L'IMPÉRATIF DE LA CYBERCOLLABORATION

Survol des principaux modèles et pratiques dans la collaboration gouvernement-industrie dans la cyberdéfense

CADSI · AICDS
Canadian Association of Defence and Security Industries
Association des industries canadiennes de défense et de sécurité

Rapport 2020 | Association des industries canadiennes de la défense et de la sécurité

TABLE DES **MATIÈRES**

Résumé Opérationnel 4

Les Nouveaux Défis Posés Par Le Domaine Cybertnétique 10

Un Changement Dans La Pensée Collaborative 13

L'impératif De La Collaboration En Cyberdéfense Et En Cybersécurité 16

Vers Un Modèle Global De Collaboration Publique-Privée Pour La Cyberdéfense 20

Principales Fonctions, Politiques Et Pratiques De Collaboration Des Alliés Du Canada 22

Principaux Facteurs Menant À Une Collaboration Fructueuse 32

Prioriser Les Partenaires Du Secteur Privé 35

Conclusion 36

Recommandations 38

RÉSUMÉ **OPÉRATIONNEL**

Le domaine cybernétique n'a aucun précédent historique. Il est bâti par l'humain, ne connaît aucune frontière et est en constant changement. Il croît aussi en complexité et évolue dans une myriade de nouvelles manières avec une vélocité extraordinaire, transformant la vie des personnes, dominant l'économie mondiale, changeant les règles d'engagement des États. Grâce aux avancées révolutionnaires dans le monde de l'intelligence artificielle (IA), des mégadonnées, de la cinquième génération des communications mobiles, des réseaux sociaux, de l'informatique quantique et l'Internet des choses, le domaine cybernétique continuera d'avoir une incidence gigantesque à tous les niveaux de la société, y compris sur la sécurité nationale.

À mesure que le domaine de la cybernétique continue à évoluer, des éléments malicieux, une catégorie qui inclut les États nations, les criminels, les terroristes, les hacktivistes et les opportunistes, prennent contrôle de toute nouvelle possibilité et amélioration de la cybertechnologie pour lancer des cyberattaques contre les personnes, les entreprises et les États. Ils sont aussi capables de brouiller les pistes. À l'échelon national, les cyberattaques ont déjà des effets économiques néfastes mesurables. Selon le gouvernement du Canada, le revenu total à risque pour le pays lié aux menaces informatiques est évalué à 100 milliards de dollars par année.[1] Aux États-Unis, l'incidence économique d'une cyberattaque majeure contre l'infrastructure critique nationale a été évaluée à une somme variant entre 243 milliards et 1 billion de dollars US, dans un scénario extrême.

Contrairement aux mesures de guerre conventionnelles entre les États, qui nécessitent une planification méticuleuse pouvant coûter des milliards de dollars à mettre en œuvre, des cyberattaques dévastatrices ayant des conséquences étendues peuvent être lancées contre l'infrastructure critique à la vitesse de l'éclair par un petit groupe de cyberexperts armés uniquement d'ordinateurs personnels connectés à Internet et quelques lignes d'un codage malicieux. Ces attaques peuvent être élaborées et lancées avec précision ou de manière aléatoire à partir de n'importe quel endroit dans le monde dans l'espace de quelques minutes ou secondes. Une fois les dommages causés, les auteurs peuvent rapidement effacer toute trace de leurs activités, rendant toute accusation presque impossible ou possiblement réfutable.

Pour les gouvernements, assurer la sécurité de l'État contre les cyberattaques est un défi considérable nécessitant un changement d'une tout aussi grande envergure dans notre façon de penser. Par exemple, l'OTAN considère désormais une cyberattaque contre l'un de ses membres une action justifiant le recours à la défense collective en vertu de l'article 5 du traité de l'OTAN. De toute évidence, ce qui commence dans le cyberespace ne reste pas dans le cyberespace. Les cyberattaques ne peuvent être contrées à l'aide des stratégies et des méthodes conçues pour éliminer les menaces traditionnelles et neutraliser les adversaires, parce que la cybernétique est fondamentalement différente.

> Les gouvernements qui travaillent en silo ne seront pas en mesure de suivre cadence de plus en plus rapide des menaces que présente le domaine cybernétique.

Les caractéristiques uniques du domaine cybernétique, c'est-à-dire une innovation plus rapide, l'infrastructure appartenant au secteur privé, les menaces asymétriques, l'économie favorisant grandement les pirates, nécessiteront la mise en place de nouvelles politiques, de nouveaux processus de décision et de nouvelles approches quant à l'approvisionnement, et l'adoption de méthodes d'intégration des ressources et des motivations entourant les objectifs communs de divers intervenants des secteurs public et privé. Toutefois, ces éléments à eux seuls ne doteront pas les gouvernements de tous les outils et capacités nécessaires pour suivre la cadence de plus en plus rapide du domaine cybernétique. En fait, peu importent les améliorations faites, les gouvernements qui travaillent en silo ont peu de chances de réussir.

Heureusement, le secteur privé possède de nombreuses forces auxquelles le gouvernement peut se fier pour protéger et défendre la sécurité nationale par le domaine cybernétique. Contrairement aux domaines traditionnels de l'air, de la terre, de la mer et de l'espace, où les gouvernements ont une certaine influence ou un certain contrôle, la cyberinfrastructure appartient presque entièrement au secteur privé. Au Canada, par exemple, des entreprises privées possèdent et opèrent 98 % de la cyberinfrastructure. Les cyberentreprises constituent aussi le moteur infatigable qui propulse la cyberinnovation et la prolifération de canaux dans la société. Elles développent les technologies sous-jacentes qui permettent au domaine cybernétique de fonctionner, et les produits et solutions commerciaux qui visent à résoudre les plus grands défis. Elles donnent accès à un large éventail de produits et services dont les cycles de développement s'harmonisent avec celui des adversaires du Canada. Ces entreprises sont perpétuellement au premier front des cyberattaques et des cyberagressions, elles ont donc régulièrement un aperçu des tactiques, des techniques et des procédures utilisées par leurs adversaires. Contrairement à leurs homologues du secteur privé, elles n'ont pas le fardeau de processus d'approvisionnement pouvant durer des années, voire des décennies. Elles peuvent plutôt lancer une nouvelle solution technologique entièrement fonctionnelle en quelques mois ou quelques semaines.

1 Dark Space (APT0) – A comprehensive report on advanced cyber security tradecraft and issues affecting Canada, PSTP02-359ESEC (Apr 2011-Mar 2015) Bell Canada, DND, CSE.

Compte tenu des nombreux domaines où l'industrie privée complète ou accroît les capacités du gouvernement dans le domaine cybernétique, la collaboration entre les deux groupes est essentielle pour garder le rythme avec les innovations rapides du domaine cybernétique, pour élaborer des politiques, des outils et des stratégies efficaces visant à assurer la sécurité et la défense nationales, et pour gérer un large écart des compétences. La portée, la vitesse et la complexité des défis que représente le domaine cybernétique touchent tous les aspects de la société

> Les alliés du Canada ont reconnu les avantages de l'approche collaborative entre le gouvernement et l'industrie dans la lutte contre les cyberdéfis.

et nécessitent une réponse conjointe. Malgré cette mission commune, la compréhension mutuelle et la confiance demeurent faibles au Canada. La recherche de l'AICDS, qui comprend une étude comparative approfondie des principaux modèles, programmes et pratiques mondiaux dans la collaboration gouvernement-industrie en matière de défense et de sécurité dans le cyberespace, montre que les alliés du Canada ont reconnu les nombreux avantages de l'approche collaborative dans la lutte contre leurs propres défis dans ce domaine. Ils ont rapidement et résolument fait l'essai de diverses approches de la collaboration gouvernement-industrie au niveau stratégique, politique et opérationnel, et ils tissent de nouvelles relations industrielles pour faire avancer la protection des actifs essentiels et le développement rapide des capacités. Ils ont eu un succès notable dans différents secteurs du domaine cybernétique grâce à leurs efforts de collaboration. Ils ont appris de dures leçons en échouant rapidement à certaines occasions.

Les États-Unis, par exemple, sont un chef de file dans la cyberapprovisionnement, permettant à son gouvernement (y compris l'armée et les agences de sécurité nationale) d'acquérir et d'itérer rapidement des technologies et des solutions à la fine pointe issues de l'industrie grâce à un éventail de programmes, de construits et de politiques à l'appui, comme la Defense Innovation Unit (DIU), l'Army Futures Commands (AFC), et les autre authorités transactionnelles (OTA). Ce pays a réalisé que l'équilibre traditionnel dans l'approvisionnement entre la gestion du risque financier et l'acquisition en temps opportun, appliquée à la cybernétique, mènerait inévitablement à l'échec, lorsqu'une solution disponible aurait pu prévenir les répercussions d'une cyberattaque, mais qu'elle ne pouvait être acquise en temps opportun. Des estimations plus réalistes, à partir d'un échantillon plus grand, des dommages causés, de la perte opérationnelle et des réparations entraînées par les cyberattaques et les brèches forcent un recalcul des coûts de report ou d'inaction, et créent une nouvelle dynamique qui redéfinit les concepts traditionnels de l'optimisation des ressources en ce qui a trait à l'acquisition de cybersolutions.

En ce qui a trait au développement et au partage des connaissances, la National Cyber Security Center (NCSC) au Royaume-Uni a lancé l'initiative « Industry 100 » afin de favoriser d'étroites relations de travail collaboratives entre la NCSC et 100 industries d'Experts en cyberdéfense. Dans le domaine cybernétique, là où les gens représentent le point final de la convergence technologique, les gouvernements et l'industrie doivent éliminer les obstacles administratifs qui les empêchent de travailler ensemble, partout où ils existent. C'est particulièrement vrai étant donné la pénurie grandissante de compétences en cybernétique que connaissent le Canada et ses alliés.

En ce qui concerne l'engagement international et la gouvernance, grâce aux efforts de l'Australie visant à assurer la coordination entre gouvernements et à engager activement les pays du sud-est de l'Asie dans des enjeux cybernétiques importants, les gouvernements et l'industrie ont travaillé ensemble à l'élaboration de l'International Cyber Engagement Strategy de l'Australie, lancée en octobre 2017. Les avantages d'une mission conjointe réalisée dans le cadre d'une collaboration des secteurs public et privé et de la mobilisation des alliés internationaux peuvent avoir des retombées positives au pays et à l'étranger. Les normes cybernétiques internationales en sont encore à leur balbutiement et font l'objet de maintes négociations bilatérales dirigées, dans le cas de l'Australie, par son ambassadeur des Affaires cybernétiques.

La collaboration entre l'industrie et le gouvernement prend différentes formes. Elle existe dans un spectre qui s'étend de la gestion traditionnelle par les intervenants à des partenariats hautement intégrés demandant la co-création de solutions complexes. Les pays étudiés ont exploré, expérimenté et mis en œuvre divers programmes et initiatives dans l'ensemble de ce spectre et ont récolté différents niveaux de succès. Les alliés du Canada continuent de faire des progrès quantifiables dans ce domaine, mais la recherche de l'AICDS laisse croire que le Canada agit lentement pour passer au-delà de la collaboration de base, malgré la mise en place de certains programmes collaboratifs avec l'industrie.

> Même s'il a lancé certains programmes de collaboration, le Canada a tardé à faire plus que la collaboration la plus élémentaire.

En étudiant les pratiques collaboratives des alliés du Canada, l'AICDS a découvert lesquelles s'étaient avérées les plus efficaces pour relever des cyberdéfis précis et a déterminé un ensemble des meilleures pratiques communes qui entraînent vraisemblablement une collaboration mutuelle avantageuse entre l'industrie privée et le gouvernement. Le présent rapport reconnaît que chaque pays est différent et a une gouvernance publique et des contextes institutionnels uniques, mais il propose aussi un modèle global de collaboration approfondie en matière de cybersécurité. Le gouvernement du Canada peut utiliser ce modèle pour lancer une discussion coordonnée concernant les meilleures formes de collaboration visant à régler leurs principaux cyberenjeux. Il faut également souligner qu'en général, les stratégies nationales liées à la cybernétique en sont encore à leur balbutiement et que même si les alliés du Canada ont tous contribué à la composition des meilleures pratiques, aucun ne les a encore intégrées ensemble dans un cadre de travail global. Ainsi, le modèle et les meilleures pratiques continuent d'évoluer.

Enfin, le rapport présente en détail des recommandations précises visant à aider le Canada à resserrer l'écart de collaboration avec ses alliés :

1. Innovation, Sciences et Développement économique Canada devrait mettre sur pied une Table sectorielle de stratégies économiques de la cyberdéfense et de la cybersécurité.

   - Les Tables sectorielles de stratégies économiques constituent une nouvelle approche de collaboration publique-privée lancée par le gouvernement fédéral en 2017 qui ont déjà des effets positifs. Ces tables contribuent aussi à la mise en œuvre d'importants changements de politique et de réglementation en jumelant des hauts directeurs de l'industrie et des hauts représentants du gouvernement pour l'élaboration conjointe de stratégies visant à s'attaquer aux enjeux les plus pressants pour le secteur.

2. Le gouvernement fédéral devrait piloter un mécanisme de partage des talents avec l'industrie afin de répondre à la grave pénurie de talent en cybernétique au Canada. Parmi les ministères et les organismes participants au projet pilote pourraient figurer Sécurité publique Canada, le Centre canadien pour la cybersécurité, et le ministère de la Défense nationale.

   - Ce programme pourrait être modelé suivant l'initiative Industry 100 du Royaume-Uni, un cadre d'échange de talents géré par le National Cyber Security Centre qui permet au gouvernement et à l'industrie de se mobiliser conjointement pour les politiques émergentes, l'innovation et les défis opérationnels grâce à des prêts de services intégrés, globaux et à court terme.

3. Innovation, Sciences et Développement économique Canada devrait mettre en place l'un des trois cyberréseaux annoncés dans le budget de 2019 afin de permettre les propositions de création d'un réseau opérationnel axé sur le partage d'information et l'analyse sur les menaces, de même que la réponse à celle-ci et la mise à l'essai de solutions pour le gouvernement et l'industrie.

   - Un réseau devrait être mis en place pour offrir un environnement opérationnel avec un réseau fédérateur physique et numérique sûr, organisé de manière à permettre le partage bidirectionnel de l'information sur les menaces, l'analyse et la réponse conjointes et la mise à l'essai de solutions aux problèmes mondiaux réels et actuels.

---

2 Cyber Interdependencies of Canada's Critical Infrastructures, Bell Canada, RAND Corporation, PSC, Apr-Mar 2007.

3 The Cyber Security Social Contact, Internet Security Alliance, Sept 2016.

4 From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence., Mar 2019.

LES NOUVEAUX **DÉFIS POSÉS PAR LE DOMAINE CYBERTNÉTIQUE**

Compte tenu de l'importance critique du domaine cybernétique pour la sécurité des citoyens canadiens, du succès de l'industrie et de la prospérité économique du Canada, rendre le cyberespace plus sûr représente une urgence pour le gouvernement du Canada. À l'échelon national, la cyberdéfense et la cybersécurité nécessitent une protection contre un large éventail d'activités malicieuses commises par une combinaison d'acteurs gouvernementaux ou non qui cherchent à atteindre divers objectifs criminels, politiques ou économiques. Toutefois, les caractéristiques uniques du domaine cybernétique, détaillées ci-dessous, rendent la défense contre des attaques de ce genre un défi sans précédent dans sa portée.

1. **La cyberinnovation est rapide** – De grandes avancées en cyberinnovation se produisent chaque jour à une vitesse vertigineuse, ce qui rend extrêmement difficile pour les gouvernements la tâche de suivre la cadence afin d'atténuer les répercussions des nouveaux types de menaces et d'attaques malicieuses en temps opportun.

2. **La cyberinfrastructure appartient au secteur privé** – Les gouvernements ont la responsabilité commune, avec l'industrie, de sécuriser le cyberespace, mais le secteur privé possède largement son infrastructure, au pays et à l'étranger. La collaboration publique-privée est donc impérative.

3. **Les menaces provenant du cyberespace sont asymétriques** – Dans le royaume cybernétique, les particuliers et les petits groupes de personnes ont la capacité de développer des technologies malicieuses rapidement et à moindres coûts, et peuvent l'utiliser pour lancer des cyberattaques dévastatrices contre les États-nations tout aussi rapidement et avec peu de ressources financières. L'économie du cyberespace favorise l'attaquant.

> Au Canada, 15 différents ministères et organismes ont des responsabilités directes en matière de cybernétique, mais il n'y a pas de coordination centralisée pour coordonner les différents mandats.

4. **La cybernétique s'immisce dans d'autres domaines** – Le domaine cybernétique est unique, car il peut s'immiscer dans d'autres domaines, de sorte que « les combattants de chacun des autres domaines seraient gravement handicapés si leur accès au cyberespace était véritablement compromis. Cela a mené à l'impression que le cyberespace était le nouveau champ de bataille. Un domaine pour les gouverner tous. Un domaine pour les amener tous et dans l'Ethernet les lier. »[5]

5. **Le cyberespace a été créé par l'humain et est facilement malléable** – Le cyberespace est différent des autres domaines créés par l'humain, mais sa malléabilité a le potentiel de le rendre réellement unique. Comme l'a écrit Martin Libicki, « la tâche de défendre le réseau n'est pas tellement de mieux manœuvrer afin d'avoir plus de puissance de tir, mais plutôt de changer les paramètres particuliers dans sa propre zone du cyberespace pour qu'elle soit plus résistante aux attaques ».[6]

6. **Le cyberespace n'a pas été conçu en fonction de la sécurité** – L'architecture du cyberespace a été « davantage propulsée par des considérations d'interopérabilité et d'efficience que par des soucis pour la sécurité ».[7]

Non seulement le domaine cybernétique est-il unique en soi, mais les gouvernements qui ont la tâche de le rendre sûr n'ont pas la structure nécessaire pour régler les nombreux problèmes de sécurité qui s'y présentent. Au sein du gouvernement des États-Unis, par exemple, « les responsabilités liées à la cybersécurité sont distribuées parmi un large éventail d'agences et de départements fédéraux, dont l'autorité de plusieurs se chevauche, et aucun n'a suffisamment de pouvoir décisionnel pour diriger des actions relatives à des enjeux souvent conflictuels de manière constante ».[8] Au Canada, au moins 15 organismes et ministères différents ont des responsabilités directes en matière de cybernétique, mais aucune fonction centralisée de coordination pour harmoniser les mandats de chacun. Nous sommes tout aussi mal structurés pour répondre à la menace.

---

5 Cyberspace Is Not a Warfighting Domain, Journal of Law and Policy for the Information Society, Martin C. Libicki, Jan 2012.

6 Ibid.

7 Cyberspace Policy Review, United States Executive Office of the President, Apr 2014.

8 Ibid.

UN CHANGEMENT **DANS LA PENSÉE COLLABORATIVE**

Définir la collaboration

La collaboration n'est pas un concept complexe. Elle peut en fait se résumer en une douzaine de mots : « deux personnes ou plus qui travaillent ensemble pour atteindre un but commun ». Au niveau le plus fondamental, cela pourrait signifier deux personnes qui travaillent ensemble pour changer un pneu crevé sur une voiture. Lorsque des groupes plus nombreux travaillent ensemble pour résoudre des problèmes plus difficiles et complexes, le processus collaboratif prend de l'ampleur et la définition de ce que constitue la collaboration commence à se multiplier et à diverger. Lorsque ces groupes proviennent de différents horizons organisationnels ayant des cultures, des politiques, des présomptions et des priorités particulières, la définition de la collaboration efficace peut représenter tout un défi en ce qui a trait dans les concepts et dans la pratique.

> Resserrer les écarts entre le gouvernement et l'industrie en ce qui concerne ce que chacun veut et s'attend d'avoir de l'autre par l'entremise de la collaboration est essentiel à la réussite.

La collaboration entre les secteurs public et privé est un bel exemple. Cette forme de collaboration a été définie de bien des façons. Examiné sous la loupe de la « gouvernance collaborative », elle a été définie comme étant « un arrangement de gouvernance où un ou plusieurs organismes mobilisent directement des intervenants ne faisant pas partie de l'État dans un processus officiel de prise de décision, axé sur le consensus et délibératif, qui vise à élaborer ou à mettre en œuvre une politique publique ou à gérer des programmes ou des actifs publics ».[9] D'un autre côté, lorsqu'on l'examine sous la loupe des « partenariats publics-privés » (P3), cette collaboration a été définie comme étant « une entente entre des acteurs publics et privés d'offrir certains services ou de réaliser certaines tâches », et qui peut être « plus axée sur la coordination que sur la prise de décision formelle et consensuelle ».[10]

Entre ces définitions, et bien d'autres,[11] il existe un large spectre de points de vue de ce que constitue la collaboration entre les secteurs public et privé. Elle s'étend du partage direct d'information et des activités de gestion de l'information entre les intervenants, aux partenariats hautement coopératifs dans lesquels le gouvernement et ses partenaires de l'industrie se mobilisent dans la co-création et la prestation de solutions (voir la figure 1 ci-dessous). Le resserrement de l'écart entre l'industrie et le gouvernement relativement à ce que chacun veut et à ce qu'il s'attend à obtenir de l'autre partie par la collaboration est essentiel au succès.

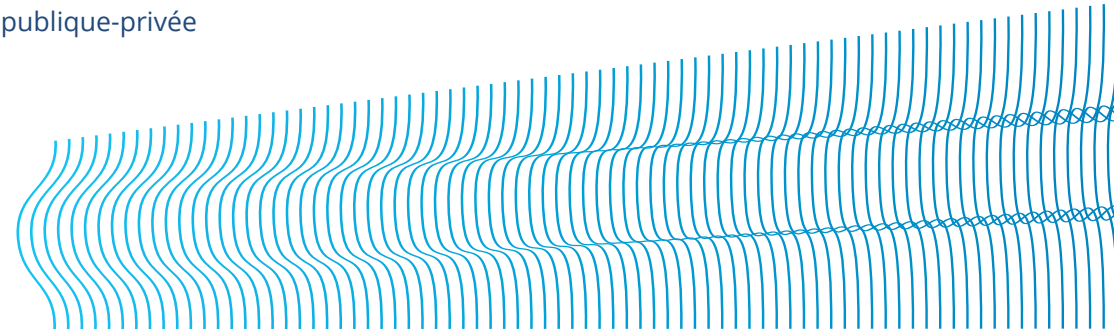
9 Ansell and Gash, 2008

10 IBID

11 For more information, see Freeman, 1997; Smith, 1998; Reilly, 1998; Padilla and Daigle, 1998; Beierle and Long, 1999; Walter and Petr, 2000; Seidenfeld, 2000; Prahalad and Ramaswamy, 2000; Connick and Innes, 2003; Porter and Kramer, 2011.

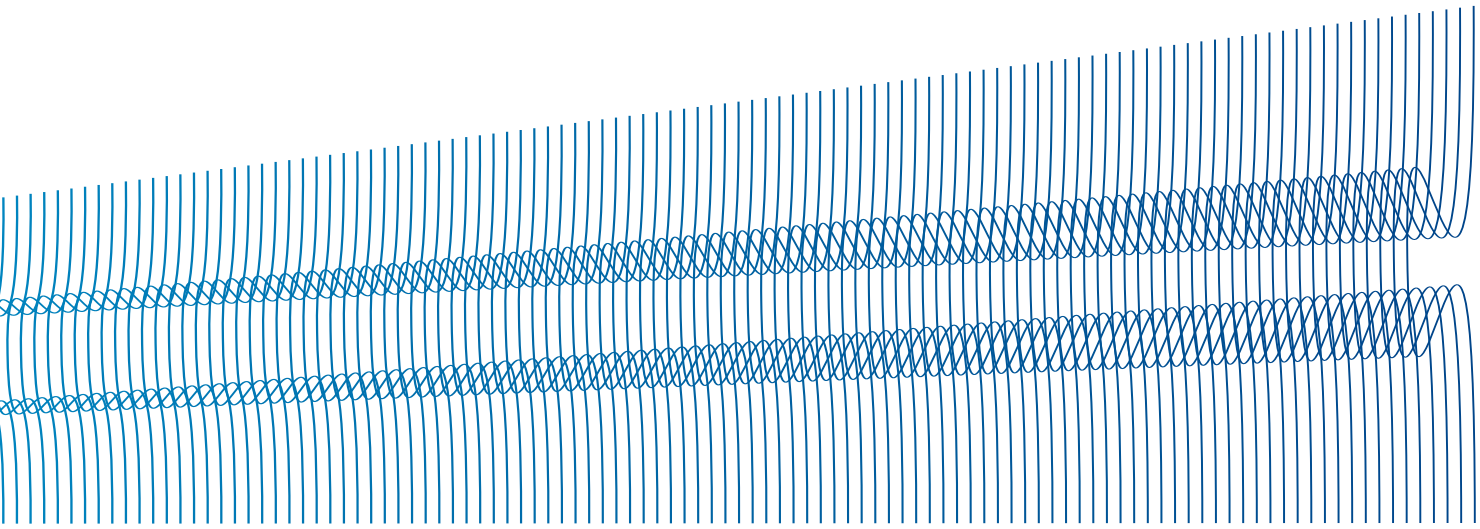
Le nouveau spectre de la collaboration

Figure 1
Le spectre de la collaboration publique-privée



	Niveau 1 **Informer**	Niveau 2 **Consulter**
Principal objectif de la collaboration à ce niveau	Fournir au secteur privé de l'information objective et équilibrée pour l'aider à comprendre le problème, les options ou les solutions.	Obtenir une rétroaction constructive de la part du secteur privé sur l'analyse du problème, ou sur les options ou les solutions élaborées par le gouvernement en réponse au problème.
Comment cela fonctionne en pratique	Le gouvernement garde le secteur privé informé sur les enjeux critiques, mais la communication bidirectionnelle est limitée.	Le gouvernement écoute le point de vue du secteur privé et donne de la rétroaction sur la manière dont cet apport a influencé le processus de prise de décision.

Heureusement, la nouvelle recherche a commencé à rationaliser ces points de vue divergents. En positionnant les activités collaboratives sur un spectre progressif où croissent progressivement la confiance dans le secteur privé et les responsabilités qui lui sont confiées quant à la détermination et à la mise en œuvre de solutions, un nouveau modèle a été créé. Les activités de collaboration auparavant dissociées sont désormais organisées dans une séquence (voir la figure 1). Les approches collaboratives situées à gauche du spectre nécessitent un niveau minime d'engagement bilatéral entre le gouvernement et l'industrie. C'est pourquoi ces approches conviennent mieux aux activités comme la sensibilisation, les campagnes de communication et la gestion traditionnelle des intervenants. Les approches situées à droite du spectre nécessitent des relations de travail grandement intégrées entre le gouvernement et l'industrie et un plus grand partage des responsabilités et de l'obligation de rendre des comptes dans la mise en œuvre des solutions. Elles conviennent alors davantage aux initiatives comme la création de programmes d'échange de talents ou de centres de développement rapide des capacités. Il faut aussi souligner qu'un « seuil de confiance » implicite doit être passé pour progresser tout au long du



Niveau 3
Mobiliser

Travailler directement et de manière constante avec le secteur privé tout au long de la détermination du problème et du processus d'analyse, ainsi que dans la formulation de solutions.

Le gouvernement travaille avec le secteur privé pour s'assurer que l'apport de l'industrie se reflète directement dans la détermination adéquate et l'analyse du problème, et dans l'élaboration de solutions alternatives.

Niveau 4
Collaborer

Travailler avec le secteur privé dans chacun des volets de la détermination et de la résolution du problème, placer sa confiance dans le secteur privé à la fois pour l'élaboration et pour la mise en œuvre de la solution.

Le gouvernement travaille main dans la main avec le secteur privé à chacune des étapes de la détermination du problème et de l'élaboration des solutions, et a confiance que l'industrie jouera un rôle défini dans la prestation des solutions.

Niveau 5
Diriger

Remettre la responsabilité de l'élaboration et de la mise en œuvre de la solution entre les mains du secteur privé, appuyé par le gouvernement, lorsque c'est approprié.

Le gouvernement délègue la responsabilité de résoudre le problème au secteur privé et met en place les contrôles nécessaires pour s'assurer de la mise en œuvre adéquate des solutions.

spectre. La reddition de comptes dans l'élaboration des résultats est de plus en plus partagée, le gouvernement délègue plus de ses responsabilités aux acteurs non gouvernementaux. La figure 1 ci-dessus met en lumière ce nouveau spectre de la collaboration.

Selon la recherche de l'AICDS, qui comprend des interviews avec des experts en cybernétique du gouvernement et de l'industrie, la plupart des formes de collaboration présentement employées par le gouvernement du Canada se situent entre les étapes 1 et 3. Le Programme de coopération en matière de sécurité lancé récemment par Sécurité publique Canada semble être l'un des rares nouveaux mécanismes utilisés officiellement par le gouvernement pour passer à la quatrième étape de la collaboration. Bien ce que programme soit nouveau et qu'il n'ait pas encore fait ses preuves, il indique l'intention du gouvernement d'essayer de prendre de nouveaux arrangements où la confiance grandit et où l'industrie a la responsabilité de résoudre certains des problèmes les plus pressants du Canada en matière de cyberdéfense et de cybersécurité.

L'IMPÉRATIF DE LA COLLABORATION EN **CYBERDÉFENSE ET EN CYBERSÉCURITÉ**

Pourquoi les gouvernements tiennent-ils à la collaboration?

Les gouvernements ne sont pas bien outillés pour s'attaquer seuls aux défis de la cyberdéfense et de la cybersécurité. La nature de la « cyberpuissance » change et évolue à une vitesse trop rapide pour permettre aux modèles de gouvernance, aux systèmes d'approvisionnement et aux cadres décisionnels existants du secteur public de réagir. Comme l'une des personnes interviewées l'a remarqué, « la cybernétique représente un défi bien plus grand que l'ensemble de compétences, les ressources, les capacités ou les connaissances d'un des acteurs ».

De nouvelles connaissances, technologies et pratiques et de nouveaux outils irradient dans toutes les directions de plus en plus rapidement. Nos alliés ont reconnu ouvertement que tenter de repousser sans fin les frontières cybernétiques et numériques en suivant la cadence n'était désormais plus possible : il n'est plus possible pour une organisation à elle seule de diriger la capacité intellectuelle requise ou d'avoir l'empreinte opérationnelle nécessaire pour accomplir la tâche toute seule. Protéger l'utilité du domaine cybernétique nécessite la formation de partenariats avec un large éventail d'intervenants afin de demeurer au courant des avancées aux points stratégiques le long de cette frontière technologique, et de rester connecté à l'expertise et aux compétences qui peuvent rapidement rendre opérationnelles de nouvelles capacités visant à contrer les innovations des adversaires.

Voir la figure 2 à la page suivante.

Pour les économies de marché démocratiques comme celle du Canada, cet enjeu est encore plus crucial, car les adversaires et rivaux clés, y compris la Chine et la Russie, ne composent pas avec la même charge administrative, législative et éthique qui réduisent l'agilité et diminuent la vitesse à laquelle sont acquises les nouvelles technologies. Leurs industries nationalisées des télécommunications et de la sécurité collaborent étroitement avec un ensemble composé de services de renseignements nationaux, de l'armée, de laboratoires de recherche gouvernementaux et (à l'occasion) le crime organisé. Ces adversaires sont donc bien équipés pour innover rapidement et agir de manière offensive contre le Canada et ses alliés. Ces États reconnaissent l'interopérabilité perméable au sein de leurs cyberécosystèmes comme étant un énorme avantage stratégique et maximisent leurs efforts pour l'exploiter.

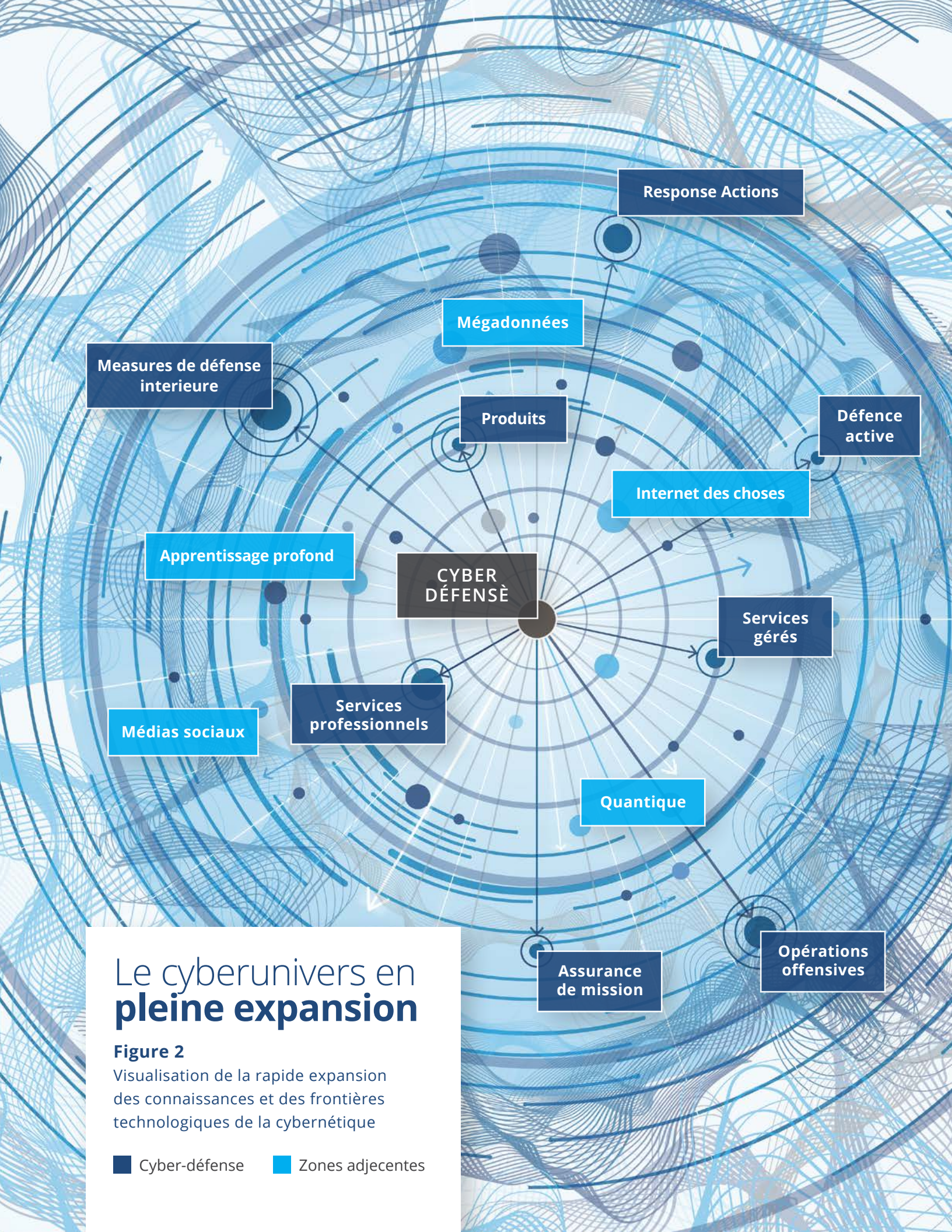
> Protéger l'utilité du domaine cybernétique nécessite la formation de partenariats avec la plus grande diversité d'intervenants afin de demeurer connecté rapidement aux connaissances et aux compétences émergentes tout le long de la frontière technologique.

Que peut offrir le secteur privé?

L'économie des marchés démocratiques n'a pas à affronter leurs cyberadversaires seuls. Au Canada et dans les pays étudiés, le secteur privé offre une manne d'expertise reconnue et un ensemble diversifié et solide de capacités que le gouvernement à lui seul ne peut posséder.

Les entreprises du secteur privé possèdent et gèrent la majorité de l'infrastructure critique au pays et ont un aperçu unique de la manière dont le domaine peut être refaçonné dans une optique de sécurité. Elles sont aussi les principaux moteurs de la cyberinnovation dans les technologies, les outils et les pratiques, en plus d'être constamment mobilisées dans le développement de nouvelles capacités novatrices visant à résoudre des cyberproblèmes dans le monde réel. Elles ont prouvé leur aptitude à offrir un éventail de cybersolutions et de services déterminants aux organismes publics et privés, grâce à un arsenal défensif et offensif en constante évolution.

De plus en plus, les entreprises du secteur privé deviennent des cibles de choix des attaquants les plus avancés et les plus persistants du domaine cybernétique. Cette exposition au premier plan leur donne un aperçu incomparable de la manière dont la menace cybernétique se transforme, ce qui leur permet de déterminer rapidement les lacunes dans les capacités, puis de les combler par le développement de nouvelles technologies, d'outils et de pratiques à une vitesse cybernétique (en 10 mois ou moins). Les secteurs où les cyberentreprises canadiennes ont fait leurs preuves sont présentés dans le rapport de mars 2019 de l'AICDS, « From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence ».



Le cyberunivers en **pleine expansion**

Figure 2

Visualisation de la rapide expansion des connaissances et des frontières technologiques de la cybernétique

Cyber-défense Zones adjecentes

Réfléchissons à l'approche heuristique suivante. La croissance du domaine numérique ressemble un peu au Big Bang : dans l'espace d'un instant, nous avons créé un nouvel univers numérique qui prend de l'expansion. Mais contrairement à la violente explosion de matière dans toutes les directions de l'espace, les technologies numériques ont explosé à travers pratiquement toutes les facettes de notre société et elles sont interreliées. Dans un rapport publié en 2016, l'Internet Security Alliance note que les technologies numériques « affectent virtuellement tous les aspects de nos vies, de notre physiologie à notre identité, en passant par notre manière d'élaborer et de gérer nos relations, la signification de nos valeurs profondes comme le respect de notre vie privée, et bon nombre des présomptions de longue date à propos des enjeux nationaux comme l'économie et la défense nationale ». Mais ce qui est encore plus important, cet univers continue de prendre de l'expansion dans toutes les directions, à un rythme de plus en plus rapide.

Repousser sans fin la frontière technologique de la cybernétique a atteint un point de non-retour, aucune organisation ne peut à elle seule accomplir cette tâche. Cette nouvelle réalité comporte une conclusion inévitable : protéger l'utilité du domaine cybernétique nécessite la formation de partenariats avec le plus large éventail d'intervenants, afin de toujours demeurer au courant des avancées tout le long de cette nouvelle frontière technologique; afin de demeurer connectées à l'expertise et aux compétences émergentes qui peuvent rapidement rendre opérationnelles les nouvelles capacités; et afin de contrer les innovations adverses partout où elles surviennent. Les partenariats et les relations collaboratives doivent être recherchés et assurés avec ceux qui se trouvent à cette frontière pour avoir une chance de réussir. Ces partenariats et ces relations doivent être entretenus avec une vigueur et une intensité correspondant à l'explosivité sous-jacente du domaine.

VERS UN MODÈLE GLOBAL DE COLLABORATION **PUBLIQUE-PRIVÉE POUR LA CYBERDÉFENSE**

Tous les principaux alliés du Canada participent activement à de multiples formes de collaboration avec le secteur privé afin de relever les défis de tout le domaine de la cybersécurité. Non seulement elles forgent de solides relations avec le secteur privé, relations qui seront précieuses pour devenir de plus agile devant la rapide innovation de la cybernétique, mais elles améliorent aussi leur capacité à défendre le gouvernement, les entreprises et les citoyens contre les menaces actuelles et jettent les bases d'une approche unifiée qui limitera l'impact de cyberattaques et de cyberagressions de la part des États adverses.

La recherche de l'AICDS montre clairement la valeur de la collaboration des alliés du Canada en matière de cyberdéfense, mais elle présente également une liste de facteurs de réussites et de principales pratiques utilisés par les alliés. Lorsqu'on les examine dans leur ensemble, les facteurs de réussite et les pratiques peuvent être combinés pour jeter les bases d'un modèle global de collaboration publique-privée en matière de cyberdéfense. Cette collaboration peut être facilement adaptée et mise en œuvre de manière sélective afin de répondre au cyberenvironnement et aux enjeux uniques d'un pays.

Toutefois, il est important de souligner qu'aucun des alliés du Canada n'a encore élaboré, mis à l'essai ou mis en œuvre des modèles ou des stratégies qui relient leur ensemble entier d'activités de collaboration dans un cadre unifié. Quelques-uns ont commencé à expérimenter et à combiner des activités, comme le développement rapide des capacités avec des environnements réels ou simulés de mise à l'essai. Aucun n'a élaboré de cadre global qui harmonise une concentration de ressources et de programmes

collaboratifs autour d'un ensemble commun d'objectifs établis et de résultats conjoints entre le gouvernement et l'industrie.

> Le Canada doit élaborer des stratégies plus globales qui relient plus des zones de cyberinfluence avec les capacités, et il doit trouver les moyens d'anticiper la manière dont ses adversaires les utiliseront, en combinaison, contre nous.

Il y a sûrement plusieurs raisons à cela, l'une étant évidemment que la plupart des activités collaboratives ayant émergé dans les systèmes de nos alliés répondaient à des besoins urgents, plutôt que d'avoir été le fruit d'une planification délibérée à long terme. Il est aussi peu probable qu'un cyberexpert aurait pu prédire les manières dont les technologies numériques et cybernétiques commenceraient à se chevaucher et produiraient des résultats inattendus. Par exemple, la combinaison de l'analyse des mégadonnées, du profilage psychologique en ligne des électeurs, de l'influence des campagnes dans les médias sociaux, des techniques avancées de modification du comportement, et des algorithmes de communications utilisées comme arme pour influencer les électeurs et des élections à l'échelle mondiale (pensons à Brexit et à Cambridge Analytica). Maintenant que, comme le dit l'expression populaire, le chat est sorti du sac, les pays devront commencer à élaborer des stratégies plus globales qui relient plus de ces zones d'influence cybernétique et numérique qui se chevauchent avec les capacités, en plus de trouver les moyens d'anticiper les différentes combinaisons pouvant être utilisées contre le Canada.

PRINCIPALES FONCTIONS, POLITIQUES ET **PRATIQUES DE COLLABORATION DES ALLIÉS DU CANADA**

Chaque pays a ses propres réalités géopolitiques, économiques, sociales et culturelles. Lorsque ces réalités sont combinées avec différents environnements opérationnels, structures d'écosystème et politiques, il est peu probable qu'un seul et unique modèle de collaboration pourrait répondre à tous leurs besoins. Comme l'a fait remarquer un des représentants du gouvernement interviewés, « les pratiques exemplaires ne sont pas toujours transférables d'un pays à l'autre, ou même d'un ministère à l'autre, parce qu'il faut reconnaître que les gouvernements sont fondamentalement différents ». Cependant, les alliés du Canada ont réussi avec un ensemble ciblé de pratiques dans leur propre environnement. Certaines pourraient être applicables dans l'environnement canadien. Chacune d'elles offre un avantage utile pour améliorer l'efficacité et l'adaptabilité des approches actuelles du Canada dans la collaboration publique-privée de la cyberdéfense.

Vus en agrégés, ces éléments peuvent être regroupés avec une relative exactitude dans l'un des quatre domaines d'intérêt de la cybercollaboration. :

1. Gouvernance, stratégie, politique et programmes
2. Missions et opérations
3. Protection des actifs essentiels
4. Développement de la technologie

De nouveaux domaines d'intérêt peuvent être ajoutés avec le temps, à mesure que de nouvelles activités, politiques habilitantes et principales pratiques émergent et sont validées. Pour l'instant, les seize grandes pratiques déterminées et validées par l'analyse d'études de cas et interviews avec les experts peuvent être regroupées logiquement dans la structure suivante.

Principales activités, politiques et pratiques

Gouvernance, stratégie, politique et programmes

- Structures de coordination et de coopération permanentes à l'échelon national
- Structures de gouvernance collaborative dans la mise en œuvre des programmes
- Réforme de l'approvisionnement
- Autres autorités transactionnelles
- Exigences opérationnelles urgentes

Missions et opérations

- Intégration approfondie des détenteurs de contrat dans les opérations du gouvernement
- Environnements de mise à l'essai des capacités et plages expérimentales en cybernétique
- Programme d'échange de talents
- Planification des scénarios et exercices conjoints

Protection des actifs essentiels

- Cadres de protection de l'infrastructure critique élaborés conjointement
- Centres d'analyse et de partage d'information

Développement de la technologie

- Centres d'innovation et d'accélération cybernétiques
- Centres de développement rapide et de déploiement des capacités
- Coopérative de recherche et de développement
- Feuilles de route technologiques
- Réseaux d'innovation et de collaboration gérés par l'industrie

1. Gouvernance, stratégie, politique et programmes

1.a. Coordination et coopération permanentes à l'échelon national

Les États-Unis s'efforcent de maximiser l'unisson des politiques, des stratégies et des opérations de cyberdéfense et de cybersécurité entre les départements, les agences et le secteur privé : un effort considérable de coordination et de gouvernance. Ces investissements ont porté leurs fruits.

Au printemps 2012, par exemple, le gouvernement a collaboré avec succès avec ses partenaires de l'industrie afin de limiter l'impact d'une attaque de déni de service distribué contre les banques américaines. En coopération avec 120 pays de différents niveaux diplomatiques, technologiques et opérationnels, ils ont pu freiner le trafic malicieux en cours partout dans le monde. Ces mesures n'ont pas mis un terme une fois pour toutes aux attaques, mais l'effet adverse sur les banques a été considérablement réduit,[12] ce qui leur a permis de reprendre pied et de reprendre le contrôle de leurs systèmes. Ce résultat a été rendu possible grâce aux discussions récurrentes et à la planification de scénarios tenues de manière permanente dans le construit du National Infrastructure Protection Plan (NIPP), plus particulièrement grâce aux Sector Coordinating Councils (SCC) et aux Government Coordinating Councils (GCC) harmonisés. Dans le cadre du NIPP, le gouvernement et les principaux représentants de l'industrie ont déjà eu de longues discussions axées sur l'élaboration d'une réponse conjointe à une attaque semblable provenant de l'intérieur des États-Unis, et ont déjà pris part à des exercices à cette fin. Lorsque cette attaque multinationale a été lancée, le plan existant a été mis en œuvre rapidement. Tout le monde connaissait son rôle, savait ce que les homologues internationaux avaient à faire, connaissait exactement les étapes pour mener le projet à bien, pour réussir à démanteler l'attaque. Mais ce qui est encore plus important, lorsque les autres départements et agences devaient se mobiliser, le Département d'État, par exemple, a pu accepter de travailler avec l'industrie plus rapidement et directement. Les partenaires actuels du gouvernement avaient déjà approuvé les partenaires de l'industrie et avaient bâti des relations de longue date fondées sur la confiance.

Cet exemple montre que les construits collaboratifs, traditionnellement restreints à une vue étroite et défensive de la protection de l'infrastructure critique, pourraient être utilisés pour soutenir un ensemble plus large d'activités stratégiques, opérationnelles et de coordination. Cette tendance a démarré avec les différents SCC ayant contribué aux discussions de haut niveau au sujet des politiques, des programmes, des opérations et de l'économie et ayant mobilisé leurs homologues des GCC.

1.b. Structures de gouvernance collaborative dans la mise en œuvre des programmes

Un thème global a émergé de la recherche et des interviews effectués dans le cadre de ce rapport : la grande importance de rôles bien définis et clairement expliqués pour tous les acteurs d'une collaboration publique-privée. Bon nombre des personnes interviewées ont souligné que sans une répartition claire et équitable des responsabilités et des tâches, et d'une responsabilité conjointe, une collaboration fructueuse est impossible. Aux États-Unis, la création du IT Sector Baseline Risk Assessment s'est avérée être une initiative de collaboration fructueuse entre le gouvernement et l'industrie. Parmi les facteurs de réussite cités par les participants du gouvernement et de l'industrie figurait la désignation de coprésidents provenant du gouvernement et de l'industrie, ce qui a assuré « une reddition de comptes et une autorité conjointes, où les rôles et responsabilités étaient définis pour chacun des coprésidents ».[13] L'exemple du NIPP cité précédemment dérive grandement de son succès résultant du jumelage du construit des SSC et des GCC, qui assure un niveau équivalent de contrôle conjoint de la part du gouvernement et de l'industrie sur la planification et la mise en œuvre des activités, en plus de mettre l'accent sur la reddition de comptes conjointe en ce qui a trait aux résultats.

1.c. Réforme de l'approvisionnement

Les personnes interviewées aux fins de ce projet de recherche ont souligné à maintes reprises le besoin pour le gouvernement du Canada d'adopter des pratiques de pointe en ce qui a trait à l'acquisition de produits et de services. Les hauts représentants du secteur privé interviewés ont laissé entendre que lorsqu'on les compare aux pratiques actuelles du gouvernement en matière d'approvisionnement

(qui se concentrent majoritairement sur le respect d'exigences détaillées et le principe du plus bas soumissionnaire), les approches fondées sur les capacités offrent l'avantage d'être plus simples, plus rapides, plus précises et plus efficaces. Les industries canadiennes souhaitent sincèrement aider à assurer la cybersécurité. Les approches axées sur les résultats et fondées sur les capacités sont importantes et constituent une valeur ajoutée certaine dans la passation des marchés indépendants. L'importance de l'approvisionnement dans une collaboration fructueuse à long terme ne peut être sous-estimée. Un haut représentant du gouvernement a indiqué que « si nous ne pouvons pas récolter le fruit de nos efforts, personne n'en sortira gagnant et la volonté de collaborer va s'estomper ». Visiblement, il manque au Canada un mécanisme récurrent entre le gouvernement et l'industrie pour discuter de ces questions et d'autres enjeux réglementaires et économiques qui touchent le domaine de la cybersécurité. Les construits comme les Tables sectorielles de stratégies économiques semblent être tout indiqués pour répondre à ce type d'enjeux, et elles ont eu un certain succès au Canada jusqu'à présent.

« Si nous ne pouvons pas récolter le fruit de nos efforts, personne n'en sortira gagnant et la volonté de collaborer va s'estomper. »

1.d. Autres autorités transactionnelles

Un autre principal facteur facilitant la collaboration cité tout au long des interviews du projet était les autres autorités transactionnelles. Employées notamment par la Defense Innovation Unit du département de la défense américain, ces autorités transactionnelles visent à simplifier les acquisitions en matière de défense dans des secteurs précis et existent en parallèle avec les règles d'approvisionnement utilisées dans les systèmes de défense traditionnels. Le département de la défense a l'autorité permanente d'effectuer « d'autres transactions » pour la recherche, le développement de prototypes et la production, ce qui lui donne « la flexibilité nécessaire pour adopter et intégrer les pratiques d'affaires qui traduisent les normes et les pratiques exemplaires de l'industrie commerciale en instruments de contrat ».[14] Le tournant des autres autorités transactionnelles, qui existent depuis assez longtemps, mais n'ont été généralement reconnus et utilisés que récemment, a été lorsque les agents d'approvisionnement ont reçu la directive d'y avoir recours à moins de pouvoir trouver une raison défendable et contraignante de ne pas le faire. Un changement nécessaire dans le focus, qui a été vu comme étant essentiel à leur montée fulgurante. À l'heure actuelle, les autres autorités transactionnelles se situent au cœur de bon nombre de programmes américains qui visent à créer des environnements où le gouvernement et l'industrie peuvent travailler conjointement pour déterminer, élaborer et mettre à l'essai et déployer des solutions aux problèmes émergents.

12 U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks, Washington Post, Ellen Nakashima, Apr 2014.

13 Best Practices for Operating Government-Industry Partnerships in Cyber Security, Journal of Strategic Security, Larry Clinton, Winter 2015.

14 Other Transaction Authority Guide, Defense Acquisition University, Dec 2018.

1.e. Exigences opérationnelles urgentes

L'adoption d'un autre facteur facilitant, les exigences opérationnelles urgentes, a grandement amélioré le système d'approvisionnement des États-Unis dans le domaine de la défense. Puisque les processus standards du department of défense ne facilitaient pas le déploiement au début des années 2000,[15] les États-Unis ont largement reconnu l'importance d'une réponse manière cohérente et rapide dans l'environnement complexe de sécurité du XXIe siècle. Les États Unis ont aussi appliqué les exigences opérationnelles urgentes au domaine de la cyberdéfense. Dans l'ensemble des instruments d'approvisionnement des États-Unis, les exigences opérationnelles urgentes sont liées aux autres autorités transactionnelles, ce qui permet au department of défense, entre autres, d'activer les canaux spéciaux de l'approvisionnement qui surpassent les moyens plus encombrants et traditionnels, mais qui ne sont pas restreints aux activités de recherche-développement ou de production rapide de prototypes.

15 Fulfillment of Urgent Operational Needs, University of Maryland, Jacques Gansler, Apr 2010.

2. Missions et opérations

2.a. Intégration approfondie des détenteurs de contrat dans les opérations du gouvernement

Faisant fond sur la réponse conjointe fructueuse face à attaque de déni de service distribué des banques américaines en 2012, dans sa National Security Strategy de 2018, le department of défense américain met encore plus l'accent sur le besoin de collaborer avec les partenaires de l'industrie dans les domaines physiques et cybernétiques. Pour respecter ses priorités en matière de cybernétiques, le gouvernement des États-Unis a réaffirmé son engagement, et les mécanismes nécessaires pour le respecter, de collaborer étroitement avec l'industrie privée. Cet engagement comprend le recours aux connaissances, aux outils et aux ressources en experts de l'industrie pour compléter les efforts du gouvernement. Dans l'ensemble, les alliés du Canada dépendent d'une bien plus grande intégration civile et entrepreneuriale dans des réseaux critiques et des environnements opérationnels et l'encouragent, allant même jusqu'à atteindre un équilibre 50/50, selon les personnes interviewées ayant une expérience approfondie des opérations alliées. Les agences de sécurité nationale canadiennes semblent exceptionnellement réticentes à accepter et à adopter cette pratique. Elles vont même parfois jusqu'à voir cette dépendance à l'intégration civile et entrepreneuriale comme étant une déficience interne au lieu d'un atout stratégique.

> Les alliés du Canada dépendent d'une bien plus grande intégration civile et entrepreneuriale dans des réseaux critiques et des environnements opérationnels et l'encouragent, atteignant même parfois un équilibre 50/50.

2.b. Environnements de mise à l'essai des capacités et plages expérimentales en cybernétique

De nombreuses personnes interviewées ont parlé du concept et de la valeur d'une plage expérimentale cybernétique, c'est-à-dire un environnement expérimental ou un polygone d'essai virtuel où l'industrie et le gouvernement peut évaluer les technologies potentielles et émergentes et éliminer les risques des solutions grâce à des données et à des réseaux uniques générés, contrôlés ou appartenant au gouvernement ou à l'armée, lorsqu'ils existent. Par exemple, dans certains pays étudiés, seule l'armée possède des données réelles sur la manière dont des systèmes d'armes complexes fonctionnent et interagissent avec d'autres systèmes sur un champ de bataille. Transposer ces données dans une plage expérimentale cybernétique permet aux entreprises qualifiées de tester et d'élaborer de meilleures solutions relatives à l'assurance de la mission et à la résilience de ces systèmes, en plus de déterminer les interdépendances possibles entre ceux-ci et les tactiques de l'adversaire. Pour les petits investisseurs, qui ne peuvent peut-être pas se permettre de mener des tests et des évaluations à grande échelle, une plage expérimentale cybernétique offre un environnement où les solutions émergentes peuvent être confrontées aux défis connus et combinées avec leurs propres données tirées des systèmes qu'ils ont créés. Pour le gouvernement, cet outil donne l'occasion d'évaluer des solutions et de mieux comprendre les développements de pointe. Pour les participants de l'industrie, le gouvernement offre un accès à des ensembles de données uniques et à des réseaux modélisés ayant des exigences et présentant des défis qu'il est peu probable de rencontrer dans le secteur privé, en plus de la possibilité d'obtenir de la rétroaction de l'armée ou des utilisateurs finaux de la sécurité nationale.

2.c. Programmes d'échange de talents

Au Royaume-Uni, le programme Industry 100 permet aux experts de l'industrie de travailler directement avec le National Cyber Security Center (NCSC). On assigne à ces experts des postes à court terme sur mesure au NCSC, habituellement à temps partiel. Ils ont donc la possibilité de comprendre et de remettre en question la manière de penser du gouvernement et la manière dont il met à l'essai les idées novatrices dans l'environnement gouvernemental. En général, Industry 100 favorise une meilleure compréhension mutuelle de la cybersécurité et l'élaboration de meilleures politiques en matière de cybernétique. Il améliore la prestation de programmes, aide le gouvernement et l'industrie à cibler les vulnérabilités des systèmes et réduit l'incidence future des cyberattaques.

3. Collaboration dans la protection des actifs essentiels

3.a. Cadres de protection de l'infrastructure critique élaborés conjointement

Aux États-Unis, l'élaboration du National Infrastructure Protection Plan (NIPP) a été qualifiée par le gouvernement et les participants de l'industrie de collaboration fructueuse menant à la création d'un cadre efficace de protection de l'infrastructure critique d'actifs du pays. Le gouvernement a mobilisé les propriétaires et les opérateurs d'infrastructure critique tout au long de l'élaboration du NIPP, afin de tenir compte du langage et des recommandations de l'industrie à chacune des étapes de développement du plan. Le gouvernement aussi fait preuve, aux échelons supérieurs, d'un engagement solide en faveur de l'élaboration et de l'intendance du plan, et en faveur de la direction de la mobilisation d'un grand nombre d'intervenants liés à l'infrastructure critique. Mais ce qui est le plus important, la mise en œuvre continue du plan est supervisée par des conseils de coordination conjoints formés par des membres du gouvernement et de l'industrie pour chacun des secteurs de l'infrastructure critique, assurant ainsi une collaboration gouvernement-industrie permanente dans la mise en œuvre du plan.

3.b. Centres d'analyse et de partage d'information

La plupart des pays alliés ont une certaine forme de collaboration entre le gouvernement et l'industrie relativement au partage de l'information sur les cybermenaces, les points vulnérables et les brèches. Les débats s'enflamment autour de la question de savoir si la participation à ce genre de construits devrait être volontaire ou réglementée, l'industrie et la majorité des intervenants universitaires étant en faveur d'une approche volontaire et incitative. Le concept du partage de l'information relative aux menaces entre différents acteurs de confiance pour améliorer considérablement la sensibilisation situationnelle est reconnu comme étant un élément essentiel à l'efficacité de la cyberdéfense nationale. Il demeure l'une des formes de collaboration les plus valorisées par le gouvernement et l'industrie, même si c'est pour des raisons quelque peu différentes (et parfois contradictoires). Les gouvernements qui ont créé ces réseaux espèrent avoir accès aux capteurs, aux données et aux réseaux privés, et être avertis immédiatement des brèches des systèmes privés essentiels. Les participants du secteur privé souhaitent un accès égal aux renseignements sensibles et aux connaissances opérationnelles souvent confidentielles ou appartenant à des concurrents qui ont fourni ces renseignements au gouvernement. Le secteur privé recherche également une orientation sur le type d'information jugée la plus utile par les gouvernements, en tant qu'acteur du milieu des renseignements liés aux menaces.

4. Développement de la technologie

4.a. Centres d'innovation et d'accélération cybernétiques

Au Royaume-Uni, le cyberaccélérateur du National Cyber Security Centre soutient la croissance de cyberentreprises qui s'efforcent à apporter de nouveaux produits de cybersécurité qui sont meilleurs, plus rapides et moins chers sur le marché. Lancé en 2017, le programme a depuis aidé 16 entreprises en démarrage par son soutien en matière de technologie, de leadership et d'orientation. En outre, le programme CyberInvest de ce pays rassemble les acteurs clés du gouvernement et de l'industrie pour investir dans le développement de la recherche de pointe en cybersécurité et soutenir ce développement dans l'ensemble du secteur universitaire du Royaume-Uni. Au total, 24 entreprises membres de CyberInvest se sont engagées à investir un minimum de 8 millions de livres au cours des cinq prochaines années.

En Australie, AustCyber agit à titre de multiplieur et de connecteur afin d'établir l'Australie en tant que leader dans le cybermarché mondial. Des Cyber Security Innovation Nodes (centre d'innovation en cybersécurité) ont été mis en place partout au pays et permettront aux entreprises en démarrage, aux corporations, aux universités et aux organismes gouvernementaux de partager de l'information et de stimuler l'innovation. L'Australie a également fondé le Cooperative Research Centre for Cyber Security (CSCRC) afin de faciliter la commercialisation et la recherche-développement propulsées par l'industrie en matière de cybersécurité.

4.b. Centres de développement rapide et de déploiement des capacités

Parmi les initiatives de collaboration étudiées, celles conçues pour accélérer la co-création de solutions technologiques pour la cyberdéfense et la cybersécurité sont peut-être les plus appréciées du gouvernement et de l'industrie. Le programme américain Army Futures Command (AFC) est l'un de ces programmes qui ressort comme étant une méthode de pointe en matière de collaboration du gouvernement avec l'industrie et de solutions d'approvisionnement à la « vitesse cybernétique ». À commencer par les questions fondamentales « Quelle sont les technologies nécessaires pour mener à bien notre mission? » et « Qui sont les innovateurs dans l'espace? », l'AFC vise à moderniser la capacité de l'armée par l'entremise d'une collaboration directe en recherche-développement et l'approvisionnement auprès des petites et moyennes entreprises et des milieux universitaires. L'organisme vise également à mettre en œuvre ces résultats la cohabitation des installations dans des centres d'innovation partout aux États-Unis afin « d'inciter les esprits les plus brillants à se concentrer sur les plus grands défis de l'armée ».

4.c. Coopérative de recherche et développement (CRADA)

Semblables en certains points aux plages expérimentales, les Coopératives de recherche et développement (CRADA) sont en fait une entente écrite entre un organisme gouvernemental (souvent un laboratoire de défense) et un intervenant privé ou une université pour qu'ils travaillent ensemble à la recherche-développement de nouvelles technologies. Le modèle de CRADA est très avantageux pour les petites entreprises technologiques, puisqu'il facilite le transfert des technologies et offre une occasion à faibles risques de collaborer et de tisser des liens avec les laboratoires de défense. Les CRADA ne versent pas de financement, mais elles permettent aux laboratoires de défense de mettre à la disposition des entreprises privées du personnel, l'accès aux installations, de l'équipement, des données et d'autres ressources, tout en étant ou non payées en retour.

> Les politiques, les outils et les pratiques soulignées dans le présent document ont le potentiel de jeter les bases d'un cadre de cyberdéfense particulièrement fort dans l'ensemble du pays.

4.d. Feuilles de route technologiques

Les feuilles de route technologiques de la cybersécurité et de la cyberdéfense constituent une autre des principales pratiques citées par les personnes interviewées. Les feuilles de route soutiennent la planification stratégique et à long terme de l'élaboration des produits et services, aident aux prévisions de l'horizon technologique et de l'ensemble connexe d'exigences gouvernementales en matière d'approvisionnement, et sont maintenues dans l'ensemble du dialogue structuré et significatif entre le gouvernement et les participants de l'industrie. Pour que les feuilles de route soient efficaces, il est essentiel que les objectifs à long terme soient accompagnés de la mise en œuvre de solutions technologiques précises à court et à long terme. Cela peut être un processus de développement des capacités où l'industrie et le gouvernement travaillent ensemble afin de définir l'horizon technologique et les défis connexes; de produire une analyse de la demande anticipée du marché et des changements dans l'offre de la technologie; d'élaborer une liste de solutions à privilégier; d'évaluer et de régler les problèmes présentés par les instruments de politique et de programmes existants; et, au bout du compte, de connecter la séquence des solutions proposées à l'évolution des acquisitions à venir du gouvernement. Le programme Niteworks au Royaume-Uni et le programme Rapid Prototyping, Development and Evaluation en Australie, qui a récemment été entièrement intégré à son Defence Innovation Hub, en sont des exemples.

4.e. Réseaux d'innovation et de collaboration gérés par l'industrie

Dans certains cas, les principales entreprises ayant établi de bonnes relations avec leur client, le gouvernement, et une bonne connaissance de l'intégration des systèmes complexes ont l'expérience de la navigation dans le milieu des acquisitions, tout en conservant la flexibilité requise pour incorporer de nouvelles technologies et pratiques dans leur chaîne d'approvisionnement. En grande partie, c'est parce qu'elles créent et gèrent leur propre écosystème d'innovation. Ouvrir ces écosystèmes aux PME ayant les grandes capacités mais sans les ressources pour répondre aux exigences techniques détaillées des demandes de propositions pourrait être une manière de produire une valeur ajoutée accrue relativement à la commercialisation de la plupart des innovations de pointe en cyberdéfense. Dans ce modèle, le gouvernement a uniquement besoin de maintenir ses relations avec quelques entreprises principales qui acquièrent une connaissance détaillée de leurs exigences en pleine évolution et qui peuvent adapter leur chaîne d'approvisionnement afin de réagir avec flexibilité et répondre au besoin. Dans d'autres cas, les grandes entreprises et les agents d'intégration peuvent valoriser leur propre capital de risque ou accélérateurs, ou encore former leur équipe et leur coentreprise pour promouvoir une mobilisation plus collaborative avec leur chaîne d'approvisionnement. Ainsi, ils ne font pas tout simplement augmenter le prix coûtant en ajoutant des fournisseurs supplémentaires. Ces approches visent à :

- réduire les obstacles à la participation des petites et moyennes entreprises;
- favoriser une meilleure concurrence;
- connecter le gouvernement avec un éventail plus large de technologies de pointe adaptées à leurs besoins uniques;
- placer une grande partie des activités de collaboration du côté de l'industrie;
- se concentrer sur des relations publiques-privées de haut niveau qui donnent le ton à la mobilisation en aval.

Il s'agit d'un concept émergent qui est privilégié par les principaux fabricants d'équipement d'origine, les agents d'intégration et certains représentants du gouvernement. L'incidence de ce concept sur les petites et moyennes entreprises et sur la santé durable à long terme de la base industrielle n'est pas définie.

Plus que la somme de leurs parties

Le portrait actuel des principales pratiques en matière de cybercollaboration est le résultat d'actions posées à différents moments, dans différents domaines et en réponse à des crises différentes, mais tout aussi urgentes, c'est-à-dire qu'elles ne sont absolument pas issues d'une action organisée ou stratégique. Toutefois, ensemble, elles présentent un construit étonnamment puissant en matière de cyberdéfense. Elles offrent un éventail d'activités de collaboration, permettent la mise en œuvre de politiques et de pratiques émergentes que les pays peuvent étudier afin de déterminer et de sélectionner les solutions adaptées à leur cyberenvironnement unique. Mises en œuvre dans le cadre de partenariats collaboratifs avec un grand nombre d'industries, de groupes universitaires et d'autres intervenants du gouvernement, elles ont le potentiel de jeter les bases d'une cyberdéfense particulièrement forte dans l'ensemble du pays.

PRINCIPAUX FACTEURS **MENANT À UNE COLLABORATION FRUCTUEUSE**

Après l'examen de six études de cas de projets de collaboration axés sur la cybernétique a été diffusé par le Department of Homeland Security américain, et appuyé par une recherche universitaire sur de nouveaux concepts comme « l'impact collectif »[16] (Stanford) et « la création d'une valeur partagée »[17] (Harvard), quinze principes directeurs et facteurs de réussite de la collaboration « qui génèrent constamment des programmes de partenariats fructueux concernant la maintenance au niveau fondamental et opérationnel »[18] ont été déterminés.

Ces facteurs de réussite sont différents des 16 principales activités, politiques et pratiques des alliés soulignées ci-dessus. Ils sont aussi davantage axés vers la gestion d'une relation saine et productive entre le gouvernement et l'industrie dans le cadre d'un processus collaboratif.

Comme l'a fait remarquer une des personnes interviewées, « la résolution de problèmes touche le fond et les relations, et la plupart des gens oublient les relations ». Les activités, les politiques et les pratiques citées précédemment concernent les éléments de fond de ce qui doit être fait pour réagir aux cyberdéfis ciblés, mais les facteurs de réussite soulignée ci-dessous devraient être considérés comme étant une combinaison des principes et comportements modèles qui, si l'on s'y tient, présentent les meilleures chances de bâtir des relations collaboratives fructueuses entre le gouvernement et l'industrie, d'où fleuriront sans problème des activités couronnées de succès. Les quinze principaux facteurs de réussite sont les suivants :

1. Le gouvernement devrait chercher à avoir l'avis du secteur privé dès le départ, idéalement à l'étape de la détermination de la grande priorité et de l'objectif initial de tout projet collaboratif, et non pas uniquement au moment de la mise en œuvre.
2. Un programme commun devrait être élaboré pour motiver les participants à atteindre une vision commune de ce qui doit être fait, en plus de faire la clarté sur ce que chaque participant est prêt à accomplir en vue de l'élaboration et de la mise en œuvre des solutions.
3. Les hauts dirigeants du gouvernement et de l'industrie doivent s'engager à collaborer. Cet engagement doit être communiqué de manière constante et démontré au personnel de soutien et aux intervenants dévoués et mobilisés.

> « La résolution de problèmes touche le fond et les relations, et la plupart des gens oublient les relations ». Agir de la sorte dans le domaine cybernétique se soldera assurément par un échec.

4. Un modèle ou un processus reconnu (qui a déjà fait ses preuves auprès du gouvernement et des intervenants de l'industrie) devrait être utilisé toutes les fois où c'est possible pour structurer les activités de collaboration. Idéalement, ce modèle en soit aurait été élaboré conjointement avec l'industrie. (par exemple, NIPP aux États-Unis, le Forum national intersectoriel et les Tables sectorielles de stratégies économiques au Canada).

5. La communication avec les intervenants doit être élargie et commencer tôt, idéalement à l'étape de la « page blanche ».

6. Une interaction et une communication continues doivent être maintenues entre le gouvernement et les intervenants de l'industrie. Cela peut se faire par l'entremise de forums permanents et récurrents ou d'interactions régulières, l'envoi de courriels, la prise d'engagements et la mise en place de projets conjoints. Cette communication et cette interaction sont essentielles à la coordination d'activités conjointes, à l'établissement de la confiance et au maintien de la lancée des projets.

7. Le gouvernement doit laisser aux intervenants assez de temps pour étudier le matériel, les requêtes, les demandes de décisions, etc., et y réagir (une période équivalant à celle prise par le gouvernement pour étudier des enjeux similaires).

8. Une direction conjointe ou des rôles de leadership partagé mutuellement acceptables devraient être créés dans l'ensemble des programmes et des activités. Le gouvernement et l'industrie peuvent tous deux prendre les commandes dans les domaines qui leur conviennent le mieux, mais une collaboration d'envergure nécessite un certain leadership équitable.

9. La prise de décisions devrait d'emblée être axée sur les consensus. Toute exception devrait être communiquée aux intervenants le plus tôt possible et de manière transparente.

10. Les activités devraient se renforcer mutuellement pour que même si les participants ne font pas tous la même chose pour contribuer aux objectifs du projet, chacun d'eux investisse son énergie et ses ressources où il peut avoir le plus grand impact, tout en contribuant aux activités des autres.

11. L'avis des intervenants doit être véritablement respecté et utilisé. Lorsqu'une personne prend le temps de faire part de ses idées en vue de la collaboration, ces idées doivent être prises en compte.

12. Les organismes gouvernementaux touchés ou pertinents doivent être adéquatement mobilisés et représentés. Cela peut parfois signifier que le gouvernement doit accomplir une partie du travail visant à convaincre ses homologues de la valeur et de l'importance de la participation à l'initiative.

13. Le gouvernement et l'industrie doivent donner suite aux décisions de partenariats, idéalement à mesure que les progrès sont réalisés et suivant un ensemble de mesure de la réussite mutuellement convenu.

14. La mesure des progrès devrait être partagée et simple, idéalement effectuée par l'entremise d'une seule courte liste intégrée d'indicateurs.

15. Un service de soutien adéquat et compétent est essentiel à la coordination des activités conjointes, à l'organisation de discussions et de réunions, au maintien des communications, au suivi des progrès du projet, à la détermination des améliorations et à la prestation d'un solide soutien administratif. [19, 20]

Les activités de collaboration mises en œuvre conjointement par les intervenants des secteurs public et privé ont plus de chance de réussir si elles font en sorte que les 15 facteurs de réussite ci-dessus y sont reflétés et délibérément intégrés dans le corps de toute nouvelle entente de collaboration. Ces principaux facteurs ont été testés par les alliés du Canada et ont fait leurs preuves, mais ils ne sont pas en soit la garantie du succès de toute future collaboration. Par contre, leur absence, par omission ou ignorance volontaire, contribuera certainement à l'échec.

---

16 Collective Impact, Standford Social Innovation Review, John Kania and Mark Kramer, Winter 2011.

17 The Ecosystem of Shared Value Creation, Harvard Business Review, Mark Kramer and Marc Pfi tzer, Oct 2016.

18 Best Practices for Operating Government-Industry Partnerships in Cyber Security, Journal of Strategic Security, Larry Clinton, Winter 2015.

19 Kania and Kramer, Ibid.

20 Kramer and Pfi tzer, Ibid.

PRIORISER LES **PARTENAIRES DU SECTEUR PRIVÉ**

Au niveau opérationnel, les initiatives de collaboration avec le secteur privé devraient être axées sur les organismes « qui sont les plus aptes à prendre des mesures liées à la cybersécurité au nom de la plus grande majorité possible; qui ont accès aux renseignements pouvant être utilisés pour la protection et pouvant être diffusés largement; ou qui ont un intérêt pour la sécurité nationale ou économique en plus d'avoir la capacité de contribuer à la cybersécurité d'une base systémique ». On peut répartir ces organismes du secteur privé en cinq catégories :

- Les fournisseurs de services de cybersécurité
- Les fournisseurs de services de télécommunications et d'Internet
- Les entreprises de technologie de l'information (équipement, logiciel et fournisseurs de services)
- Les entreprises du secteur de l'infrastructure critique importantes pour les systèmes
- Les organismes de partage de l'information qui ont développé des capacités particulières en matière de cybersécurité et de sources d'information.[21]

Pour poursuivre les activités de collaboration avec l'industrie, le gouvernement doit s'assurer que ces principaux groupes d'intervenants sont représentés aux échelons supérieurs.

21 An Operational Collaboration Framework for Cybersecurity, Aspen Cybersecurity Group, Nov 2018.

CONCLUSION

Ensemble, les domaines d'intérêt, les activités de soutien, les politiques habilitantes et les pratiques exemplaires, les principaux facteurs de réussite, les lignes directrices, et une liste de partenaires priorisés peuvent être réunis pour former une évaluation assez exacte d'un modèle global de collaboration publique-privée en matière de cyberdéfense.

> La liste des partenaires priorisés peut offrir au gouvernement un point de départ lui permettant de communiquer immédiatement avec un ensemble d'entreprises du domaine reconnues comme ayant le potentiel d'avoir une incidence sur une base plus large de cybersystèmes et d'environnements.

En utilisant le modèle comme base, les gouvernements peuvent d'abord déterminer leurs principaux défis en matière de cybernétique, puis décider si la collaboration pourrait être utile pour trouver et élaborer des solutions. Si les enjeux se trouvent dans la portée de l'un des quatre domaines d'intérêt de la collaboration, des activités précises peuvent alors être ciblées selon leur capacité à répondre au problème; l'efficacité possible et la mise en œuvre de solutions alternatives seront par la suite étudiées. À ce point, les gouvernements peuvent envisager de lancer des discussions sur la collaboration ou de prendre des engagements avec l'industrie, et il peut miser sur les facteurs de réussite et les lignes directrices pour former une forte base relationnelle assurant une mobilisation collaborative mutuellement productive et profitable pour les deux parties. Enfin, la liste initiale de partenaires priorisés peut offrir au gouvernement un point de départ efficace lui permettant de communiquer immédiatement avec un ensemble d'entreprises du domaine reconnues comme ayant le potentiel d'avoir une incidence sur une base plus large de cybersystèmes et d'environnements.

Le modèle était considéré comme global à l'origine. Mais à l'heure actuelle, lorsque le niveau et la maturité de la collaboration publique-privée en matière de cyberdéfense au Canada sont pris en compte (décrits comme étant « naissants » par plusieurs des personnes interviewées), le modèle sera probablement utilisé de manière sélective, afin de cibler un ou deux domaines prioritaires où le Canada doit relever des cyberdéfis qui semblent insurmontables et où l'industrie peut aider à la mise en œuvre de solutions grâce à des ententes de collaboration. Voir la figure 3.

Figure 3
Proposition d'un modèle de collaboration publique -privée en matière de cyberdéfense nationale

Domaines d'intérêt où la collaboration peut aider à relever des cyberdéfis.	Politiques et pratiques précises pouvant être utilisées pour répondre	Facteurs de réussite et ignes directrices visant à assurer une saine collaboration	Liste de partenaires priorisés de l'industrie à mobliser
Gouvernance, stratégie, politique et programmes	• Structures nationales permanentes de coordination et coopération • Structures de gouvernance collaborative dans la mise en œuvre des programmes • Réforme de l'approvisionnement • Autres autorités transactionnelles • Exigences opérationnelles urgentes	• Le gouvernement devrait chercher à avoir l'avis du secteur privé dès le départ, idéalement à l'étape de détermination de la grande priorité et de l'objectif initial. • Un programme commun devrait être élaboré pour motiver les participants à atteindre une vision commune de ce qui doit être fait. • Les hauts dirigeants du gouvernement et de l'industrie doivent s'engager à collaborer et à démontrer cet engagement. • Un modèle ou un processus reconnu devrait être utilisé toutes les fois où c'est possible pour structurer les activités de collaboration.	• Fournisseurs de services de cybersécurité • Fournisseurs de services de télécommunications et d'Internet • Entreprises des technologies de l'information (matériel, logiciels, fournisseurs de services) • Propriétaires et opérateurs d'infrastructures critiques importantes pour les systèmes • Organismes de partage de l'information ayant accès aux sources publiques ou privées d'information sur les menaces et les failles.
Missions et opérations	• Intégration approfondie des détenteurs de contrat dans les opérations du gouvernement • Environnements de mise à l'essai des capacités et plages expérimentales • Programme d'échange de talents • Planification de scénarios et exercices conjoints	• La communication avec les intervenants doit être élargie et commencer tôt. • Une interaction et une communication continues doivent être maintenues entre le gouvernement et les intervenants de l'industrie. • Le gouvernement doit laisser aux intervenants assez de temps pour étudier le matériel, les requêtes, les demandes de décisions, etc., et y réagir. • Une direction conjointe ou des rôles de leadership partagé mutuellement acceptables devraient être créés dans l'ensemble des programmes et des activités.	
Protection des actifs essentiels	• Cadres de protection de l'infrastructure critique élaborés conjointement • Centres d'analyse et de partage d'information	• La prise de décisions devrait être axée sur les consensus. • Les activités devraient se renforcer mutuellement.	
Développement de la technologie	• Centres d'innovation et d'accélération cybernétiques • Centres de développement rapide et de déploiement des capacités • Coopérative de recherche et développement • Feuilles de route technologiques • Réseaux d'innovation et de collaboration gérés par l'industrie	• L'avis des intervenants doit être véritablement respecté et utilisé. • Les organismes gouvernementaux touchés ou pertinents doivent être adéquatement mobilisés et représentés. • Le gouvernement et l'industrie doivent donner suite aux décisions de partenariats. • La mesure des progrès devrait être partagée et simple, idéalement effectuée par l'entremise d'une seule courte liste intégrée d'indicateurs. • Un service de soutien adéquat et compétent et un solide soutien administratif sont nécessaires au succès.	

RECOMMANDATIONS

Selon la recherche examinée aux fins de la présente étude et éclairée par des interviews approfondis et des discussions de suivi avec les grands experts en cybernétique des secteurs public et privé, l'AICDS a ciblé trois actions et initiatives prioritaires qui devraient être mises en œuvre par le gouvernement du Canada pour améliorer la collaboration publique-privée en matière de cyberdéfense. Les recommandations s'appuient sur les construits et les programmes canadiens existants, lorsque possible, tirent leur inspiration des pratiques exemplaires des alliés, et sont énoncées dans une séquence.

> « Le manque de confiance et de dialogue » a constamment été cité comme étant la raison principale du retard actuel dans la collaboration en matière de cyberdéfense.

Recommandation principale (court terme – 1-2 ans)

1. 1. **Innovation, Sciences et Développement économique Canada (ISDE) devrait mettre sur pied une Table sectorielle de stratégies économiques de la cyberdéfense et de la cybersécurité.**

« Le manque de confiance et de dialogue » a constamment été cité comme étant la raison principale du retard actuel dans la collaboration entre le gouvernement du Canada et l'industrie en matière de cyberdéfense. Une Table sectorielle de stratégies économiques permettrait la tenue régulière d'un forum visant à appuyer les discussions stratégiques et la planification conjointe entre le gouvernement et l'industrie, établissant ainsi un processus pour faire tomber les barrières relationnelles, économiques et politiques ciblées par les deux parties qui ralentissent la collaboration en matière de cyberdéfense.

Les Tables sectorielles de stratégies économiques constituent une nouvelle approche collaborative publique-privée lancée par le gouvernement fédéral en 2017 (d'autres Tables sectorielles ont été lancées en 2019) dans le but de déterminer et d'éliminer les obstacles à la croissance que doivent surmonter les secteurs clés de l'économie.

Les Tables sectorielles fonctionnent déjà. Elles contribuent à la mise en œuvre d'importants changements de politique et de réglementation en jumelant des hauts directeurs de l'industrie et des hauts représentants du gouvernement pour l'élaboration conjointe de stratégies visant à s'attaquer aux enjeux les plus pressants pour le secteur.

La Table sectorielle de stratégies économique de la cyberdéfense et de la cybersécurité proposée devrait être distincte de celle des industries numériques. La Table sectorielle des industries numériques se concentre sur la prolifération des technologies dans l'ensemble de la société; celle de la cyberdéfense et de la cybersécurité serait plutôt axée sur la manière de faire en sorte que les avantages de cette prolifération sont durables face à la montée des cyberagressions et des attaques contre les gouvernements, les citoyens et les entreprises. Elles sont de chaque côté du même bitcoin, essentielles l'une à l'autre.

Recommandations secondaires (moyen terme : 2-3 ans)

Les recommandations à moyen terme touchent la mise en œuvre de projets collaboratifs probablement plus ambitieux et visent à resserrer la faille grandissante dans les cybertalents et à remédier au manque d'environnement numérique pour soutenir la recherche, l'analyse, la mise à l'essai et les opérations conjointes. Ces types d'activités font encore plus avancer la collaboration le long du spectre (voir la figure 1), et englobent non seulement la planification conjointe, mais aussi l'élaboration et la mise en œuvre de solutions conjointes, en plus de l'obligation partagée de rendre des comptes sur les résultats. Ces activités nécessitent aussi une plus grande confiance entre les partenaires, l'assurance de l'engagement de chacun et la capacité d'accomplir des tâches et de produire des résultats qui font avancer les objectifs communs. Ainsi, elles devraient suivre la séquence à partir de la première recommandation.

2. **Le Centre de la sécurité des télécommunications devrait piloter un mécanisme de partage des talents avec l'industrie afin de répondre à la grave pénurie de talents en cybernétique au Canada.**

Ce programme pourrait être modelé suivant l'initiative Industry 100 du Royaume-Uni, un cadre d'échange de talents géré par le nouveau Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications. Cette approche imiterait le modèle fructueux du Royaume-Uni, qui est dirigé par le National Cyber Security Centre, au sein d'un construit plus large, le Government Communications Headquarters (GCHQ).

En basant la structure du programme d'échange sur Industry 100, le gouvernement et l'industrie pourraient se mobiliser conjointement pour les politiques émergentes, l'innovation et les défis opérationnels grâce à des prêts de services intégrés, globaux et à court terme.

Ces échanges pourraient faire d'abord l'objet d'un projet pilote dans des domaines moins sensibles (par exemple, l'analyse des données ou la prévision des compétences) pour bâtir la confiance entre le gouvernement et les participants de l'industrie, avant d'intégrer des domaines plus sensibles, comme l'approvisionnement ou la défense active. Innovation, Sciences et Développement économique Canada (ISDEC) devrait mettre en place l'un des trois cyberréseaux annoncés dans le budget de 2019 afin de permettre les propositions de création d'un réseau opérationnel axé sur le partage d'information et l'analyse sur les menaces, de même que la réponse à celle-ci et la mise à l'essai de solutions pour le gouvernement et l'industrie.

3. **Innovation, Sciences et Développement économique Canada (ISDE) devrait être actif dans l'un des trois cyberréseaux annoncés dans le budget de 2019 afin de permettre les propositions de création d'un réseau opérationnel axé sur le partage d'information et l'analyse sur les menaces, de même que la réponse à celle-ci et la mise à l'essai de solutions pour le gouvernement et l'industrie.**

- Contrairement aux réseaux traditionnels de recherche normalement financés par le gouvernement, un réseau pourrait créer un environnement opérationnel avec un réseau fédérateur physique sécurisé optimisé pour permettre le partage bilatéral d'information sur les menaces, une analyse et une réponse conjointes, et la mise à l'essai de solutions aux problèmes réels et actuels.
- Cela permettrait la création d'une plateforme physique et virtuelle de collaboration entre le gouvernement et l'industrie, une plateforme qui serait axée sur les cybermenaces ayant des répercussions sur la sécurité et la défense nationale.
- Les infrastructures publiques et privées existantes de partage d'information sur les menaces pourraient être intégrées à ce réseau.

Il convient de souligner que l'AICDS ne s'est pas directement penchée sur la réforme dans l'approvisionnement dans les recommandations du présent rapport. L'approvisionnement à la vitesse cybernétique est un enjeu de taille que notre gouvernement doit résoudre, mais un rapport axé sur la collaboration n'est pas le bon canal pour en discuter. L'AICSD participera à la recherche de suivi sur les pratiques exemplaires en matière d'approvisionnement et reconnaît que notre système d'approvisionnement actuel demeure un obstacle considérable à l'efficacité de la cybersécurité et de la cyberdéfense.

Annexe A : Méthodologie du rapport

La méthodologie suivie pour le présent rapport comprend l'examen, l'évaluation et la détermination des pratiques, des modèles et des programmes mondiaux de pointe issus de la collaboration entre le gouvernement et l'industrie en matière de cyberdéfense et de cybersécurité. Le rapport s'est penché sur les trois grandes catégories de mobilisation suivantes : politique, opérationnelle et internationale. L'aspect politique inclut les fonctions suivantes : la gouvernance, l'approvisionnement et le développement des talents en matière de cybersécurité et de cyberdéfense en tant qu'éléments clés. L'aspect opérationnel inclut les fonctions de collaboration visant à préparer les cybercapacités; à surveiller et à déterminer les cybermenaces, de même qu'à les déclarer et à y réagir; et les fonctions de partage de l'information et de coordination de la réponse à la menace. Reconnaissant la nature sans frontière de la menace et des occasions d'affaires, le rôle des alliés internationaux et des autres pays a été saisi par l'examen des fonctions suivantes comprises dans la catégorie de la mobilisation internationale : l'interopérabilité (des opérations à l'acquisition) avec les alliés dans les principales pratiques et les différences de politique ou de réglementation dans le modèle des autres pays qui permettent les le recours aux pratiques de pointe, ou la coopération, la collaboration, le partenariat ou l'approvisionnement efficaces visant à éclairer le nouveau modèle canadien de collaboration et de partenariat entre les secteurs public et privé.

Les conclusions initiales issues de l'examen et de l'évaluation des rapports, des publications, des articles de périodiques et d'autres sources d'information, publics ou fournis par l'AICDS, ont été validées et enrichies par la conduite d'interviews avec des experts en la matière du gouvernement du Canada, de l'industrie et des partenaires internationaux. L'AICSD a élaboré cinq ou six questions sur la gouvernance et les principales pratiques afin de faire la comparaison des réponses. Ces questions ont été fournies aux personnes interviewées à l'avance. Au total, 20 interviews ont été menés et l'accent a été mis sur les personnes qui en savent le plus sur les opérations de cyberdéfense au Canada, aux États-Unis, au Royaume-Uni et en Australie.

Le rapport met en lumière un modèle de collaboration idéalisé entre le gouvernement et l'industrie dans le domaine de la cyberdéfense et de la cybersécurité, y compris les fonctions et les activités essentielles, qui ont servi de base à la comparaison entre le Canada et ses alliés. Toutes les recommandations faites sont appuyées par des exemples précis de modèles et de mécanismes de collaboration fructueux en cyberdéfense et en cybersécurité mis en œuvre dans d'autres pays ou énoncés au cours des interviews. Cette preuve constitue l'élément principal du présent rapport.

Annexe B : Principaux contributeurs à la recherche et aux recommandations

Dans le cadre de ses efforts constants de faire la promotion du secteur canadien novateur de la cyberdéfense, l'AICSD a mis sur pied un Conseil consultatif en cybernétique. Ce conseil est formé de spécialistes de l'industrie de la cyberdéfense qui font de la rétroaction des activités et les efforts de recherches de l'AICDS dans le domaine cybernétique, en plus de participer au travail de l'Association afin de créer des liens plus étroits entre l'industrie au pays et le gouvernement.

> Les recommandations de l'AICDS visent à faire avancer la collaboration dans tout le spectre afin d'inclure non seulement la planification conjointe, mais aussi le développement et la prestation de solutions conjoints et une responsabilité conjointe des résultats.

Le Conseil consultatif en cybernétique a joué un rôle essentiel dans l'élaboration du présent rapport et des recommandations qu'il renferme. Il est formé des personnes suivantes :

Al Amlani
Directeur des cyberopérations,
General Dynamics Mission Systems – Canada

Chris Bartlett
Président,
CCX Technologies

Shaun Covell
Directeur,
Sapper Labs

Al Dillon
Directeur général,
Root9B-C

Steve Drennan
Directeur de la cybersécurité et de la gestion du risque de l'entreprise,
ADGA

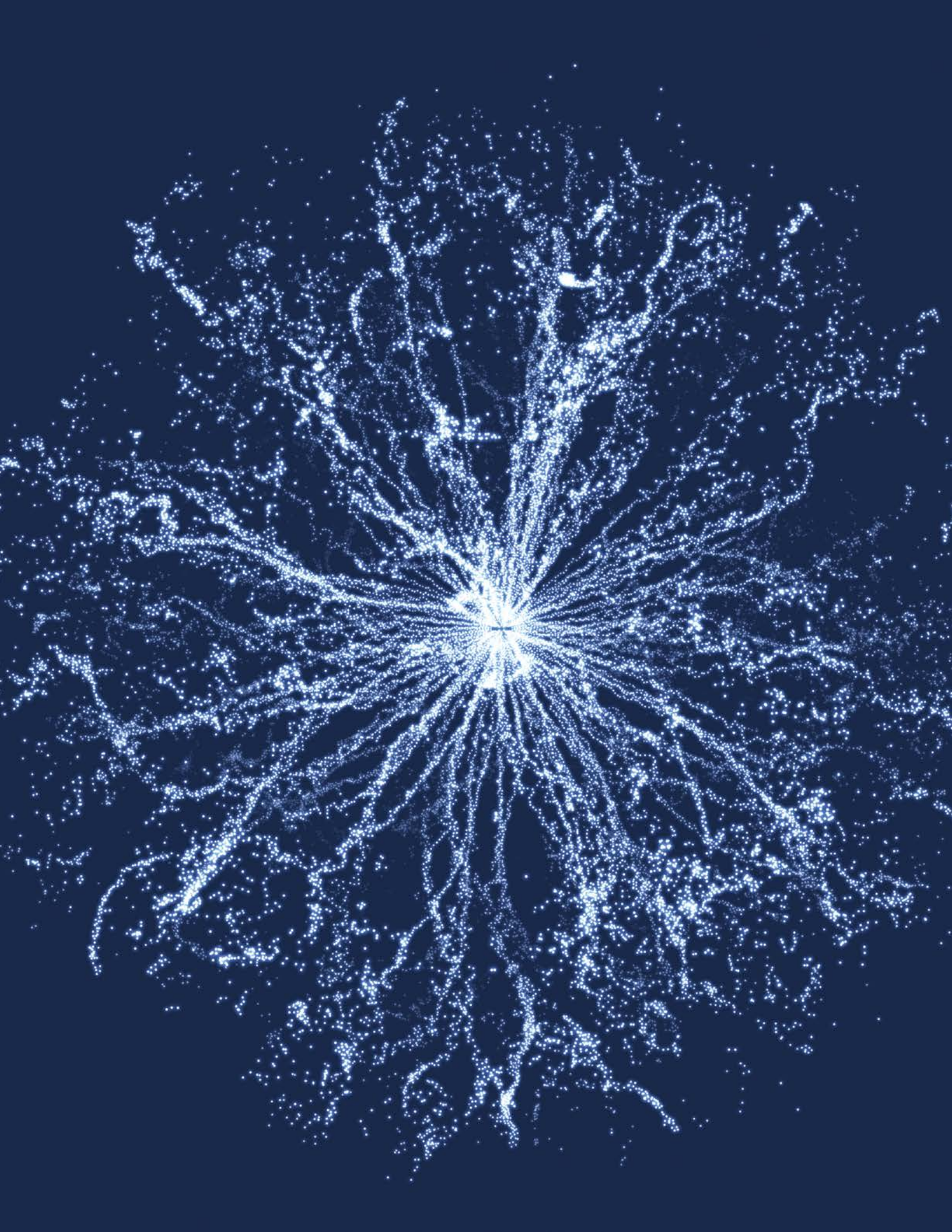
Bill Dunnion
Directeur de la cyberrésilience,
Calian

Rob Mazzolin
Vice-directeur des plans et des politiques de la U.S. Cyber Command (à la retraite) et chef stratège de la cybersécurité,
RHEA

Dave McMahon (président)
Directeur,
Clairvoyance Cyber Corporation

Daina Proctor
Partenaire associée, services consultatifs aux renseignements et aux opérations liés à la sécurité,
IBM

Rafal Rohozinski
Directeur général,
SecDev



Canadian Association of Defence and Security Industries

300-251 avenue Laurier Ouest
Ottawa, ON K1P 5J6

defenceandsecurity.ca
@cadsicanada