'application de la loi pour déclencher une enquête sur l'ingérence d'acteurs étrangers sont assez rigoureux, exigeant souvent qu'il y ait une grande criminalité ou des liens directs avec un État étranger ». À son avis, la « barre est trop haute », ce qui crée « un environnement favorable à l'influence des acteurs étrangers ». Pour ces raisons, M. Leuprecht souhaite que l'architecture de sécurité nationale du Canada soit « plus active et plus ferme dans la lutte contre l'EVCI et l'ingérence d'acteurs[171] ».

Sans mentionner de menaces précises, d'autres témoins se sont attachés à la stratégie à la base de l'approche du Canada en matière de sécurité nationale et aux capacités qui s'y rattachent. M. Wark a souligné « l'étonnante constatation que le Canada n'a actuellement aucune stratégie globale sur la sécurité nationale » et que la « dernière et l'unique stratégie » a été publiée en 2004[172]. Citant les conclusions d'un rapport spécial du Centre pour l'innovation dans la gouvernance internationale, il a également rappelé que le dernier examen des capacités du Canada d'assurer la sécurité nationale a été réalisé par un examinateur externe en 1970[173].

M. Wark estime que l'invasion de l'Ukraine par la Russie « nous a donné l'occasion de repenser notre approche en matière de sécurité nationale » et qu'il nous faut reconnaître que « nous vivons dans un monde de menaces dans lequel les frontières n'existent pas ». Selon lui, face à ces menaces, « [n]ous devons développer la capacité souveraine requise pour en comprendre les origines et les répercussions à l'échelle mondiale » et « renforcer la capacité générale de collecte et d'évaluation du

170 SECU, *Témoignages*, 17 mai 2022, 1100 (Christian Leuprecht).

171 *Ibid*.

172 SECU, *Témoignages*, 17 mai 2022, 1105 (Wesley Wark).

173 *Ibid*. Voir Aaron Shull et Wesley Wark, *Reimagining a Canadian National Security Strategy*, rapport spécial du Centre pour l'innovation dans la gouvernance internationale (CIGI), 2021. [DISPONIBLE EN ANGLAIS SEULEMENT].

renseignement[174] ». Le Canada doit également être prêt « à déployer une capacité d'intervention offensive, y compris en utilisant le renseignement et des outils cybernétiques[175] ».

Réimaginer l'approche du Canada en matière de sécurité nationale, c'est aussi chercher une plus grande transparence. Charles Burton a fait part de ses inquiétudes au sujet des pratiques de divulgation des organismes canadiens de sécurité nationale, posant la question à savoir si ces organismes « ont été suffisamment transparents envers le Parlement, représenté par votre comité de la Chambre des communes, sur les préoccupations en matière de sécurité publique et nationale[176] ». Au sujet de la transparence, il a soulevé des enjeux tels que les poursuites en cas d'espionnage, le transfert des technologies à des États étrangers et la possibilité de connaître « l'identité des Canadiens qui sont influents dans le processus stratégique du Canada et qui sont dans une situation de conflit d'intérêts qui menace la sécurité et la souveraineté du Canada parce qu'ils ont reçu des avantages d'un État étranger ». En réponse à ce dernier problème, M. Burton croit que le Canada devrait mettre en place sans tarder une loi créant un registre des agents étrangers ou encore une mesure équivalente à la loi australienne sur le régime de transparence en matière d'influence étrangère[177].

Reconnaissant l'influence que peuvent avoir les comités parlementaires sur « le cadre général, la gouvernance et les questions stratégiques », M. Wark a parlé des difficultés qu'éprouvent ces comités à entrer « dans les détails du renseignement et de la sécurité nationale, en raison du manque d'accès aux renseignements classifiés et aux séances d'information classifiées ». À son avis, « c'est un rôle que le Comité des parlementaires sur la sécurité nationale et le renseignement peut jouer, comme le Parlement l'a prévu[178] ».

Dans une optique plus large, Aaron Shull a donné deux suggestions concrètes pouvant servir de point de départ. Il a proposé qu'une évaluation annuelle de la menace soit déposée devant le Parlement et qu'il y ait chaque année une discussion des priorités en

174 SECU, *Témoignages*, 17 mai 2022, 1105 (Wesley Wark). M. Wark a plus tard reconnu les « capacités limitées relativement au renseignement étranger » du CST et d'Affaires mondiales Canada, mais a affirmé que « [n]ous pourrions faire beaucoup plus », commentant que « [l]e Canada a souvent fait l'objet de critiques discrètes de la part de ses partenaires du Groupe des cinq qui considèrent qu'il se comporte un peu comme un profiteur dans le partenariat de l'alliance ». Voir *ibid*., 1115.

175 SECU, *Témoignages*, 17 mai 2022, 1105 (Wesley Wark).

176 SECU, *Témoignages*, 3 mai 2022, 1135 (Charles Burton).

177 *Ibid*.

178 SECU, *Témoignages*, 17 mai 2022, 1135 (Wesley Wark).

matière de renseignement[179]. Le CST et le Service canadien du renseignement de sécurité produisent des rapports annuels et des rapports publics, respectivement, ainsi que des rapports portant sur des enjeux particuliers, comme les cybermenaces et les menaces que fait peser l'ingérence étrangère sur le processus démocratique de notre pays[180]. Or, il n'y a pas d'évaluation annuelle de la menace comme celle produite par le directeur du renseignement national des États-Unis, qui présente une évaluation stratégique des menaces mondiales à la sécurité nationale des États-Unis selon les services du renseignement américains[181].

Tous ces témoignages donnent à penser qu'il y a lieu de mener un examen de l'architecture de sécurité nationale du Canada dans le but de s'assurer que le cadre est bien calibré, que des ressources suffisantes sont en place et que l'on peut réagir au nouveau contexte de la menace. En trois ans à peine, le Canada et ses alliés ont dû composer avec les conséquences d'une pandémie mondiale, un nombre accru de catastrophes naturelles, l'intensification du changement climatique et le pire conflit armé en Europe depuis de Seconde Guerre mondiale, sans compter l'accélération des changements technologiques. Selon le Comité, l'évolution rapide de la situation et des tendances souligne à quel point il est important d'avoir une stratégie qui nous guide et la capacité d'évaluer les menaces, les capacités et les intentions, tout en maintenant la capacité de voir plus loin. Par conséquent, le Comité conclut son étude par les recommandations ci-dessous :

Recommandation 18

Que le gouvernement du Canada mette en place un registre des agents étrangers ou une mesure équivalente à la loi australienne sur le régime de transparence en matière d'influence étrangère.

179 SECU, *Témoignages*, 17 mai 2022, 1135 (Aaron Shull). Le rapport du CIGI recommande qu'une déclaration annuelle sur les menaces mondiales pour le Canada soit présentée au Parlement par le premier ministre et coordonnée par le conseiller en matière de sécurité nationale et de renseignement. Voir Aaron Shull et Wesley Wark, *Reimagining a Canadian National Security Strategy*, CIGI, 2021, p. 5.

180 Voir Service canadien du renseignement de sécurité, *Publications*; CST, *Rapports*; et Centre canadien pour la cybersécurité, *Évaluation des cybermenaces nationales 2023-2024*.

181 Voir États-Unis, Bureau du directeur du renseignement national, *Annual Threat Assessment of the U.S. Intelligence Community*.

Recommandation 19

Que le gouvernement du Canada publie une stratégie globale et intégrée sur la sécurité nationale, qui prend en compte les résultats d'un examen interne des capacités du Canada en matière de sécurité nationale.

Recommandation 20

Que, conformément à l'article 34 de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*, la Chambre des communes désigne le Comité permanent de la sécurité publique et nationale pour mener un examen approfondi des dispositions et de l'application de cette loi.

Recommandation 21

Que le gouvernement du Canada présente au Parlement une évaluation annuelle des menaces touchant la sécurité nationale du pays.

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
À titre personnel	2022/04/05	17
Ahmed Al-Rawi, professeur adjoint, Simon Fraser University		
Alexander Cooley, professeur de science politique lauréat du prix Claire Tow, Barnard College, et membre auxiliaire du corps professoral, Chatham House		
James Fergusson, directeur adjoint, Centre d'étude sur la défense et la sécurité, University of Manitoba		
Robert Huebert, professeur associé, Département de sciences politiques, University of Calgary		
Veronica Kitchen, professeure agrégée, Département des sciences politiques, University of Waterloo		
David Perry, président, Institut canadien des affaires mondiales		

Organismes et individus	Date	Réunion
À titre personnel	2022/04/07	18
Andrea Charron, directrice et professeure agrégée, Centre for Defence and Security Studies, University of Manitoba		
David A Etkin, professeur, Disaster and Emergency Management, York University		
Paul Goode, titulaire de la chaire d'études russes McMillan, Carleton University		
Marcus Kolga, agrégé supérieur, Institut Macdonald-Laurier		
Adam Lajeunesse, titulaire de la chaire Irving Shipbuilding sur la sécurité maritime de l'Arctique canadien, Brian Mulroney Institute of Government, St. Francis Xavier University		
À titre personnel	2022/05/03	21
Charles Burton, agrégé supérieur, Centre for Advancing Canada's Interests Abroad, Macdonald-Laurier Institute		
Frédéric Cuppens, professeur, Polytechnique Montréal		
Nora Cuppens, professeure, Polytechnique Montréal		
Jonathan Paquin, professeur titulaire, Département de science politique, Université Laval		
Échange canadien de menaces cybernétiques	2022/05/03	21
Jennifer Quaid, directrice exécutive		
Optiv Canada Federal	2022/05/03	21
Michael Doucet, directeur exécutif, Bureau du chef de la sécurité de l'information		

Organismes et individus	Date	Réunion
À titre personnel	2022/05/17	25
William Browder, président-directeur général, Hermitage Capital Management Ltd		
Christian Leuprecht, professeur, Collège militaire royal du Canada, Queen's University		
Jeffrey Mankoff, chercheur universitaire émérite, National Defense University		
Errol P. Mendes, professeur, Droit constitutionnel et international, Université d'Ottawa		
Centre pour l'innovation dans la gouvernance internationale	2022/05/17	25
Aaron Shull, directeur général		
Wesley Wark, agrégé supérieur		
Ministère de la Sécurité publique et de la Protection civile	2022/06/02	27
L'hon. Bill Blair, C.P., député, ministre de la protection civile		
Rob Stewart, sous-ministre		
À titre personnel	2022/06/07	28
Ken Barker, professeur, Institute for Security, Privacy, and Information Assurance, University of Calgary		
Juliette Kayyem, maître de conférences en sécurité internationale, chaire d'enseignement Belfer, Kennedy School of Government, Harvard University		
Beauceron Security	2022/06/07	28
David Shipley, directeur général		
Agence des services frontaliers du Canada	2022/06/09	29
John Ossowski, président		
Scott Harris, vice-président, Direction générale du renseignement et de l'exécution de la loi		
Gendarmerie royale du Canada	2022/06/09	29
S.-comm. Michael Duheme		
Surint. Denis Beaudoin, Criminalité financière		

Organismes et individus	Date	Réunion
Ministère de la Sécurité publique et de la Protection civile	2022/06/09	29
L'hon. Marco Mendicino, C.P., député, ministre de la sécurité publique		
Rob Stewart, sous-ministre		
Service canadien du renseignement de sécurité	2022/06/09	29
Michelle Tessier, sous-directrice, Opérations		
Centre de la sécurité des télécommunications	2022/10/06	37
Caroline Xavier, chef		
Sami Khoury, dirigeant principal, Centre canadien pour la cybersécurité		
Ministère de la Défense nationale	2022/10/06	37
Gén Wayne D. Eyre, chef d'état-major de la défense, Forces armées canadiennes		
Vam J.R. Auchterlonie, commandant du Commandement des opérations interarmées du canada		
Mgén Michael Wright, commandant, Commandement du renseignement des Forces canadiennes et chef du renseignement de la Défense		

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.

BlackBerry

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 17, 18, 21, 25, 27 à 29, 34, 37, 47, 48, 55 et 58) est déposé.

Respectueusement soumis,

Le président,
Ron McKinnon

RAPPORT COMPLÉMENTAIRE DU BLOC QUÉBÉCOIS
Prêt à relever le défi : renforcer la posture de sécurité du Canada par rapport à la Russie

Le Bloc Québécois salue les membres du Comité ainsi que le personnel de la Bibliothèque du Parlement pour le travail accompli au cours de cette étude. Les mêmes remerciements s'adressent à tous les témoins, à tous les citoyens et à toutes les organisations interpellées ainsi qu'aux experts qui ont nourri le débat public sur le sujet en soumettant leurs observations sous forme de lettres et de mémoires. Il ne fait aucun doute qu'il sera utile de revoir ces contenus dans un avenir proche. La posture de sécurité du Canada soulève des enjeux importants. Nous pouvons espérer que la société sera, au fil des prochaines années, de plus en plus conscientisée à ce sujet et que cela permettra de corriger les lacunes qui ont été constatées lors de la présente étude.

Bien que le Bloc Québécois soutienne le principe sous-tendant la recommandation 2, selon laquelle le gouvernement du Canada doit promouvoir des programmes de formation postsecondaire dans le domaine de la cyberdéfense, il ne faut pas oublier que l'éducation relève exclusivement du Québec et des autres provinces. Par conséquent, il ne revient pas au gouvernement fédéral de créer de tels programmes, et seules les provinces ont la compétence pour le faire. Le rôle du gouvernement fédéral dans ce cas-ci est de retourner l'argent des Québécois et des provinces au moyen de transferts inconditionnels. Le gouvernement du Canada doit garder à l'esprit que le Québec a un réseau unique d'études postsecondaires et donc une expertise dans un domaine à l'égard duquel le gouvernement fédéral n'a aucune compétence.

Le Bloc Québécois soutient également la recommandation indiquant que le gouvernement du Canada, en consultation avec les parties concernées, mise sur la Stratégie nationale de cybersécurité, mais avec des bémols. Le fédéral tente de trouver toutes les excuses possibles pour s'ingérer dans des domaines qui relèvent clairement de la compétence des provinces. Pourtant, les exemples de mauvaise gestion fédérale sont la norme plutôt que l'exception. Toute stratégie nationale de cybersécurité doit s'en tenir aux entreprises et aux infrastructures sous responsabilité fédérale. La stratégie doit faire en sorte que les propriétaires et exploitants d'infrastructures essentielles fédérales de toute taille disposent des spécialistes, de l'expertise et des ressources dont ils ont besoin en matière de cybersécurité pour faire face à une cyberattaque et s'en remettre. Elle doit aussi s'assurer que les normes de cybersécurité soient respectées et fassent l'objet de rapports. Le gouvernement du Canada doit consulter le Québec à ce sujet. Il doit garder à l'esprit que lorsque le gouvernement du Québec n'en a pas la complète maîtrise, les politiques fédérales axées sur l'uniformisation viennent souvent dédoubler des programmes québécois et en complexifier l'application. Ainsi, la Stratégie nationale de cybersécurité doit être appliquée en collaboration avec le Québec, et non lui être imposée, en plus de viser uniquement les entités sous responsabilité fédérale. Étant donné les nombreux ratés du gouvernement fédéral dans la gestion de ses champs de compétence, il est impératif

que le Comité rappelle au gouvernement fédéral de s'en tenir uniquement à ce qui relève de sa responsabilité. Il éviterait ainsi de créer des conflits avec le Québec et les provinces.