Revu par le SMA(Svcs Ex) conformément à la *Loi sur l'accès à l'information*. Renseignements NON CLASSIFIÉS.

Évaluation des cyberforces

Directeur général – Évaluation
Comité de la mesure du rendement et de l'évaluation
Avril 2021 1258-3-031 – SMA(Svcs Ex)

Canada

TABLE DES MATIÈRES

Sigles

AC	Armée canadienne
ACM	Assurance de la cybermission
ACS+	Analyse comparative entre les sexes plus
AF	Année financière
AICDS	Association des industries canadiennes de défense et de sécurité
ARC	Aviation royale canadienne
ARR	Autorités, responsabilités et responsabilisations
BPR	Bureau de première responsabilité
C3IR	Commandement, contrôle, communications, informatique et renseignement
CCF	Commandant de la cyberforce
CCCFI	Commandant de la cybercomposante de la force interarmées
CDF	Chef – Développement des Forces
CEM Cyber	Chef d'état-major du cyberespace
CEMD	Chef d'état-major de la Défense
CEM(GI)	Chef d'état-major (Gestion de l'information)
CMR	Cadre ministériel des résultats
CMR	Collège militaire royal
COIC	Commandement des opérations interarmées du Canada
COMFOSCAN	Commandement – Forces d'opérations spéciales du Canada
COMRENSFC	Commandement du renseignement des Forces canadiennes
CORFC	Centre d'opérations des réseaux des Forces canadiennes
CPM/GIGPM	Chef du personnel militaire/Groupe d'instruction de la génération du personnel militaire
CST	Centre de la sécurité des télécommunications du Canada
DDFOC	Directeur – Développement des Forces (opérations cybernétiques)
DG Cyber	Directeur général – Cyberspace
DGDFCI	Directeur général – Développement des Forces (Capacité d'information)
DG Éval	Directeur général – Évaluation
DGOGI	Directeur général – Opérations (Gestion de l'information)
DOAD	Directives et ordonnances administratives de la défense
EECFC	École d'électronique et des communications des Forces canadiennes
FA	Autorité fonctionnelle
FAC	Forces armées canadiennes
GI	Gestion de l'information
GOIFC	Groupe des opérations d'information des Forces canadiennes
Gp GI	Groupe de Gestion de l'information
ISDE	Innovation, Sciences et Développement économique Canada
MDN	Ministère de la Défense nationale
MRC	Marine royale canadienne
N1	Niveau 1
NORAD	Commandement de la défense aérospatiale de l'Amérique du Nord
Ops	Opérations
OTAN	Organisation du Traité de l'Atlantique Nord
PACM	Programme d'assurance de la cybermission
PF&DO	Posture de la force et disponibilité opérationnelle
PSE	Politique de défense du Canada : *Protection, Sécurité, Engagement*
RH	Ressources humaines
SCT	Secrétariat du Conseil du Trésor
SMA	Sous-ministre adjoint
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
SMA(IE)	Sous-ministre adjoint (Infrastructure et Environnement)
SMA(Mat)	Sous-ministre adjoint (Matériels)
SMA(S & T)	Sous-ministre adjoint (Science & Technologie)
SMA(Svcs Ex)	Sous-ministre adjoint (Services d'examen)
SPC	Services partagés Canada
TI	Technologie de l'information
USA	United States of America
VCEMD	Vice-chef d'état-major de la défense

GUIDE DE PRÉSENTATION DU RAPPORT

En tant que rapport pilote pour ce format de rapport au Directeur général – Évaluation, voici quelques lignes directrices pour lire le présent document.

Il vaut mieux lire ce document sur un dispositif électronique, tel qu'un ordinateur ou une tablette, à l'opposé d'une version imprimée.

Le rapport comporte des liens qui renvoient à d'autres sections du rapport, à des documents externes ou à des sites publics pour information complémentaire. **Les liens actifs de ce document ne seront pas mis à jour après la publication du document.**

Certains mots dans les paragraphes sont écrits en couleur. Cette couleur sert à mettre en évidence les points les plus pertinents pour le lecteur, et permet à celui-ci de lire les pages plus rapidement. De plus, certaines couleurs sont associées à des thèmes précis du rapport (p. ex., mise en œuvre du programme ou recherche et développement).

Si ce document est imprimé, il vaut mieux le faire en couleur, pour maintenir l'intégrité et l'intention des éléments graphiques.

Cette icône indique une recommandation formulée par le SMA(Svcs Ex), et pour laquelle l'annexe A présente un plan d'action de la direction.

RÉSUMÉ

Ce rapport présente les résultats de l'évaluation des cyberforces, qui a été menée pendant l'année financière (AF) 2019-2020 par le Sous-ministre adjoint (Services d'examen) (SMA[Svcs Ex]) conformément à la *Politique sur les résultats* 2016 du Conseil du Trésor. Dans le cadre de cette évaluation, nous avons examiné le rendement des cyberforces sur une période de trois ans, de l'AF 2017-2018 à l'AF 2019-2020. Nous avons mené cet examen avec la collaboration du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC).

Description du programme

Les cyberforces comprennent trois programmes du répertoire de programmes de la Défense : 1.5 Cyberopérations; 2.6 Cyberforces prêtes au combat; 4.6 Développement des cyberforces et du C3IR. En bref, les cyberforces représentent le personnel civil et militaire pour la mise sur pied, l'emploi et le développement des cyberforces aux fins des cyberopérations, des opérations de réseaux et d'assurance de la cybermission (ACM).

Les cyberforces sont sous l'autorité du Sous-ministre adjoint (Gestion de l'information) (SMA[GI]), par l'intermédiaire duquel le Directeur général – Opérations (Gestion de l'information) (DGOGI) est responsable des programmes 1.5 et 2.6, et le Directeur général – Cyberespace (DG Cyber) responsable du programme 4.6. En tant qu'organisations militaires, le DGOGI et le DG Cyber relèvent du Chef d'état-major (Gestion de l'information) (CEM[GI]), qui occupe aussi les fonctions de commandant de la cyberforce (CCF) et de chef d'état-major du cyberespace (CEM Cyber).

Portée

En raison de la nouveauté des cyberforces, nous avons mené une évaluation formative, qui s'est attardée à la conception du programme, à la prestation du programme et aux premiers résultats.

Résultats

Nous avons catégorisé les résultats en fonction des thèmes Mise en œuvre et gestion du programme, Recherche et développement, et Mise sur pied du personnel.

Mise en œuvre et gestion du programme

- Les autorités, les responsabilités et les responsabilisations (ARR) associées au cyberdomaine demeurent floues en termes d'orientation et de responsabilités; elles font l'objet de travaux par le DGOGI et le DG Cyber, et seront éclaircies dans une nouvelle Directive et ordonnance administrative de la défense (DOAD).
- La mise en œuvre du programme est limitée par le manque de personnel, de fonds et de matériel sécurisé pour entreprendre des initiatives du cyberdomaine (p. ex., le programme d'assurance de la cybermission [dans la politique de défense du Canada *Protection, Sécurité, Engagement (PSE)*, initiative 87]*)*.

Recherche et développement

- Les cyberprojets ont peu d'influence directe sur les activités à cause des processus d'acquisition lents, des modifications nécessaires aux projets existants pour intégrer les cyberexigences et les changements technologiques rapides.
- Il y a une grande mobilisation des intervenants au MDN, dans les FAC et dans les autres ministères et organismes gouvernementaux.

Mise sur pied du personnel

- Il est difficile d'attirer et de maintenir en poste du personnel militaire et civil dans ce domaine.
- Les échéances relatives au processus d'autorisation de sécurité nuisent à la capacité des cyberforces de satisfaire aux exigences [redacted]
- La progression de carrière s'améliore grâce aux occasions d'emploi auxquelles ont accès les professionnels du cyberdomaine.

Conclusions générales

Comme nouveaux groupes, le DG Cyber et le DGOGI travaillent sur diverses initiatives pour mettre en place les composantes fondamentales requises pour des cyberforces efficaces dans l'avenir. Toutefois, à moins d'accorder une attention appropriée au cyberdomaine, le rythme de mise en œuvre continuera d'être limité.

- La théorie de conception du programme est robuste.
- Les cyberforces requièrent le soutien et des investissements de l'ensemble du MDN et des FAC pour assurer une mise en place complète de l'ACM et des autres initiatives du cyberdomaine.
- Les intervenants du cyberdomaine ont besoin d'une plus grande orientation stratégique.
- Les premiers développements du programme montrent des signes de progrès dans l'instruction des cyberforces.

SOMMAIRE – PRINCIPALES CONSTATATIONS ET RECOMMANDATIONS

PRINCIPALE CONSTATATION	RECOMMANDATION
MISE EN ŒUVRE ET GESTION DU PROGRAMME	
1. L'intégration des cyberforces aux activités des FAC et l'habilité d'influencer les prises de décision de la haute direction sont [redacted] des ARR floues, [redacted] actuel du SMA(GI) et l'absence d'un champion du cyberdomaine.	1. Pour améliorer la gestion des cyberforces, le SMA(GI) doit revoir, mettre à jour et publier des ARR relatives au cyberdomaine dans tout le MDN et les FAC pour les faire connaître.
2. Le cyberdomaine ne possède pas d'organe de gouvernance interne qui lui est propre. Le cyberdomaine utilise les organes de gouvernance existants du SMA(GI), avec l'appui de groupes de travail qui tendent à avoir une nature informative. Les intervenants sont responsables d'élaborer leurs propres cyberstratégies.	2. Revoir le cadre de gouvernance actuel pour déterminer si le cyberdomaine a besoin d'une structure distincte.
3. Même s'il existe des documents stratégiques pour la planification des cyberforces, ceux-ci ne sont pas connus ni utilisés largement au MDN et dans les FAC.	Voir la recommandation 1.
4. La mise en œuvre de l'initiative 87 de la PSE [redacted] dans l'ensemble du MDN et des FAC.	Voir la recommandation 1.
5. La responsabilité de définir la cyberpréparation opérationnelle n'est pas réglée. Bien que la Marine a réalisé des progrès dans ce domaine, [redacted]	**Suggestion de suivi :** Examiner l'officialisation, l'orientation et la conformité de la cyberpréparation opérationnelle.
6. [redacted]	3. Créer un terrain de cyberentraînement centralisé, institutionnalisé et soutenu, assorti de la capacité d'adapter la classification et d'un accès à distance.

RÉSUMÉ – PRINCIPALES CONSTATATIONS ET RECOMMANDATIONS

PRINCIPALE CONSTATATION	RECOMMANDATION
RECHERCHE ET DÉVELOPPEMENT	
7. [redacted]	
8. La conception du programme a intégré les connaissances pertinentes des intervenants du MDN, des FAC, des autres ministères et des intervenants alliés; toutefois, la mobilisation de l'industrie privée et du milieu universitaire pose problème.	
MISE SUR PIED DU PERSONNEL	
9. Des postes du cyberdomaine ont été alloués partout au MDN et dans les FAC, [redacted]	
10. L'avancement de carrière est limité au sein du cyberpersonnel. Toutefois, on y remarque des signes d'amélioration.	**Suggestion de suivi :** Examiner les occasions d'avancement de carrière des cyberopérateurs.
	Suggestion de suivi : Examiner les résultats de l'étude sur le cyberleadership qui a été menée par le Directeur – Développement des Forces (Opérations cybernétiques) (DDFOC) qui devait commencer en mars 2020, qui servira à examiner cette question [redacted]
11. Les échéances et les processus relatifs [redacted]	
12. Au fur et à mesure que se poursuivent l'élaboration et l'officialisation du cyberentraînement, [redacted]	4. Évaluer la faisabilité de standardiser l'instruction donnée par des tiers et de valider cette instruction.

PORTÉE DE L'ÉVALUATION

Portée et responsabilités

Les trois programmes suivants ont été examinés dans le cadre de l'évaluation : 1.5 Cyberopérations; 2.6 Cyberforces prêtes au combat; 4.6 Développement des cyberforces et du C3IR. La période visée par l'évaluation couvre l'AF 2017-2018 à l'AF 2019-2020.

Les principales constatations ont été regroupées en trois thèmes :

1. **Mise en œuvre et gestion de programme**
2. **Recherche et développement**
3. **Mise sur pied du personnel**

Photo : Caméra de combat des Forces canadiennes, MDN, IS2014-7532-10

Une **évaluation formative** met l'accent sur l'évaluation de la conception et de la prestation d'un nouveau programme, pour s'assurer que ce programme est élaboré et livré d'une manière qui lui permettra de connaître du succès au fil de son avancement.

En raison de la nouveauté des cyberforces, nous avons mené l'évaluation au titre d'une **évaluation formative**. Par conséquent, nous avons examiné la conception et la prestation des programmes et nous nous sommes penchés sur les résultats immédiats initiaux au contraire des résultats intermédiaires ou finaux, puisqu'il est encore trop tôt pour évaluer de manière précise et utile les résultats intermédiaires et finaux des programmes. Les résultats immédiats évalués sont les suivants :

- Des cyberprojets pertinents, pleinement interopérables et capables sont disponibles en appui aux opérateurs des FAC.
- Les unités sont adéquatement entraînées et dotées en personnel apte à réaliser ses tâches efficacement selon les plans de posture de la force et de disponibilité opérationnelle.
- Le matériel est disponible selon les quantités, le type et l'état requis pour atteindre le niveau de préparation requis.
- La gouvernance et les structures de forces sont en place pour atteindre les niveaux de préparation.

Hors portée

Les discussions sur la portée avec les gestionnaires de programme nous ont permis d'apprendre que la conduite de cyberopérations n'avait pas encore assez de maturité pour être évaluée. Pour cette raison, cet aspect a été exclu de notre évaluation. De plus, des limitations concernant la classification de sécurité du contenu spécifique au développement de la force relativement au commandement, contrôle, communications, informatique et renseignement (C3IR) de la portée ont entraîné son exclusion de la portée.

PROFIL DU PROGRAMME

Le cyberespace est essentiel à la conduite d'opérations militaires modernes et est reconnu comme un domaine d'opérations.

L'arrivée de l'âge de l'information a mené à une évolution dans la conduite des opérations du MDN et des FAC. Même si la terre, l'air et la mer demeurent les principaux environnements d'opérations, le besoin d'engager le cyberespace et d'y mener des opérations se fait de plus en plus sentir. À la lumière de la nature complexe et de l'évolution rapide du cyberdomaine, le MDN et les FAC reconnaissent le besoin d'avoir de robustes cybercapacités afin d'assurer le succès de la mission, tel que l'énonce la PSE.

Le terme « cyberforces » renvoie à trois programmes du répertoire de programmes de la Défense :

1.5 Cyberopérations

2.6 Cyberforces prêtes au combat

4.6 Développement des cyberforces et du C3IR

Les cyberforces représentent le personnel civil et militaire pour la mise sur pied, l'emploi et le développement des cyberforces aux fins des cyberopérations, des opérations de réseaux et d'assurance de la cybermission (ACM).

Les cyberforces sont sous l'autorité du Sous-ministre adjoint (Gestion de l'information) (SMA[GI]), par l'intermédiaire du Directeur général – Opérations (Gestion de l'information) (DGOGI), qui est responsable des programmes 1.5 et 2.6, ainsi que par l'intermédiaire du Directeur général Cyber (DG Cyber), qui est responsable du programme 4.6. En tant qu'organisations militaires, le DGOGI et le DG Cyber relèvent du Chef d'état-major (Gestion de l'information) (CEM[GI]), qui occupe aussi les fonctions de commandant de la cyberforce (CCF) et de chef d'état-major du cyberespace (CEM Cyber). De plus, en tant qu'entités du QGDN, elles relèvent du SMA(GI) pour leur administration.

Le DGOGI fournit les éléments de base opérationnels du Groupe Gestion de l'information (Groupe GI). À ce titre, le DGOGI mène et soutient les opérations des FAC et fournit aussi du soutien en gestion de l'information et en technologie de l'information (GI/TI) à certaines activités ministérielles. De plus, le DGOGI est responsable des réseaux informatiques et de la cyberdéfense.

Le DG Cyber s'occupe de la conception et de la mise au point des cybercapacités ainsi que des capacités en matière de C3IR pour les FAC pour ensuite les élaborer et les mettre en œuvre, de même que de les intégrer aux forces existantes pour mener le spectre complet des cyberopérations.

PROFIL DU PROGRAMME

Cyberopérations

Objectifs du programme

Employer des cyberforces pour détecter, dissuader, défendre et contrer les menaces, ennemis ou attaques à l'encontre du MDN et des FAC dans le cyberenvironnement mondial, afin d'atteindre les objectifs militaires du Canada.

Activités du programme

- Mener des opérations défensives
- Mener des opérations actives
- Soutenir les opérations

Cyberforces prêtes au combat

Objectifs du programme

Préparer et maintenir en puissance des cyberforces prêtes au combat qui sont capables d'intervenir dans toutes circonstances, selon les instructions du gouvernement du Canada dans le temps d'intervention requis.

Activités du programme

- Mener l'instruction collective
- Mener la cyberinstruction individuelle
- Maintenir l'état de préparation du cybermatériel
- Gérer la préparation opérationnelle

Développement des cyberforces

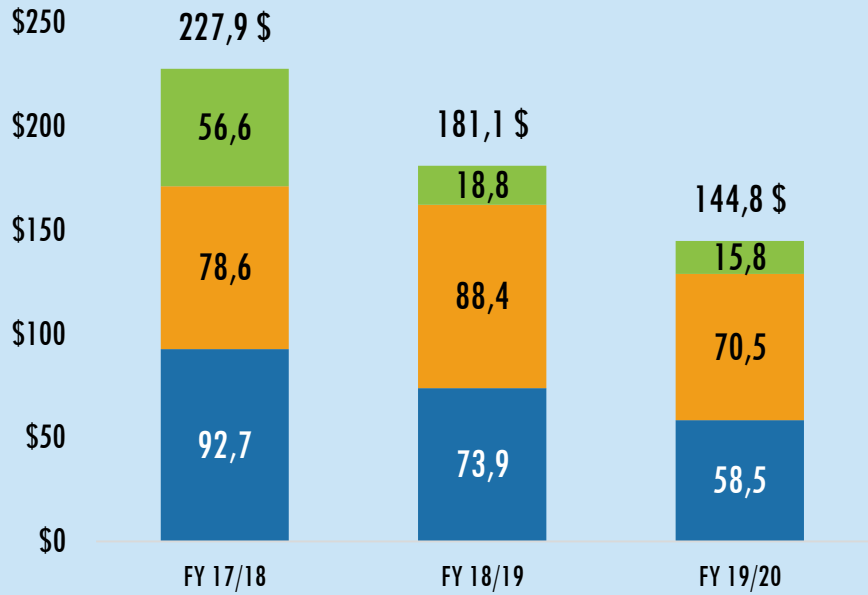
Objectifs du programme

Développer et gérer les activités de développement des cyberforces et du C3IR, notamment l'analyse, la mise à l'essai et la validation des capacités interarmées, des éléments habilitants et des structures de la force qui doivent être intégrées et mises en œuvre dans les FAC, et assurer leur interopérabilité avec les partenaires nationaux et les partenaires et alliés internationaux.

Activités du programme

- Réaliser l'analyse stratégique et le développement de concepts et de doctrine
- Coordonner et superviser l'architecture
- Réaliser la recherche et le développement
- Réaliser le développement et la mise à l'essai de l'instruction
- Assurer l'intégration à la structure de la force
- Déterminer les leçons retenues
- Concevoir et évaluer des capacités de rechange
- Assurer le développement et la supervision de projets

Dépenses de programme



Les dépenses de programme pour chaque programme remontent uniquement à l'AF 2017-2018, comme le montre le graphique. À noter, les chiffres de l'AF 2019-2020 représentent les dépenses prévues.

À l'AF 2019-2020, les cyberforces comptaient en tout 1 309 équivalents temps plein, 671 dans le programme 1.5 (bleu), 602 dans le programme 2.6 (orange), et 36 dans le programme 4.6 (vert).

[1] Dépenses réelles et dépenses prévues par programme de 2014-2015 à 2022-2023 ($) [Consulté le 23 octobre 2020].

PROFIL DU PROGRAMME

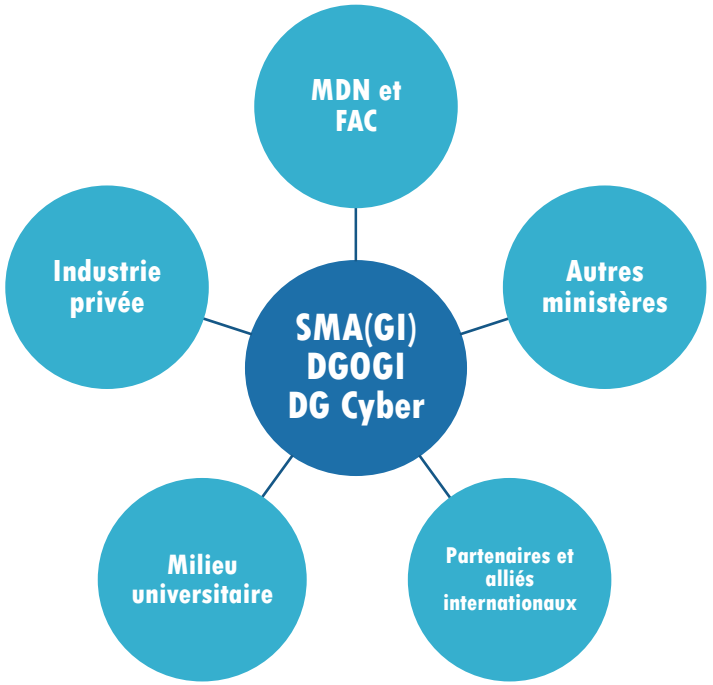
INTERVENANTS DU PROGRAMME

MDN et FAC : Sous-ministre adjoint (Ressources humaines – Civils) (SMA[RH-Civ]), Sous-ministre adjoint (Infrastructure et Environnement) (SMA[IE]), Sous-ministre adjoint (Matériels) (SMA[Mat]), Sous-ministre adjoint (Politiques) (SMA[Pol]), Sous-ministre adjoint (Affaires publiques) (SMA[AP]), SMA(Svcs Ex), Sous-ministre adjoint (Sciences et Technologie) (SMA[S & T]), Chef – Développement des Forces (CDF), Chef du personnel militaire (CPM), Juge-avocat général (JAG), État-major interarmées stratégique (EMIS), Vice-chef d'état-major de la Défense (VCEMD), Armée canadienne (AC), Aviation royale canadienne (ARC), Marine royale canadienne (MRC), Commandement – Forces d'opérations spéciales du Canada (COMFOSCAN), Commandement du renseignement des Forces canadiennes (COMRENSFC), Commandement des opérations interarmées du Canada (COIC).

Autres ministères et organisation du gouvernement : Service canadien du renseignement de sécurité (SCRS), Centre de la sécurité des télécommunications (CST), Construction de Défense Canada, ministère des Finances, Innovation, Sciences et Développement économique (ISDE), Bureau du Conseil privé, Sécurité publique, Services publics et Approvisionnement Canada, Partenariats public-privé Canada, Gendarmerie royale du Canada, Services partagés Canada (SPC), Secrétariat du Conseil du Trésor (SCT).

Partenaires et alliés internationaux : CYBERCOM – États-Unis, National Security Agency – États-Unis (NSA), Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD), Organisation du Traité de l'Atlantique Nord (OTAN), Groupe des cinq (États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande et Canada).

Industrie privée et milieu universitaire : Il y a près de 275 sociétés recensées qui sont liées à la cyberdéfense et à la cybersécurité au Canada, et 91 établissements universitaires qui offrent des diplômes en science informatique.



La Force opérationnelle cybernétique a été lancée en 2010 et a évolué au fil du temps.

2010 – La Force opérationnelle cybernétique est établie au SMA(GI)

2011 – La Force opérationnelle cybernétique est transférée au CDF et renommée DG Cyber

2017 – **Création des cyberforces**
- Le DG Cyber est transféré au SMA(GI)
- 6 initiatives de la PSE* liées au cyberdomaine (63, 65, 87, 88, 89, 90)
- Publication de la Directive de mise en œuvre du CEMD sur le cyberdomaine
- Création du groupe professionnel de cyberopérateurs

Les cyberforces dans le MDN et les FAC

* Lien consulté le 23 oct 2020.

PROFIL DE PROGRAMME

Le Programme d'assurance de la cybermission

Nous avons évalué le développement du Programme d'assurance de la cybermission (PACM), qui relève de l'autorité des cyberforces. Le PACM forme une grande partie du développement des cyberforces et a été créé pour répondre à l'initiative 87 de la PSE. L'ACM intègre les concepts de « cyberespace » et « d'assurance de la mission », qui constitue la capacité d'une organisation, d'un service, d'une infrastructure, d'une plateforme, d'un système d'arme ou de l'équipement de fonctionner dans le cyberespace contesté et d'accomplir sa mission[2].

Le PACM est une entreprise de l'ensemble du MDN et des FAC pour mettre sur pied une équipe de défense cyber-résiliente. Le PACM est spécialement conçu pour augmenter la cyber-résilience des personnes, des processus et de la technologie contre les cybermenaces associées aux cinq lignes d'activités suivantes :

1. **Politique**
2. **Gouvernance**
3. **Mobilisation et collaboration des intervenants**
4. **Éducation et instruction**
5. **Rapport**

L'équipe du PACM travaille à établir une structure de supervision centralisée et d'exécution décentralisée pour l'assurance de la cybermission afin d'accorder aux Niveaux 1 (N1) les autorités, responsabilités et responsabilisations (ARR) appropriées pour qu'ils puissent s'acquitter de leur obligation consistant à veiller à l'assurance de la cybermission et la cyber-résilisence à tous les échelons du MDN et des FAC. En bref, le concept d'ACM est la responsabilité de tous.

Objectifs du PACM[2]

- Permettre des décisions et des mesures informées, opportunes et efficaces en matière de gestion de risque tant à l'échelon supérieur du MDN et des FAC que dans les programmes de soutien
- Établir des apports d'information permanents provenant de diverses sources pour étayer les décisions relatives aux activités de gestion du risque
- Améliorer les actions collectives avec les alliés, les autres ministères et organismes
- Améliorer la résilience des éléments de force des FAC dans le cyberespace
- Renforcer la cyberprotection des infrastructures et des services essentiels du MDN et des FAC
- Améliorer l'assurance relative à l'acquisition et au soutien du matériel (notamment de la chaîne d'approvisionnement et le maintien en puissance)
- Combler les lacunes en matière de risque entre les programmes existants
- Établir une surveillance permanente pour déceler les nouvelles vulnérabilités et les indices relatifs aux adversaires qui tentent d'en profiter

« Protéger les réseaux et l'équipement militaire critiques contre des cyberattaques en créant un nouveau programme d'assurance des cybermissions qui incorpore les exigences en matière de cybersécurité au processus d'approvisionnement » – Initiative 87 de la PSE

[2] *Ébauche de la charte du PACM (2020).*

CONTEXTE DE L'ÉVALUATION

Le rapport présente les résultats d'une évaluation des cyberforces, qui a été menée à l'AF 2019-2020 par le SMA(Svcs Ex) en conformité avec la *Politique sur les résultats* 2016 du Conseil du Trésor. Dans cette évaluation, nous avons examiné le rendement des cyberforces sur une période de trois ans, de l'AF 2017-2018 à l'AF 2019-2020 et nous avons réalisé cet examen conformément au plan d'évaluation quinquennal du MDN et des FAC. Les constatations et les recommandations de cette évaluation peuvent servir à influencer les décisions de la direction relatives à la conception et à la prestation de programme, à l'affectation des ressources ainsi que de servir de seuil de référence pour les évaluations futures.

Photo : Cplc Simon Duchesne, VL2015-0010-003

Les cyberforces ont été créées récemment, soit à la suite de l'établissement du Cadre ministériel des résultats (CMR) en 2017.

- Les cyberforces n'avaient pas fait l'objet d'une évaluation précédemment; toutefois, le MDN et les FAC ont fait partie de l'*Évaluation horizontale de la Stratégie de cybersécurité du Canada** *(2017)* réalisée par Sécurité publique Canada. « La stratégie repose sur trois piliers : protéger les systèmes du gouvernement du Canada; nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement du Canada; aider les Canadiens à se protéger en ligne[3]. » L'Évaluation horizontale a porté sur les aspects suivants :
  - dans quelle mesure la structure de gouvernance horizontale a supervisé efficacement la mise en œuvre de la Stratégie;
  - dans quelle mesure les ministères et organismes participants ont mis en œuvre les activités financées dans le cadre de la Stratégie;
  - dans quelle mesure les activités prévues ont contribué à l'atteinte des objectifs principaux de la Stratégie[3].

[3]Sécurité publique Canada
Rapport final – Évaluation horizontale de la Stratégie de cybersécurité du Canada (2017)

*Consulté le 23 octobre 2020

MISE EN ŒUVRE ET GESTION DU PROGRAMME

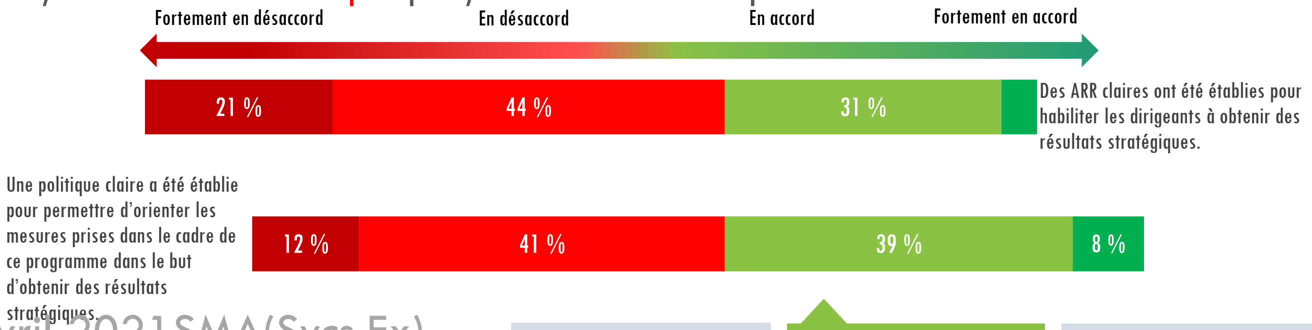
Les cyberforces manquent d'orientation sans ARR claires et d'une représentation suffisante pour influencer les décisions.

CONSTATATION 1 : L'intégration des cyberforces aux activités des FAC et l'habilité d'influencer les prises de décision de la haute direction [redacted] des ARR floues, [redacted] actuel du SMA(GI) et l'absence d'un champion du cyberdomaine.

Des ARR floues

- La majorité des intervenants de programme croient que les autorités, responsabilités et responsabilisations (ARR) associées au cyberdomaine sont encore floues en termes d'orientation et de responsabilités.
- Les concepts de technologies de l'information (TI), de technologies opérationnelles et de technologies des plateformes ont été utilisés pour définir les autorités fonctionnelles du cyberdomaine du SMA(GI), du SMA(IE) et du SMA(Mat). Or, en pratique, les intervenants reconnaissent qu'il n'est pas toujours simple de classer la technologie selon ces concepts et qu'un éclaircissement supplémentaire est requis.
- Le DGOGI et le DG Cyber travaillent à préciser les ARR, par exemple, par la détermination des responsabilités entre la cyberdéfense (Centre d'opérations des réseaux des Forces canadiennes [CORFC]) et la cybersécurité (Directeur – Sécurité [Gestion de l'information] [Dir Sécur GI]).
- La haute direction du programme reconnaît que de nombreuses ARR concernant le cyberdomaine sont encore floues; elle prévoit cependant que de nouvelles Directives et ordonnances administratives de la défense (DOAD) aideront à les éclaircir au fil du développement des cyberforces.

Les résultats du sondage indiquent que les intervenants supérieurs du cyberdomaine ne croient pas qu'il y a des ARR claires en place



Le contexte organisationnel

- Le fait d'avoir des postes du cyberdomaine dans l'organisation du SMA(GI) a mené à des difficultés pour les cyberforces :
  - Le SMA(GI) existe à l'extérieur de la chaîne de commandement opérationnelle, par conséquent, ne possède pas d'autorité de commandement.
  - Le SMA(GI), avec ses intérêts organisationnels, pan-ministériels, proactifs et à long terme, [redacted]
  - Bien que la supervision du PACM est assurée par le SMA(GI), l'autorité fonctionnelle réside auprès du VCEMD. Selon les gestionnaires de programme, cette situation a entraîné des retards dans les approbations.
- Les entrevues avec les gestionnaires supérieurs de programme et les réponses au sondage ont mis en lumière l'importante synergie entre le cyberdomaine et les activités de réseau, et ont indiqué que leur séparation aurait des conséquences négatives.
- Des gestionnaires supérieurs ont suggéré d'établir un commandant militaire dans l'organisation du SMA(GI), doté des ARR appropriées. Toutefois, pour éviter de nuire aux cyberopérations, ce commandant aurait besoin d'un effectif, similaire en taille à celui des autres commandements opérationnels.

MISE EN ŒUVRE ET GESTION DU PROGRAMME

Les cyberforces manquent d'orientation sans ARR claires et d'une représentation suffisante pour influencer les décisions.

CONSTATATION 1 : (Suite)

L'absence d'un champion du cyberdomaine

- Les entrevues avec les gestionnaires de programme ont mis en lumière des préoccupations relativement à la représentation insuffisante du cyberdomaine dans les niveaux les plus élevés de la haute direction.
  - Un examen des procès-verbaux des réunions de l'an dernier (2019) du Conseil de gestion de l'information, du Conseil de développement des capacités de GI/TI, du Conseil de gestion du programme et du Conseil des capacités de la Défense a révélé peu, voire aucune, discussion sur le cyberdomaine dans ces comités de la haute direction.
- Les ARR du CCF n'ont pas été officialisées ni exercées.
  - Le rôle du CCF est l'un des cinq rôles qu'occupe le CEM(GI) sans aucun soutien en personnel. Par conséquent, les cyberinitiatives n'ont pas reçu la priorité ou n'ont pas pu être abordées dans les réunions décisionnelles de la haute direction.
  - Même si le CCF est censé avoir un lien direct avec le CEMD, ce rôle est peu exercé, ce qui cause des retards dans la prise de mesures pour mettre en œuvre les cyberinitiatives militaires.
  - Les personnes interviewées ont suggéré que le rôle du CCF est de conseiller au contraire de commander, et pour cette raison, il n'a pas les mêmes ARR qu'un commandant.
  - Les personnes interviewées croient que des ARR d'un commandant en bonne et due forme sont requises pour intégrer pleinement les cyberforces aux activités. L'officialisation de ce rôle se compare à l'établissement du commandant du renseignement au COMRENSFC ou au commandant de l'Espace dans l'ARC.

Photo : Cplc Patrick Blanchard, IS2014-3024-02

R1 **Pour améliorer la gestion des cyberforces, le SMA(GI) doit revoir, mettre à jour et publier des ARR relatives au cyberdomaine dans tout le MDN et les FAC pour les faire connaître.**

MISE EN ŒUVRE ET GESTION DU PROGRAMME

Le cyberdomaine est actuellement intégré aux organes de gouvernance existants, mais ne possède pas d'organe propre.

CONSTATATION 2 : Le cyberdomaine ne possède pas d'organe de gouvernance interne qui lui est propre. Le cyberdomaine utilise les organes de gouvernance existants du SMA(GI), avec l'appui de groupes de travail qui tendent à avoir une nature informative. Les intervenants sont responsables d'élaborer leurs propres cyberstratégies.

- Tous les intervenants et les gestionnaires de programme du cyberdomaine ont reconnu qu'il n'y a pas d'organe de gouvernance distinct pour le cyberdomaine.
- Quelques groupes de travail agissent en guise d'organe de partage d'information, mais aucune donnée ne montre que des décisions sont prises, ou qu'il y a des autorités fonctionnelles associées qui pourraient permettre ces décisions.
- Dans le cadre du PACM, tous les intervenants du cyberdomaine sont censés élaborer leurs propres cyberstratégies. L'Armée, la Marine et l'Aviation élaborent actuellement leurs propres stratégies, sans cyberstratégie globale des FAC.

- Certains gestionnaires de programme ont déclaré que le cyberdomaine est déjà pris en compte dans des organes de gouvernance existants et n'a pas besoin d'un organe de gouvernance précis. De cette manière, les questions du cyberdomaine sont intégrées aux organes de gouvernance de haut niveau.
- D'un autre côté, d'autres gestionnaires de programme ont fait valoir que les cyberforces devraient avoir un organe de gouvernance indépendant.
  - Cette structure serait conforme à l'orientation stratégique selon laquelle les cyberforces sont un domaine précis.
  - Selon un gestionnaire de programme que nous avons interviewé, un Conseil des cyberforces devrait se réunir régulièrement.
  - Un organe de gouvernance interne pourrait répondre aux préoccupations concernant l'absence du cyberdomaine dans les organes de gouvernance de haut niveau et le manque d'orientation stratégique, tel que présenté à la Constatation 3.

2 **Revoir le cadre de gouvernance actuel pour déterminer si le cyberdomaine a besoin d'une structure distincte.**

GESTION ET MISE EN ŒUVRE DU PROGRAMME

Il y a évidence de planification stratégique et de connaissance en matière de développement de programme.

CONSTATATION 3 : Même s'il existe des documents stratégiques pour la planification des cyberforces, ceux-ci ne sont pas connus ni utilisés largement au MDN et dans les FAC.

Nous avons examiné un nombre de documents de base concernant le cyberdomaine, le développement des cyberforces et l'assurance de la cybermission. Parmi ceux-ci :

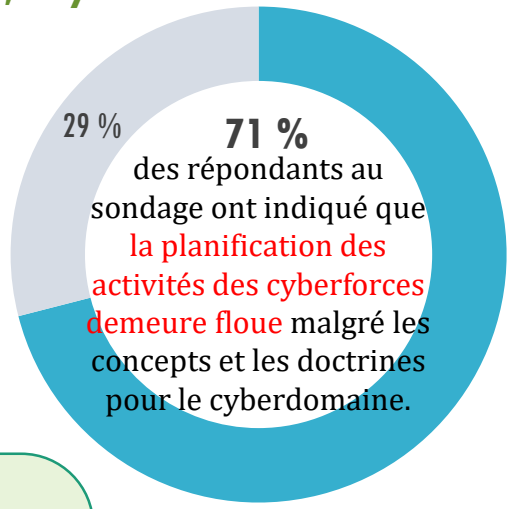
- Directive de mise en œuvre du CEMD (2017);
- Note de doctrine interarmées sur le cyberdomaine (2017);
- Mandat du PACM (2018);
- Note de concept des cyberopérations défensives (2019);
- [Ébauche] Charte du PACM (2019);
- Mises à jour de la Base de terminologie de la Défense.

Par ailleurs, les gestionnaires de programme ont révélé une quantité considérable de travail en cours pour le développement d'autres concepts et doctrines, tel que le renouvellement de la note de doctrine interarmées, ainsi que la rédaction de nouvelles DOAD.

Le DG Cyber a publié et continue nécessairement de publier de multiples documents de doctrines et de concepts de base pour le cyberdomaine…

…Toutefois, malgré les doctrines et les concepts, il y a toujours un manque de clarté.

Les données montrent qu'il y a toujours un manque de clarté concernant le cyberdomaine, dans les aspects qui ont déjà été établis par les gestionnaires de programme, par exemple, la terminologie approuvée. Dans les entrevues avec les intervenants, ils ont indiqué que malgré les documents qui ont été créés, ceux-ci n'étaient pas bien compris ou publiés dans tout le MDN et les FAC. Il s'agit d'un facteur limitatif pour les intervenants qui cherchent à mettre en œuvre des cyberinitiatives dans tout le ministère et à mobiliser l'ensemble du ministère à leur égard.



Stratégies d'amélioration

Pendant les entrevues, les directeurs de programme étaient d'accord qu'il y a un manque de clarté concernant le cyberdomaine. Le DG Cyber a des plans pour mieux intégrer la sensibilisation et la compréhension du cyberdomaine dans le développement professionnel des officiers et des militaires du rang. Ils ont toutefois reconnu que l'élaboration de l'instruction prendrait beaucoup de temps.

- De plus, d'autres mesures de diffusion pourraient être explorées de manière à ce qu'un large public du MDN et des FAC reçoive ces documents stratégiques et en ait connaissance.

Voir Recommandation 1

MISE EN ŒUVRE ET GESTION DU PROGRAMME

La mise en œuvre du Programme d'assurance de la cybermission a été retardée.

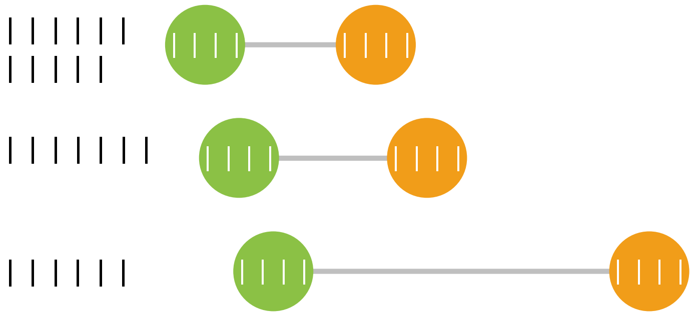
CONSTATATION 4 : La mise en œuvre de l'initiative 87 de la PSE [redacted] étant donné que le soutien pour l'assurance de la cybermission n'est pas une priorité universelle dans l'ensemble du MDN et des FAC.

« L'ACM a besoin non seulement du Groupe GI, mais aussi du VCEMD et des autres N1 concernés pour s'en occuper. »

Comme nous l'avons mentionné précédemment, le PACM est une composante clé du cyberdomaine pour tout le MDN et les FAC. L'importance de l'ACM a été notée et reconnue par toutes les personnes interviewées; elles ont toutefois [redacted]

Les gestionnaires de programme ont les mêmes préoccupations; ils parlent de diverses difficultés dans la mise en œuvre des initiatives de PACM. En particulier [redacted]

Les échéances de mise en œuvre de la définition de la portée, de l'établissement et de l'état final de la PACM [redacted]



Personnel

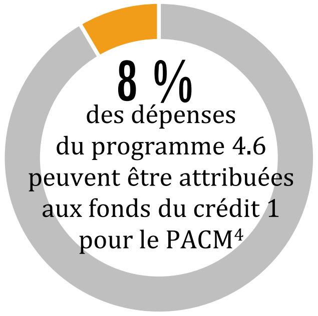
- Les cyberresponsabilités sont souvent assignées au personnel qui a déjà d'autres rôles pré-établis. Par conséquent, l'ACM n'est pas toujours une priorité dans les tâches à accomplir.
- Les cybergroupes dans le MDN et les FAC sont généralement [redacted]
- [redacted]

Signes de progrès

- L'établissement récent d'un chef d'équipe permanent pour le PACM a mené à des progrès et à de la stabilité.
- Des travaux sont en cours pour établir la charte du PACM, afin d'obtenir du financement plus fiable, dans l'attente de l'officialisation du programme.
- Le SMA(Mat) a joué un rôle très important en amorçant les activités de développement et de mise en œuvre pour l'ACM et les processus d'acquisition du matériel visant la résilience de la chaîne d'approvisionnement.

Financement

- Les fonds initiaux de l'AF 2018-2019 n'ont pas été affectés à l'initiative 87 de la PSE (PACM) parce que les budgets du programme ne sont pas encore définis en raison de la nature expérimentale du domaine; la planification et la mise en œuvre ont par alors été restreintes, étant donné les fonds limités qui ont été distribués (p. ex., l'embauche d'entrepreneurs pour mener l'élaboration de programme devient plus difficile).
- La portée et la complexité du PACM ne concordent pas avec les niveaux actuels de financement.
  - Pendant l'AF 2019-2020, le PACM avait un budget de 1 467 000 $ de crédit 1 et de 0 $ de crédit 5.
  - Il y a peu d'indications de budget ou de fonds consacrés spécifiquement aux activités de mise en œuvre du PACM par les autres N1.



[4] GC Infobase [consulté le 23 octobre 2020], [Ébauche] Charte du PACM (2020).

Voir Recommandation 1

MISE EN ŒUVRE ET GESTION DU PROGRAMME

Les cyberforces n'ont pas indiqué les niveaux de préparation opérationnelle requis.

CONSTATATION 5 : La responsabilité de définir la cyberpréparation [redacted] Bien que la Marine a réalisé des progrès dans ce domaine, [redacted]

Suggestion de suivi : Examiner l'officialisation, l'orientation et la conformité de la cyberpréparation opérationnelle

- Des niveaux définis de cyberpréparation opérationnelle deviennent de plus en plus importants alors que les demandes de cyberactivités ne cessent de croître, indiquant des défis à venir relativement à la préparation opérationnelle.
- La préparation opérationnelle ne fonctionnera pas de la même façon pour le cyberdomaine que pour les autres domaines opérationnels. Le terrain change constamment, et le concept de cyberguerre est difficile à définir formellement. La cyberpréparation pourrait avoir une terminologie plus descriptive.
- Les gestionnaires du cyberdomaine ne s'entendent pas pour savoir s'il faut définir les normes de cyberpréparation avant d'établir les qualifications personnelles ou vice-versa. À l'heure actuelle, la définition se fait ponctuellement, individuellement ou en équipe, et est transmise à l'échelon supérieur, au lieu d'être une orientation descendante. Ce point est abordé plus en détail à la Constatation 12.
- Bien qu'il soit important d'intégrer les cybercomposantes à la posture de la force et la disponibilité opérationnelle (PF&DO), il est encore trop tôt pour ce faire étant donné que les cyberforces sont encore en développement. [redacted] comme présenté à la Constatation 9, on nous a signalé que les cyberforces [redacted]
- En ce qui a trait à la responsabilité d'établir des normes de préparation opérationnelle, l'argument le plus convaincant consiste à ce que les normes soient établies par les cyberforces pour faire en sorte que les normes techniques sont établies et que les liens techniques aux organisations externes demeurent à jour. Cette façon de procéder semble poser des difficultés pour le Groupe GI, puisque selon ce que nous avons appris des gestionnaires supérieurs pendant les entrevues, le Groupe GI semble plus axé sur les demandes organisationnelles que sur les demandes opérationnelles.
- En [redacted], la Marine est en train de développer ses propres niveaux de cyberpréparation opérationnelle au sein de trois exigences en matière de préparation au combat.

Photo : Cpl Braden Trudeau, Trinity – Services d'imagerie de la formation, RP24-2019-0043-002

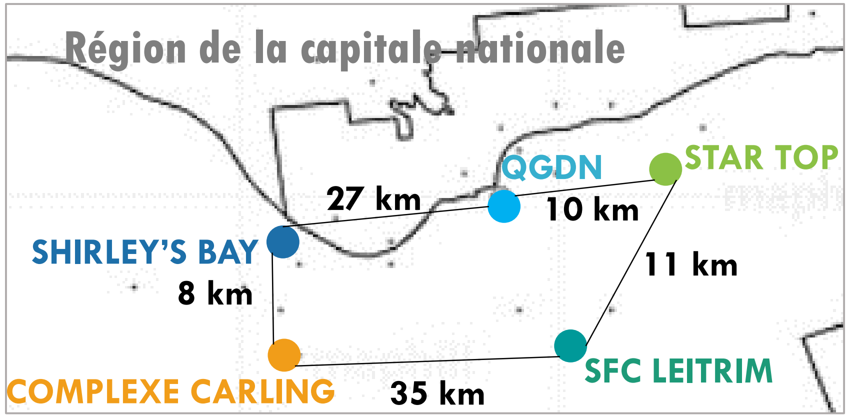
Jusqu'à ce que les structures de la force soient en place, la cyberprépration n'aura pas d'orientation ou d'officialisation.

MISE EN ŒUVRE ET GESTION DU PROGRAMME

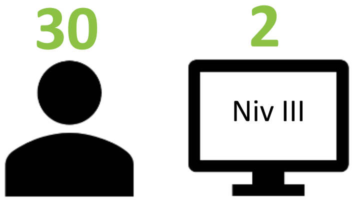
L'absence d'espace de travail prêt pour le cyberdomaine nuit aux opérations et à l'entraînement

CONSTATATION 6 : [redacted]

- L'ébauche de la charte du PACM (2020) énonce : « On prévoit trouver des locaux convenables pour le personnel requis dans les installations existantes du MDN. » Toutefois, la charte ne donne aucun autre détail, [redacted]
- Certains membres du personnel doivent se déplacer entre cinq emplacements distincts répartis d'un bout à l'autre de la région de la capitale nationale afin d'obtenir l'accès aux réseaux autorisés nécessaires, étant donné que les principaux immeubles qui hébergent le cyberpersonnel à l'extérieur du Groupe des opérations d'information des Forces canadiennes (GOIFC) [redacted] Cette situation peut entraîner jusqu'à 200 $ en frais de taxi par semaine pour une seule personne.
- Les personnes interviewées ont indiqué que [redacted] Les réponses au sondage ont également fait écho de cette préoccupation concernant des infrastructures physiques très limitées.
- [redacted]



Courtoisie de Maphill.com



- [redacted]
- Les répondants au sondage [redacted]
- Dans son rapport intitulé *Cyber Collaborative Imperative*, l'Association des industries canadiennes de défense et de sécurité (AICDS) note que les principales fonctions, politiques et pratiques de collaboration des alliés du Canada comprennent des terrains d'expérimentation et des environnements de test des cybercapacités. Ces installations « offrent un environnement où les solutions nouvelles peuvent être mises à l'essai contre des menaces connues. »

[redacted]

- Bien que le complexe sécurisé de la Défense nationale pourrait constituer une solution, entretemps, les opérations, le personnel et les activités courantes se heurtent à des inefficacités hors de proportion.
- À la réunion de janvier 2020 du Conseil des capacités de la Défense, le Chef – Développement des Forces a indiqué que « Le complexe sécurisé de la Défense nationale est une capacité essentielle importante, et sa mise en place doit être accélérée autant que possible. » Le sujet a été abordé à la réunion du Comité de gestion de projet en mars 2020.

R3 **Créer un terrain de cyberentraînement centralisé, institutionnalisé et soutenu, assorti de la capacité d'adapter la classification et d'un accès à distance.**

RECHERCHE ET DÉVELOPPEMENT

Les cyberprojets du MDN et des FAC n'ont pas l'agilité nécessaire pour composer avec les changements dans l'environnement de menaces.

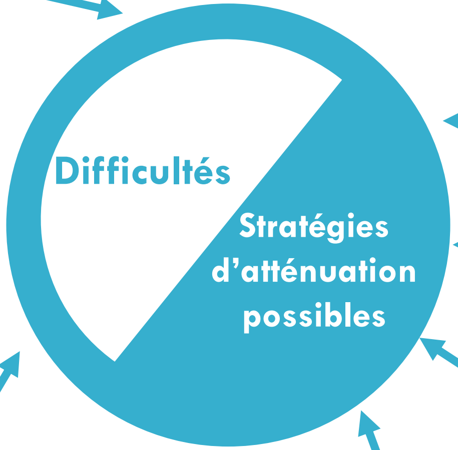
CONSTATATION 7 : [redacted]

Les responsables de la mise sur pied de la force (RMPF) et les utilisateurs de la force[5] ont indiqué que [redacted] en raison du processus actuel d'acquisition.

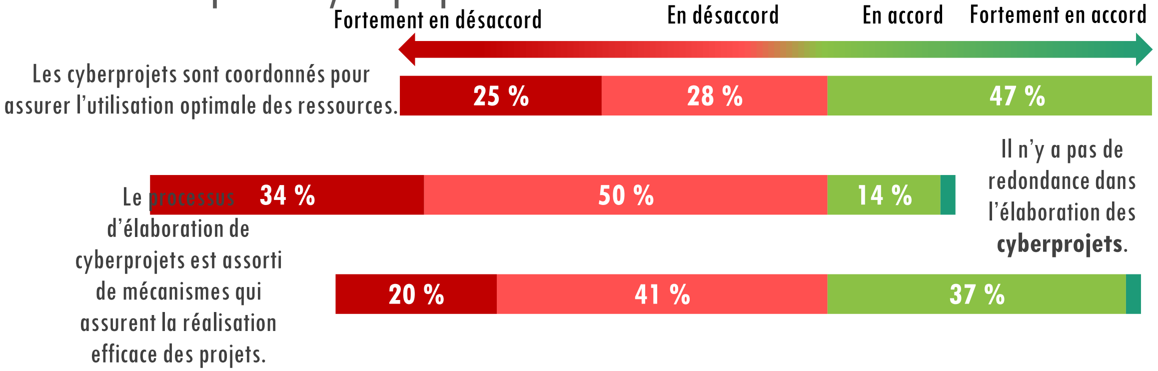
Toutes les personnes interviewées ont noté [redacted]

Le cyberdomaine fait maintenant partie de toutes les capacités de défense – Il faut des organes de gouvernance mobilisés et motivés dans tout le MDN et les FAC. La plateforme relative à l'ACM est liée au processus d'acquisition d'immobilisation. Si ce dernier est nébuleux par rapport au cyberdomaine [redacted]

Beaucoup de projets en cours ont commencé avant que les cyberexigences soient prises en compte, et requièrent alors des modifications coûteuses pour inclure ces cyberexigences.



Les répondants au sondage sont fortement en désaccord ou en désaccord que les cyberprojets sont efficaces.



Les projets qui demeurent sous la barre des 5 M$ peuvent avancer plus rapidement dans le processus d'acquisition, et ainsi diminuer les menaces et les risques associés aux changements technologiques et augmenter les possibilités d'exploiter la technologie.

Le SMA(GI) discute des options avec le SCT afin d'examiner le processus relatif aux projets d'immobilisation dans le but de trouver des moyens de le rendre plus efficaces, selon les personnes interviewées.

Le SMA(S & T) peut informer sur ce qui peut être fait au moyen du développement de prototypes, pour montrer aux intervenants le type de fonctions auxquelles ils devraient s'attendre s'ils achètent un produit commercial.

La mise en œuvre d'un programme financé afin de permettre l'acquisition rapide d'outils au lieu d'y aller projet par projet est l'une des options. Le programme de cryptographie du SMA(GI) est un exemple de ce genre de programme; le COMFOSCAN met en œuvre un processus d'acquisition axé sur la capacité pour résoudre le même problème.

L'intégration appropriée du PACM pourrait atténuer l'incidence des changements technologiques et l'inclusion des cyberconsidérations.

[5] Les responsables de la mise sur pied de la force sont responsables d'organiser, d'instruire et d'équiper les forces pour l'utilisation de la force. P. ex. : AC, MRC, ARC. Les utilisateurs de la force sont responsables du commandement, du contrôle et du maintien en puissance de la force attribuée. P. ex. : (COIC, COMFOSCAN)

RECHERCHE ET DÉVELOPPEMENT

Les cyberforces interagissent grandement avec de nombreux intervenants.

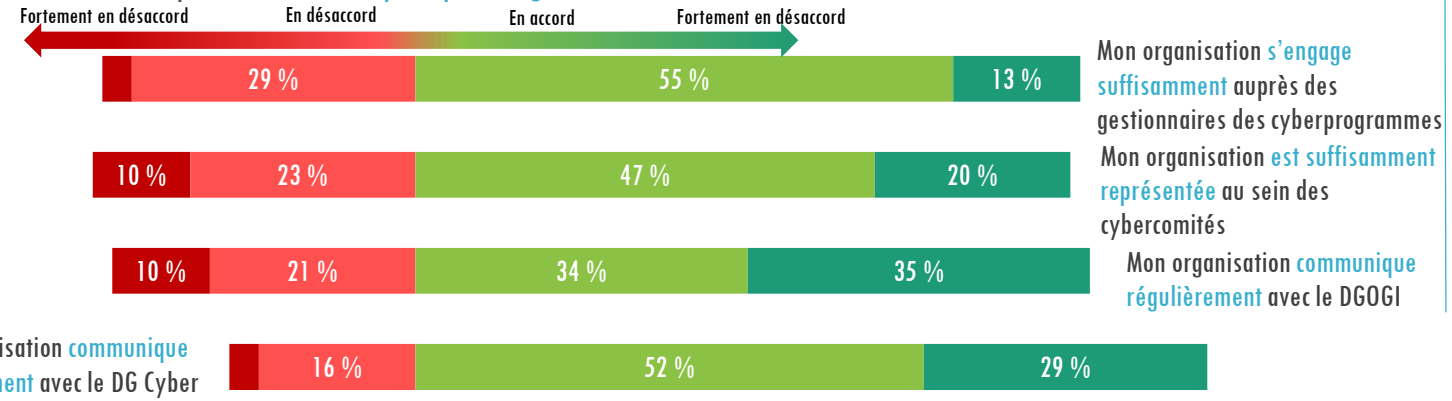
CONSTATATION 8 : La conception du programme a intégré les connaissances pertinentes des intervenants du MDN, des FAC, des autres ministères et des alliés; toutefois, la mobilisation de l'industrie privée et du milieu universitaire pose problème.

MDN et FAC

Nous avons trouvé beaucoup de preuves de mobilisation interne et de participation des organisations N1 et des commandements d'armée :

- Les 12 organisations internes d'intervenants du MDN et des FAC qui ont été interviewées ont indiqué qu'elles participent au développement des cyberforces dans leur secteur respectif et qu'elles continuent d'interagir avec le DG Cyber par l'intermédiaire des groupes de travail. En particulier, le Comité directeur sur la cybersécurité facilite le transfert de connaissances; il n'est toutefois pas un organe de gouvernance.
- Le SMA(Mat) est suffisamment mobilisé dans les pourparlers concernant les plateformes technologiques et prend appui sur le SMA(S & T) pour intégrer les systèmes de cybersoutien.
- Le SMA(S & T) détermine et met en ordre de priorité les cyberexigences et en fait l'essai, relativement aux capacités qui ne peuvent pas être acquises commercialement. Il démontre aussi les liens entre la TI et les plateformes technologiques pour les commandements d'armée.
- Le SMA(IE) participe à des discussions concernant la technologie opérationnelle dans le cadre de ses travaux pour élaborer et mettre en œuvre des cyberstratégies pour les infrastructures de défense.

Les résultats du sondage montrent que la majorité des intervenants du cyberdomaine du MDN et des FAC sont en accord ou fortement en accord qu'ils ont vécu des pratiques de gestion efficaces.



Autres ministères

Dans l'ensemble, les entrevues avec les gestionnaires de programme ont mis en évidence les différentes relations avec les autres ministères. Le MDN et les FAC sont présents dans quelques comités interministériels, comme le comité stratégique du DG Cyber.

- Le CST a été mentionné comme un important partenaire gouvernemental du MDN et des FAC à titre de responsable principal de la mise sur pied du Centre canadien pour la cybersécurité.
  - Des initiatives prometteuses de collaboration accrues entre les organisations ont vu le jour, comme pour l'instruction. Toutefois, des différences dans les cultures organisationnelles entre le CST et le MDN mènent parfois à des malentendus qui nuisent aux occasions de collaboration.
- Le MDN et les FAC interagissent régulièrement avec la Sécurité publique, qui dirige un certain nombre de forums du gouvernement du Canada sur le cyberdomaine.
- Le SMA(S & T) siège à divers comités de cyberrecherche, tels que celui dirigé par Innovation, Sciences et Développement économique concernant la main d'œuvre en formation.
- Quelques personnes interviewées ont noté cependant le besoin d'éclaircir les ARR avec SPC.

RECHERCHE ET DÉVELOPPEMENT

Les cyberforces interagissent grandement avec de nombreux intervenants.

CONSTATATION 8 : (Suite)

Alliés

Le DGOGI et le DG Cyber entretiennent des relations avec nombre de partenaires et d'alliés internationaux, qui représentent une source de meilleures pratiques à intégrer dans les cyberforces. Dans certains cas, les relations avec les alliés sont plus actives que celles avec les autres ministères :

- Les postes de liaison hors du Canada servent d'intermédiaire avec les alliés pour le partage d'information; toutefois, [redacted]
- Particulier aux États-Unis, des séances d'information régulières du comité de cybercoordination entre les cyberforces des FAC et le US CYBERCOM permettent un partage d'information efficace et la détermination des meilleures pratiques.
    - Le Cyber Safe Program des États-Unis a été ciblé comme un modèle de protection et de sécurité de l'information, qui pourrait être émulé.
- Le MDN et les FAC participent aux exercices CYBER FLAG des États-Unis pour découvrir et partager des stratégies pour l'élaboration de l'entraînement des cyberforces avec les partenaires du Groupe des cinq.
- Le MDN et les FAC participent à diverses cyberinitiatives de l'OTAN et d'autres conférences multinationales.

Industrie privée

Le Canada compte 275 cyberentreprises, parmi lesquelles 250 sont liées à la cybersécurité des TI et 25 à la cyberdéfense[6]. L'industrie a beaucoup à offrir, comme l'innovation et l'agilité, qui pourraient servir à renforcer les cyberforces. Le programme Mobilisation des idées nouvelles en matière de défense et de sécurité (MINDS) du MDN réunit à une même table le MDN et l'industrie et peut être le moyen le plus rapide d'intégrer le cyberdomaine aux activités et aux opérations du MDN et des FAC. Il y a toutefois quelques obstacles qui limitent des partenariats accrus :

- Un manque de financement en recherche, selon l'industrie;
- La mobilisation tardive de l'industrie par le MDN, à cause des processus d'acquisition actuels;
- L'absence d'un poste de liaison permanent entre le MDN et l'industrie;
- Des visions de portée différentes entre le MDN et l'industrie;
- Des règles qui dictent la participation ministérielle dans les contrats de développement et d'acquisition de capacités;
- Des préoccupations de sécurité générale, en raison de :
    - La propriété et la protection des droits de propriété intellectuelle des capacités de cyberdéfense du MDN;
    - Les risques d'échec ou de vente de l'entreprise partenaire.

Milieu universitaire

Il y a eu très peu de mobilisation du milieu universitaire, à l'exception du Collège militaire royal (CMR), où la mobilisation est robuste. Il réalise de la science et de la technologie, et offre des perspectives en recherche et développement dans le cyberdomaine. Dans les entrevues avec les gestionnaires supérieurs de programme, ils ont indiqué certaines difficultés dans la mobilisation du milieu universitaire :

- les risques de sécurité inhérents à former des partenariats avec le milieu universitaire;
- Un manque de fonds de subventions du crédit 10 pour financer la recherche.

« Le CMR comble l'écart mais n'est pas une solution modulable. »

[6] *The Cyber Collaboration Imperative, AICDS (2019)* [consulté le 23 octobre 2020]

MISE SUR PIED DU PERSONNEL

Les cyberforces comptent un nombre suffisant de postes; toutefois, la dotation de ces postes pose problème.

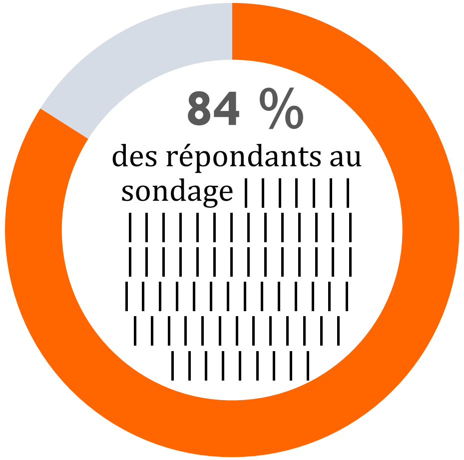
CONSTATATION 9 : Des postes du cyberdomaine ont été alloués partout au MDN et dans les FAC, [redacted]

- L'attrait et le maintien en poste du cyberpersonnel tant civil que militaire ont été [redacted]
- [redacted]
- [redacted]
- De plus, [redacted] par les exigences en ressources organisationnelles du SMA(GI).
- De manière cyclique, [redacted] comme l'indique le sondage.
- Des progrès ont récemment été réalisés dans l'établissement de relations plus solides avec les établissements d'éducation, par une présence dans les événements pour attirer la main d'œuvre et par l'utilisation du Programme subventionné de formation universitaire pour attirer des postulants.
- Le CORFC signale qu'il avait [redacted] au moment de l'évaluation.

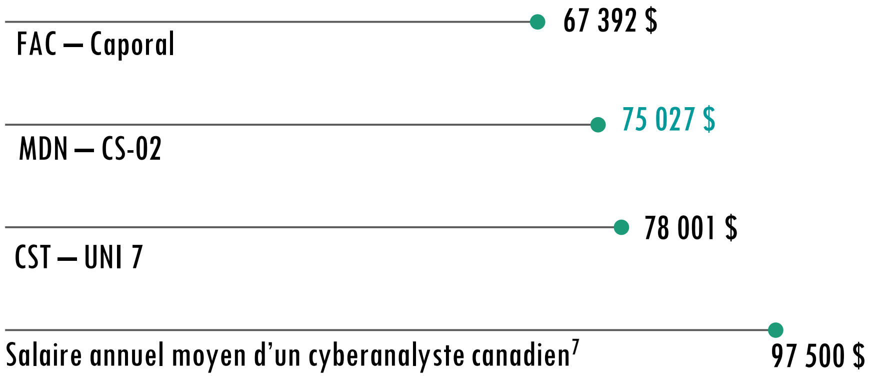
Cyberforces civiles

- Il est particulièrement difficile d'attirer du personnel civil et de le maintenir en poste en raison de la nature concurrentielle des occasions d'emploi dans le cyberdomaine.
- 93 pour cent des répondants au sondage et la majorité des personnes interviewées sont d'accord que le MDN et les FAC bénéficieraient de l'embauche (additionnelle) de cyberpersonnel civil, pour stabiliser la mémoire institutionnelle.
- L'embauche de cyberpersonnel civil demeurera un défi en raison des modèles actuels de rémunération, qui sont liés à la classification, et qui limitent le potentiel de croissance du personnel technique. Cette raison a aussi causé des problèmes de maintien en poste du personnel militaire, dès qu'il est formé dans le cyberdomaine. La classification Systèmes d'ordinateur (CS) est jugée inadéquate pour les activités liées au cyberdomaine.
- « ...[si] vous leur accordez une promotion pour augmenter leur rémunération, selon la définition de l'emploi, ils ne feront pas le travail concret pour lequel vous les avez embauchés. » Les personnes interviewées ont indiqué que beaucoup d'employés dans des postes techniques ne veulent pas occuper des fonctions de gestion.

« Nous ne sommes pas concurrentiels dans un milieu concurrentiel. »



Le MDN et les FAC ne sont pas en mesure d'offrir des salaires concurrentiels aux cyberanalystes



[7] www.neuvoo.ca fondé sur 53 salaires [consulté le 23 octobre 2020]

Le manque de cyberpersonnel met à risque la mise en œuvre du programme.

MISE SUR PIED DU PERSONNEL

L'avancement professionnel du cyberpersonnel militaire a besoin d'amélioration.

CONSTATATION 10 : L'avancement de carrière du cyberpersonnel est limité. Toutefois, on y remarque des signes d'amélioration.

- L'absence de plan d'avancement de carrière a été notée comme une difficulté par les répondants du sondage, un aspect susceptible de nuire au maintien en poste des cyberopérateurs. Même si les préoccupations relatives au maintien en poste sont largement théoriques en ce moment en raison du petit nombre des personnes dans cet emploi et de la nouveauté des cyberforces, les problèmes de maintien en poste dans des emplois connexes causent des préoccupations pour les cyberforces.
- Les cyberforces dépendent des gestionnaires de carrière pour fournir du personnel doté de cybercompétences, de manière ponctuelle. Si les gestionnaires de carrière ne sont pas au courant d'un intérêt ou d'une compétence technique, ou si les cyberforces vivent une croissance qui dépasse ce qui est facilement gérable dans une petite communauté, cette manière de procéder pourrait entraîner des risques. Une étude sur l'emploi de cyberopérateur est une initiative prévue pour résoudre cette situation. Cette étude est présentée dans l'étude de cas qui a été menée pour l'évaluation.
- L'érosion des compétences se produit rapidement dans le cyberdomaine. Les personnes qui alternent entre les affectations dans le cyberdomaine et les affectations dans d'autres domaines perdent rapidement l'expertise technique qu'ils ont mis des années à acquérir.
- À titre de comparaison, l'AICDS énonce dans son rapport *The Cyber Collaboration Imperative* (2020) qu'aux États-Unis, le cyberpersonnel travaille dans ce domaine depuis 20 ans, et en Russie, depuis 30 ans.
- Le cyberpersonnel technique promu à un poste de gestion a mené à de la démotivation et à de l'attrition. À l'inverse, le cyberpersonnel qui compte le plus d'expérience, et qui travaille pour du personnel qui possède peu d'expérience du cyberdomaine a mené à beaucoup de frustration, selon les données d'entrevue et de sondage.
- La composition et le développement du cybereffectif restent à définir alors que la taille éventuelle de la totalité des effectifs des cyberforces continue d'évoluer.
- Malgré ces difficultés, les répondants au sondage ont souligné que l'avancement de carrière s'améliore puisque le personnel qui occupe des postes du cyberdomaine peut maintenant avoir accès aux occasions d'emploi requises pour faire avancer leur carrière. Un appel d'intérêt pour occuper des cyberpostes vient d'être récemment affiché dans l'ensemble du MDN et des FAC, pour permettre aux cyberforces d'avoir recours aux compétences du personnel existant.

« La structure d'emploi ad hoc … ne résout pas le problème de donner aux bonnes personnes l'instruction appropriée et puis de les employer dans les opérations du cyberdomaine. » – Cyber Operator Occupation Briefing

Suggestion de suivi : Examiner les occasions d'avancement de carrière des cyberopérateurs.

63 % des répondants au sondage ont indiqué qu'il n'y avait pas de gestion de carrière réelle pour l'emploi de cyberopérateur.

Afin de suivre le rythme des alliés et des adversaires, le MDN et les FAC doivent voir à garder les compétences du cyberpersonnel à jour et à le garder en poste dans le cyberdomaine.

MISE SUR PIED DU PERSONNEL

Les opinions demeurent partagées sur la nécessité d'établir un groupe professionnel de cyberofficiers.

ÉTUDE DE CAS : Cyberofficier

Pourquoi : Dans le cadre de l'évaluation, nous avons réalisé une étude de cas sur un quasi-cyberofficier, après que le sujet ait été soulevé dans les entrevues pour établir la portée, et pour déterminer si les attentes et les exigences techniques à l'égard des cyberopérateurs justifiaient la possibilité de la création d'un emploi de cyberofficier. Puisqu'il est encore trop tôt pour former une opinion éclairée à cet égard, nous avons analysé les opinions actuelles et le contexte concernant un emploi de cyberofficier possible.

Comment : Nous avons interviewé le sujet de l'étude, nous avons posé des questions aux répondants du sondage et des questionnaires et nous avons parlé avec les personnes interviewées.

Faits saillants de l'analyse

- Un officier assume des responsabilités supplémentaires qui concernent la gestion ainsi que la planification et la mise en œuvre stratégique d'initiatives.
- Un niveau de compréhension et de connaissance technique du cyberdomaine est attendu et prend des années à acquérir afin d'être fonctionnel dans le cyberdomaine.
- La personne visée par l'étude de cas a informé que les responsabilités actuelles des cyberopérateurs, particulièrement ceux qui travaillent dans les cyberopérations actives, requièrent un sens de l'initiative et une débrouillardise bien plus grands que ceux associés aux rôles de cyberopérateurs types, mais plus similaires à ceux généralement associés aux officiers.
- Si le cyberdomaine est un domaine en soi, pour être pleinement développé comme les autres domaines (terrestre, maritime et aérien), on a fait valoir qu'un emploi de cyberofficier devrait exister pour permettre le développement continu des cyberforces.
- Même avec la croissance prévue dans les prochaines années, le personnel ne sera peut-être pas suffisant pour justifier un emploi de cyberofficier pour superviser le groupe des cyberopérateurs, et l'avancement de carrière serait limité aux postes disponibles.
- Certaines personnes interviewées ont plaidé pour un rôle d'officier de nature plus générale, pour faire en sorte qu'il ne soit pas trop axé sur le cyberdomaine et qu'il perde de vue le portrait général des opérations de commandement, contrôle, communication, informatique, renseignement, surveillance et reconnaissance et réseau. Un bassin de cyberofficiers pourrait être rassemblé à partir des groupes professionnels des officiers du génie électronique et des communications et des officiers des transmissions.

84 % des répondants au sondage croient que le MDN et les FAC bénéficieraient de la création d'un groupe professionnel de cyberofficiers. La majorité de ces répondants se trouve aux niveaux tactique et opérationnel.

Toutefois, la majorité des gestionnaires supérieurs interviewés n'étaient pas d'accord.

- 66 pour cent des personnes interviewées pensent qu'il n'est pas nécessaire de créer un groupe professionnel de cyberofficiers.

- Sans égard à l'opinion concernant la nécessité d'un groupe professionnel de cyberofficiers, 53 pour cent des personnes interviewées ont parlé du besoin d'une meilleure gestion de carrière dans le cyberdomaine, tel que présenté à la Constatation 10.

Suggestion de suivi :
Examiner les résultats de l'étude sur le cyberleadership qui a été menée par le Directeur – Développement des Forces (Opérations cybernétiques) (DDFOC) qui devait commencer en mars 2020, qui servira à examiner cette question

MISE SUR PIED DU PERSONNEL

Des retards dans les autorisations de sécurité affectent négativement les cyberforces.

CONSTATATION 11 : Les échéances et les processus relatifs aux autorisations de sécurité

- Des données écrasantes montrent que les échéances et les processus relatifs aux autorisations de sécurité pour le personnel civil et militaire

-

- Des personnes interviewées ont rapporté qu'elles ne peuvent pas assister aux réunions nécessaires en raison des exigences en matière d'autorisation de sécurité.

- Des gestionnaires supérieurs rapportent qu'ils ne sont pas en mesure de recruter des stagiaires ou des étudiants au moyen de certains mécanismes comme le Programme fédéral d'expérience de travail étudiant, puisqu'ils ne peuvent pas leur montrer le travail qui pourrait les intéresser à cause de l'absence d'exigences appropriées en matière d'autorisation de sécurité en place, Toutefois, des personnes interviewées ont signalé que les autres ministères et organismes sont capables de recruter des centaines d'étudiants par été, et de leur obtenir une autorisation de sécurité TRÈS SECRET dans leur premier mois d'emploi à l'aide du polygraphe. Cette méthode pourrait être explorée davantage par les cyberforces.

- Le problème joue sur deux plans – L'obtention des autorisations de sécurité est lente, et le travail à faire doit être classifié correctement. Les personnes interviewées ont indiqué que beaucoup de travail qui est réalisé au niveau TRÈS SECRET n'a pas besoin de ce niveau sécurité, ce qui crée un problème auto-imposé. Le travail non classifié et SECRET devrait être maximisé pour réduire le fardeau sur les infrastructures sécurisées limitées, tel que présenté à la Constatation 6.

82 % des gestionnaires supérieurs qui ont répondu au sondage ont indiqué que les approbations pour les autorisations de sécurité

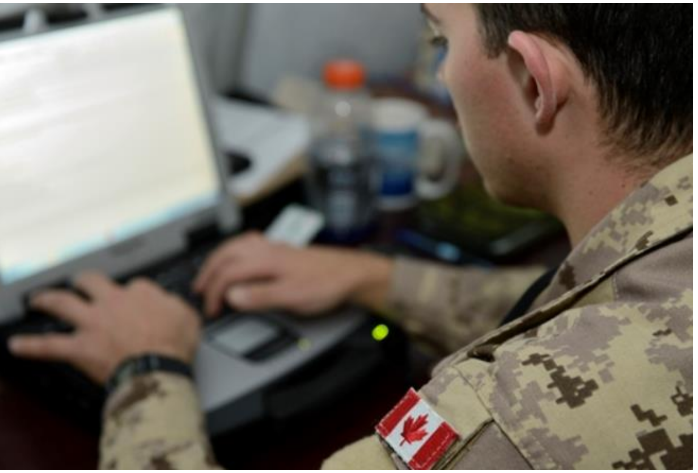
72 % des répondants au sondage ont indiqué que les approbations pour les autorisations de sécurité

MISE SUR PIED DU PERSONNEL

Les FAC ne parviennent pas à suivre le rythme des besoins dans le cyberdomaine; la cyberinstruction donnée par des tiers manque de normes et de validation.

CONSTATATION 12 : Au fur et à mesure que se poursuivent l'élaboration et l'officialisation du cyberentraînement, [redacted]

- Les personnes interviewées sont d'accord qu'en raison de la complexité et de l'évolution constante du cyberdomaine, l'instruction des FAC n'est pas assez agile pour suivre le rythme. 91 pour cent des répondants préfèrent l'instruction donnée par des tiers, mais que cette instruction requiert une standardisation et une validation.
- Dans les entrevues, une personne a noté que « L'École d'électronique et des communications des Forces canadiennes (EECFC) ne peut à elle seule soutenir le cycle d'instruction du cyberdomaine. » Cette déclaration est appuyée par le *Cyber Operator Occupation Briefing* (2017) dans lequel on note que les cyberforces utilisent un modèle d'instruction « juste assez, juste à temps ».
- L'instruction donnée par des tiers est perçue comme étant plus économique et pourrait mieux permettre aux cyberforces de réagir aux avancées rapides vécues dans ce domaine.
- Les commentaires des répondants au sondage mettent aussi en évidence cette lacune dans l'instruction, alors que les répondants étaient préoccupés du manque de normes pour les compétences attendues, combinés avec l'absence d'une validation des cours donnés par des tiers qui pourraient poser un risque que les opérateurs n'aient pas les compétences requises.
- Comme nous l'abordons à la Constatation 9, [redacted] Les FAC sont dans la situation où elles doivent choisir entre mener des cyberopérations ou mener de l'instruction pour les cyberforces pour acquérir les compétences nécessaires. Les données montrent que les opérations reçoivent la priorité.



Caméra de combat des FAC, MDN, IS2014-7532-11

L'ébauche de la charte du PACM (2020) énonce que « Il est attendu que l'instruction de certains spécialistes sera requise pour développer les compétences nécessaires à ce programme – la nature de ces compétences sera déterminée pendant l'analyse des options. »

À l'AF 2020-2021, l'équipe du PACM mènera une analyse des besoins en matière d'instruction, officialisera le cadre d'instruction et de sensibilisation, et publiera une orientation sur l'instruction commune, qui sont tous en bonne voie de réalisation.

Sans savoir si l'instruction des cyberopérateurs respecte une norme attendue, les cybereffets pourraient avoir des conséquences inattendues.

R4

Évaluer la faisabilité de standardiser l'instruction donnée par des tiers et de valider cette instruction.

Conclusions

En tant que nouveau groupe, les cyberforces sont activement engagées dans diverses activités pour établir la position du Canada dans le cyberdomaine de la guerre. Le DG Cyber et le DGOGI, qui sont responsables des cyberactivités au MDN et dans les FAC, ont préparé plusieurs initiatives et y travaillent pour mettre en place les composantes fondamentales requises pour des cyberforces efficaces à l'avenir. Toutefois, à moins d'accorder une attention appropriée au cyberdomaine, le rythme de mise en œuvre continuera d'être limité.

La théorie de la conception du programme des cyberforces est robuste. Une planification stratégique approfondie et une vaste connaissance sont manifestes dans le développement des cyberforces, dans la préparation des concepts et des doctrines du cyberdomaine, ainsi que dans l'officialisation de la terminologie. De plus, le DG Cyber et le DGOGI ont maintenu un engagement élargi pour voir à ce que les connaissances pertinentes et la mobilisation des intervenants soient prises en compte dans la conception des cyberforces. Une mobilisation continue avec les intervenants ainsi que l'intégration des meilleures pratiques et des leçons retenues feront en sorte d'avoir des cyberforces efficaces.

Les cyberintervenants ont besoin d'une plus grande orientation stratégique. Malgré une théorie de programme robuste, les cyberintervenants ont indiqué qu'ils ont besoin d'une plus grande orientation stratégique pour guider leur propre mise en œuvre des cyberinitiatives. Ils agissent sans cette orientation en ce moment (p. ex., cyberpréparation). Pendant la période visée par l'évaluation, il n'existait pas de cybervision d'ensemble du MDN ou des FAC.

Les cyberforces ont besoin d'un soutien et d'un investissement de l'ensemble du MDN et des FAC pour assurer une mise en œuvre complète et efficace de l'ACM et des autres cyberinitiatives. Le MDN et les FAC doivent procéder à un changement culturel pour reconnaître l'importance de l'ACM, puisqu'elle est essentielle à toutes les activités et les opérations du MDN et des FAC. Les cyberinitiatives touchant la totalité du MDN et des FAC ne peuvent pas être mises en œuvre sans le soutien des N1 et de leurs cyberéquipes respectives. Les processus pourraient avoir à évoluer afin de tenir compte des cyberforces. À l'heure actuelle, les activités de mise en œuvre du cyberdomaine risquent de vivre des retards et des limitations si elles n'ont pas les ressources appropriées pour faciliter leur mise en œuvre dans tout le Ministère.

Les premiers développements de programme montrent des signes de progrès pour l'instruction des cyberforces. La création du groupe professionnel des cyberopérateurs a exigé l'élaboration rapide du contenu de cours et de perfectionnement professionnel pour soutenir le nouveau groupe. De plus, des initiatives pour accroître la sensibilisation et les connaissances à l'égard du cyberdomaine parmi le personnel civil et militaire ont été lancées partout au pays.

ANNEXE A — PLAN D'ACTION DE LA DIRECTION

Recommandation du SMA(Svcs Ex)

1. Pour améliorer la gestion des cyberforces, le SMA(GI) doit revoir, mettre à jour et publier des ARR relatives au cyberdomaine dans tout le MDN et les FAC et les faire connaître.

Mesure de la direction 1

- Le SMA(GI) reconnaît la décision du Conseil des Forces armées de février 2018, dans laquelle il adopte les ARR pour la création d'un commandant des cyberforces (CCF), d'un chef d'état-major du cyberespace (CEM Cyber) et du commandant de la cybercomposante de la force interarmées (CCCFI). Le poste de CCF a été établi par la SM et le CEMD dans la lettre d'organisation du QGDN en février 2018.
- Plan d'action en trois parties, comme suit :
  - **1.1 :** Déterminer l'état des postes de leadership des cyberforces, comme le CCF, le CEM Cyber, le CCCFI, et prendre les mesures nécessaires pour que chaque poste soit correctement établi;
  - **1.2 :** À la suite d'une orientation stratégique supplémentaire, travailler avec les intervenants de N1 pour déterminer les ARR appropriées pour chaque rôle (gestion de la force, développement de la force, mise sur pied de la force, emploi de la force) à l'intérieur des cyberforces au niveau de la haute direction;
  - **1.3 :** Publier les ARR à l'aide des instruments organisationnels appropriés, tels que les DOAD, la doctrine et les politiques du MDN.

BPR : CEM Cyber / DGDFCI
Date cible : Mars 2021

Recommandation du SMA(Svcs Ex)

2. Revoir le cadre de gouvernance actuel pour déterminer si le cyberdomaine a besoin d'une structure distincte.

Mesure de la direction 2

- Le CEM Cyber et le Directeur général – Développement des forces (Capacités d'information) (DGDFCI), en consultation avec le CEMD et d'autres autorités de N1, élaboreront, évalueront et formuleront des recommandations pour déterminer si le cyberdomaine a besoin d'une structure de gouvernance distincte. Les recommandations tiendront compte des critères suivants :
  - **2.1 :** Faire correspondre les mécanismes de gouvernance pour le cyberdomaine avec ceux des domaines terrestre, maritime, aérien et spatial, conformément à l'approche des FAC au concept d'emploi de la force dans tous les domaines;
  - **2.2 :** Voir à ce que la gouvernance du PACM reflète la nature globale au MDN et dans les FAC de la cyberrésilience des personnes, des processus et des technologies, dans le but d'assurer le succès de la mission dans tous les cyberdomaines contestés;
  - **2.3 :** Mener la conception organisationnelle des systèmes de gouvernance pour faire en sorte que ces systèmes soient pratiques et viables.

BPR : CEM Cyber / DGDFCI
Date cible : Juin 2021

ANNEXE A — PLAN D'ACTION DE LA DIRECTION

Recommandation du SMA(Svcs Ex)

3. Créer un terrain de cyberentraînement centralisé, institutionnalisé et soutenu, assorti de la capacité d'adapter la classification et d'un accès à distance.

Mesure de la direction 3

- Le CEM Cyber et le DGDFCI reconnaissent les préoccupations relatives à l'accès limité aux cyberespaces d'entraînement qui servent aux simulations et aux entraînements, ainsi qu'aux infrastructures physiques pour y accéder.
- Plan d'action en trois parties, comme suit :
  - **3.1 :** Accepter officiellement l'environnement de collaboration de test de sécurité / l'environnement intérimaire de cyberentraînement comme environnement d'entraînement cyberimmersif intérimaire des FAC;
  - **3.2 :** Déterminer les exigences de l'environnement d'entraînement cyberimmersif intérimaire des FAC en collaboration avec les N1;
  - **3.3 :** Déterminer si un projet d'immobilisation est requis pour établir une solution permanente de cyberespace d'entraînement.

BPR : CEM Cyber / DGDFCI
Date cible : Mars 2022

Recommandation du SMA(Svcs Ex)

4. Évaluer la faisabilité de standardiser l'instruction donnée par des tiers et de valider cette l'instruction.

Mesure de la direction 4

- Pendant que le CEM Cyber et le DGSFCI élaborent le cyberentraînement et envisagent de l'instruction donnée par des tiers, l'autorité de la cyberinstruction (Chef du personnel militaire/Groupe d'instruction de la génération du personnel militaire [CPM/GIGPM]) collaborera pour en faire la validation. Une partie de l'instruction donnée par des tiers est considérée comme la norme de l'industrie (certification ou qualification), et ne requiert donc pas de validation.
- Plan d'action en trois parties, comme suit :
  - **4.1 :** En collaboration avec l'autorité de la cyberinstruction, le DGDFCI continuera de valider l'instruction donnée par des tiers. Nous miserons sur l'instruction donnée par des tiers, y compris par les alliés au besoin quand il y a des lacunes d'instruction;
  - **4.2 :** Continuer de travailler avec le programme d'accréditation, de certification et d'équivalences des FAC pour reconnaître les institutions postsecondaires admissibles;
  - **4.3 :** Continuer de travailler avec le groupe de travail sur les cybercompétences et le perfectionnement de la main d'œuvre, du gouvernement du Canada, qui examine la cyberinstruction globale pour tout le gouvernement, et qui utilise des domaines d'intérêt communs pour l'instruction et l'éducation individuelle, et lorsque possible, mettre en commun les validations et les leçons retenues.

BPR : CEM Cyber / DGDFCI
BRC : CPM / GIGPM
Date cible : Processus de validation en cours / résultats du groupe de travail sur les cybercompétences, juillet 2021

ANNEXE B — ANALYSE COMPARATIVE ENTRE LES SEXES PLUS (ACS+)

Selon la *Directive sur les résultats* (2016) du CT, Procédures obligatoires pour les évaluations, nous avons pris compte dans cette évaluation de la politique pangouvernementale sur l'ACS+ parce qu'elle avait été jugée pertinente.

La grille d'évaluation comportait un indicateur de rendement clé relatif à l'ACS+ : « Les considérations liées à l'ACS+ sont prises en compte durant le processus d'embauche »

Le sondage sur les cyberforces comportait diverses questions liées à l'ACS+ :

- Dans la section sur l'auto-identification, dans le but de ventiler les données, nous avons demandé aux répondants : s'ils étaient militaires, civils ou anciens militaires; leur âge; leur langue maternelle et seconde; leur sexe; leur identité de genre; leur origine ethnique.
- Les questions suivantes étaient incluses dans la section sur l'instruction :

Questions du sondage sur les cyberforces	% en accord
La planification et la mise en œuvre du Programme des cyberforces tiennent compte des initiatives en matière de diversité et d'inclusion du MDN et des FAC.	96 %
Les politiques relatives aux cyberforces intègrent des considérations liées à l'ACS+.	85 %
Les considérations liées à l'ACS+ sont prises en compte durant le processus d'embauche du cyberpersonnel.	87 %
Les initiatives liées au genre et à la diversité sont prises en compte dans l'élaboration de l'instruction à l'intention des cyberopérateurs.	77 %

- Alors que les résultats du sondage étaient généralement positifs concernant les considérations d'ACS+, les réponses aux entrevues ont varié. Beaucoup ont exprimé qu'il n'y avait pas de facteurs uniques à l'ACS+ intégrés à la planification ou à l'embauche, et qu'aucun suivi de ces facteurs n'était fait.
- Un répondant au sondage a indiqué que le DG Cyber est un employeur qui souscrit au principe de l'égalité des chances en matière d'emploi, et qu'il embauche des personnes avec des facteurs d'identité différents tant qu'elles satisfont aux critères d'études et de compétences techniques et qu'elles peuvent obtenir l'autorisation de sécurité requise. Le même répondant a indiqué que son organisation est en train d'évaluer si l'accès à ses services présente des obstacles à l'égalité pour les personnes de compétences différentes.

Condition féminine Canada définit l'ACS+ comme suit :

L'ACS+ est un processus analytique qui fournit une méthode rigoureuse pour évaluer les inégalités systémiques, ainsi qu'un moyen de déterminer comment différents groupes de femmes, d'hommes et de personnes de diverses identités de genre peuvent vivre les politiques, programmes et initiatives. Le signe « plus » dans ACS+ reconnaît que l'ACS+ ne se limite pas aux différences biologiques (sexe) et socioculturelles (genre). Nous avons tous de multiples facteurs identitaires qui se recoupent et contribuent à faire de nous ce que nous sommes. L'ACS+ examine de nombreux autres facteurs identitaires comme la race, l'origine ethnique, la religion, l'âge, et les handicaps de nature physique ou mentale.

Seuls environ **5 pour cent** des répondants au sondage sur les cyberforces se sont identifiés comme des femmes, et la majorité de celles-ci étaient militaires. À la lumière de l'initiative du CEMD d'augmenter la présence des femmes dans les FAC, certaines initiatives pourraient être explorées pour s'harmoniser avec cette intention. La Stratégie des Forces armées canadiennes à l'égard de la diversité (2016) du CEMD stipule que « il est essentiel que les Forces armées canadiennes (FAC) reflètent la société qu'elles servent si elles veulent établir des liens avec les Canadiens et conserver leur pertinence en tant qu'institution nationale. […] De plus, nos expériences opérationnelles récentes nous démontrent que le fait de compter sur des membres en provenance de différents horizons constitue un élément habilitant qui accroît l'efficacité opérationnelle des FAC. » Selon l'initiative 10 de la PSE, le MDN et les FAC feront la promotion de la diversité et de l'inclusion à titre de valeur primordiale dans l'ensemble de l'Équipe de la Défense.

De tous les répondants au sondage sur les cyberforces, en ce qui concerne les statistiques sur la langue maternelle, 81 pour cent ont indiqué l'anglais, 18 pour cent le français, et 1 pour cent le mandarin. Environ 15 pour cent des répondants ont indiqué une origine ethnique autre que blanche, ce qui illustre un certain degré de diversité dans les cyberforces.

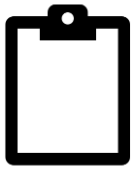
Une conscientisation aux différentes identités devrait être activement intégrée à tous les aspects des cyberforces pour assurer une structure de la force inclusive et diversifiée.

ANNEXE C — MÉTHODOLOGIE D'ÉVALUATION

Sources de données

Les constatations et les recommandations de ce rapport sont le fruit de multiples sources de données recueillies pendant toute la conduite de cette évaluation. Nous avons mis les données en correspondance et nous avons consulté les gestionnaires de programme pour en vérifier la validité. Nous avons utilisé la méthodologie de recherche suivante pour établir la portée de l'évaluation et pour mener l'évaluation en soi :

Examen de la littérature : Dans le cadre de la planification de l'évaluation, nous avons mené un examen préliminaire des documents pour établir une compréhension de base des cyberforces et de l'assurance de la cybermission afin de déterminer la portée de l'évaluation. Cet examen a été élargi pendant la conduite de l'évaluation, lorsque nous examinions d'autres documents pour trouver des données qui aideraient à l'évaluation. Les documents examinés sont : les sites Web du gouvernement, des rapports administratifs des ministères, des documents de programme, en version préliminaire ou finale, et des rapports externes.



Questionnaires courts : Pendant le déroulement de l'évaluation, certains sujets ont été relevés qui devaient être éclaircis ou mieux documentés. Ainsi, nous avons envoyé un certain nombre de questionnaires courts (deux ou trois questions) à des points de contact clés par courriel. Nous avons ainsi contacté les organisations suivantes : DGOGI, SMA(IE), VCEMD et les gestionnaires de carrière des officiers des transmissions et des officiers du génie électronique et des communications.

Études de cas : L'équipe d'évaluation a mené une étude de cas concernant la nécessité de mettre en place un groupe professionnel d'officiers du cyberdomaine. Cette étude a reposé sur les documents militaires, les données du sondage, les notes d'entrevues et les données administratives. D'autres informations concernant l'étude de cas se trouvent dans le rapport.

Entrevues : L'équipe d'évaluation a mené plus de 30 entrevues avec des organisations internes et externes au MDN et aux FAC. Nous avons regroupé les réponses pour établir des opinions et des perspectives en appui à l'évaluation. À moins d'indication contraire, la mention « directeur de programme » réfère uniquement aux personnes dans des postes de directeur ou supérieur dans les organisations du DG Cyber et du DGOGI. Les organisations qui ont participé aux entrevues sont les suivantes :

- SMA(GI)
  - DG Cyber
  - DGOGI
  - GOIFC
  - Directeur – Réalisation de projet (Commandement et contrôle)
  - D Sécur GI
- SMA(S et T)
- SMA(Mat)
- EMIS
- VCEMD
- AC
- MRC
- ARC
- COMFOSCAN
- COMRENSFC
- EECFC

Externe au MDN et aux FAC

- CST
- AICDS

ANNEXE C — MÉTHODOLOGIE D'ÉVALUATION

Sondage :
L'équipe d'évaluation a mené un sondage pendant le mois d'octobre 2019. Certaines questions ciblaient des personnes en particulier, comme des cadres supérieurs, des militaires ou des intervenants des organisations externes au DG Cyber ou au DGOGI du cyberdomaine. Les graphiques dans le rapport reflètent ces nuances dans les populations dans leurs titres. À moins d'indication contraire, par « répondants au sondage » on entend toute la population du sondage.

Dans le but de faire participer une vaste population pour obtenir les opinions, les perspectives et des données relatives à l'ACS+, l'équipe d'évaluation a conçu un sondage en anglais et en français. Certaines questions ont été élaborées pour cibler certains membres de la population, comme les gestionnaires supérieurs, les militaires ou des intervenants du cyberdomaine externe aux cyberforces. Ces nuances sont reflétées dans les graphiques qui illustrent les données dans tout le rapport.

Le sondage a été rempli par des organisations et des personnes ciblées qui travaillent dans le cyberdomaine ou qui ont des liens avec le Programme d'assurance de la cybermission au MDN et dans les FAC. Le sondage a été diffusé d'abord aux points de contact recensés à l'aide d'une recherche dans le répertoire du MDN. Les personnes recensées ont ensuite acheminé le sondage aux autres personnes pertinentes ou subordonnées dans leur chaîne de commandement.

Le sondage est demeuré en ligne pendant environ un mois, et au total, 120 réponses ont été reçues du SMA(GI), du SMA(S & T), du SMA(Mat), du SMA(IE), du JAG, de l'EMIS, du VCEMD, du COMRENSFC, du COIC, du COMFOSCAN et des commandements d'armée (AC, MRC, ARC). À noter, des personnes en poste ont soumis leurs réponses au sondage à l'aide de Microsoft Word, puisqu'elles n'avaient pas accès au RED.

Visites de sites : L'équipe d'évaluation a visité la SFC Leitrim et a mené des entrevues avec cinq personnes qui travaillent au GOIFC, notamment le commandant du GOIFC. En raison des autorisations de sécurité limitées, l'équipe n'a pas pu visiter l'ensemble des installations, mais a reçu des présentations et des exposés des unités du GOIFC sur leur travail.

Établissement de seuils de référence : L'équipe d'évaluation a mené une analyse comparative en établissant des points de comparaison entre les cyberforces du Canada et les cybergroupes militaires des États-Unis, du Royaume-Uni et de l'Australie. À l'aide de divers indicateurs, l'équipe a recueilli des données de diverses sources en ligne, tels que des sites Web du gouvernement pour permettre la comparaison.

Groupes de discussion : L'équipe d'évaluation a mené des groupes de discussion pour recueillir des données de populations cibles dans les secteurs du programme. En particulier, un groupe de discussion a eu lieu avec le Directeur – Ingénierie et intégration (Gestion de l'information).

ANNEXE D — LIMITATIONS DE L'ÉVALUATION

Les limitations vécues dans l'évaluation, et les stratégies d'atténuation employées dans le processus d'évaluation.

	Autorisations de sécurité	Accès au sondage	Programmes nouveaux	Biais dans la sélection des participants	Biais dans les entrevues	Pandémie mondiale
Limitations	La nature des cyberforces fait en sorte que la majorité de leurs activités se déroulent dans un environnement SECRET ou TRÈS SECRET.	Une partie du cyberpersonnel n'a pu accéder de manière électronique au sondage qui a été diffusé, en particulier ceux qui étaient en affectation hors du Canada.	Étant donné la nouveauté des cyberforces, nous avons mené une évaluation formative, et de nombreux documents de fond ont été modifiés pendant le déroulement de l'évaluation.	Un biais pouvait survenir selon la sélection des personnes ou des organisations pour participer au sondage, ce qui pourrait fausser les résultats du sondage.	Un biais peut survenir selon l'impression subjective et les commentaires des personnes interviewées, ce qui pourrait donner lieu à des opinions biaisées.	En raison de l'éclosion de la pandémie de COVID-19 à l'échelle mondiale et au Canada, nous n'avons pas été en mesure de terminer la dernière ronde de mobilisation des intervenants de haut niveau.
Stratégies d'atténuation	Nous avons gardé l'évaluation au niveau sans classification, et avons exclu de la portée les aspects qui ne pouvaient pas respecter ce niveau, comme le contenu relatif au C3IR, tel que décrit dans la portée de l'évaluation.	Après avoir reçu de l'information sur ces difficultés, l'équipe d'évaluation a envoyé le sondage en format Word et a saisi manuellement les réponses à inclure dans l'analyse.	L'équipe d'évaluation a gardé un contact régulier avec les intervenants du programme pour obtenir les versions courantes des documents pertinents.	Nous avons communiqué avec toutes les organisations liées au cyberdomaine aux fins du sondage. Les répondants ont été choisis dans les unités au sein des organisations membres.	Nous avons corroboré les commentaires d'entrevue avec d'autres sources pour en vérifier la validité. Les notes d'entrevues ont été prises par plus d'une personne pour confirmer la compréhension des discussions et diminuer la possibilité d'un biais.	Les membres de l'équipe d'évaluation ont mené la dernière phase du projet à distance.