RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Title - Sujet CD-DAR - ITQ Invitation to Qualify: Cyber Defence – Decision Analysis and Response	
Solicitation No. - N° de l'invitation W6369-20CY06/C	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client W6369-20CY06	**Date** 2021-04-28
GETS Reference No. - N° de référence de SEAG PW-$$QE-049-28197	
File No. - N° de dossier 049qe.W6369-20CY06	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-06-17 Heure Avancée de l'Est HAE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (873) 355-3543 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
See Herein

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

L'AMENDEMENT 001 EST SOULEVÉ POUR:

1. Corriger les erreurs de lien de référence dans l'annexe A, l'EBO et le CONOPS. Les documents corrigés sont joints.

TOUS LES AUTRES TERMES ET CONDITIONS DE CETTE SOLLICITATION RESTENT INCHANGÉS.

Invitation à se qualifier

POUR

CYBERDÉFENSE - DÉCISION, ANALYSE ET RÉPONSE (CD-DAR)

ISQ NO, W6369-20-CY06/C

Table des matières

1. Renseignements généraux

1.1 Introduction

Objectif de la présente invitation à se qualifier (ISQ) : le projet Cyberdéfense – Décision, Analyse et Réponse (CD-DAR) est le regroupement des projets de sensibilisation à la cybersécurité (SC) et de cyberopérations défensives – aide à la décision (CD-AD). L'objectif de cette invitation à se qualifier (ISQ) émise par Services publics et Approvisionnement Canada (SPAC)[1] est de qualifier les fournisseurs qui sont en mesure de fournir une capacité CD-DAR pour entreprendre les étapes ultérieures du processus d'approvisionnement. Un aperçu plus détaillé du processus d'approvisionnement souple et collaboratif figure dans la section 1.3 et l'annexe D.

Le présent processus d'ISQ ne constitue pas une demande de soumissions ni un appel d'offres**.** Aucun contrat ne sera attribué à la suite des activités tenues pendant l'étape de l'ISQ. En tout temps pendant l'étape de l'ISQ, le Canada se réserve le droit d'annuler toute exigence de qualification incluse dans le projet. Étant donné que le Canada peut annuler le processus d'ISQ en totalité ou en partie, le processus d'approvisionnement subséquent décrit dans le présent document peut ne jamais avoir lieu. Les fournisseurs préqualifiés peuvent se retirer du processus d'approvisionnement à tout moment. Par conséquent, les fournisseurs préqualifiés peuvent décider de ne pas soumettre de proposition à une demande de soumission subséquente, quelle qu'elle soit.

1.2 Résumé du projet

1.2.1 **Renseignements généraux :** Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) ont fortement investi dans des technologies qui ont radicalement augmenté la rapidité et la précision des opérations militaires modernes. La plupart de ces progrès incroyables en matière de capacité découlent de la dépendance à un cyberespace de plus en plus complexe. Pour s'acquitter de leurs principales responsabilités de défendre le Canada, de défendre l'Amérique du Nord et de contribuer à la paix et à la sécurité internationales, le MDN et les FAC doivent être une force militaire moderne efficace, agile, adaptée, bien formée et bien équipée, dotée des capacités essentielles et de la souplesse qui sont requises pour contrer les menaces traditionnelles et asymétriques, y compris les cyberattaques.

Le projet CD-DAR s'harmonise aux objectifs de l'initiative no 65 de Protection, Sécurité, Engagement: La politique de défense du Canada, qui cite l'engagement du MDN et des FAC à « améliorer les capacités cryptographiques, les capacités des opérations d'information et les

[1] La dénomination sociale du Ministère est « ministère des Travaux publics et des Services gouvernementaux ». « Services publics et Approvisionnement Canada » et « SPAC », de même que « Travaux publics et Services gouvernementaux Canada » et « TPSGC » sont les appellations usuelles.

cybercapacités, ce qui inclura des projets de cybersécurité et de connaissance de la situation, l'identification des cybermenaces et la réponse à celles-ci, ainsi que le développement de capacités pour mener des opérations d'information et des cyberopérations offensives militaires dans le but de cibler, d'exploiter, d'influencer et d'attaquer à l'appui des opérations militaires ».[2]

À l'appui de leur structure de commandement et de contrôle, le MDN et les FAC ont besoin de pouvoir surveiller et contrôler leur cyberespace afin qu'il reste défendable. À cette fin, le projet CD-DAR du programme de développement de la cyberforce du MDN et des FAC se concentre sur l'application de ces exigences. Le projet CD-DAR est l'unique résultat du regroupement des projets de SC et de CD-AD.

1.2.2 **Résumé du projet :** Au moyen du projet CD-DAR, le MND et les FAC acquerront une solution de cyberdéfense (qui se traduit en capacités) dans le but d'améliorer l'aide à la décision en général et la sécurité du cyberespace du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'y réagir. La capacité intégrée du projet CD-DAR doit fournir une analyse contextuelle fiable à l'appui des décisions et des mesures du MDN et des FAC à l'intérieur d'extensions et d'interfaces désignées du réseau de commandement ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables. En fin de compte, la capacité du projet CD-DAR permettra à la cyberforce des FAC de défendre la liberté d'action et les intérêts des FAC dans le cyberespace à l'appui des missions et des opérations des FAC. Néanmoins, le projet CD-DAR doit être conçu pour permettre l'évolutivité vers d'autres environnements de réseau, selon les besoins.

Le projet est entré dans la phase de définition en juin 2020.

On trouve d'autres renseignements sur les exigences, les objectifs, les résultats et la portée du projet à la fin de ce document, dans l'ébauche de l'énoncé des besoins opérationnels (EBO) et dans l'ébauche du concept des opérations (CONOPS) qui y sont joints.1.2.3

Portée du processus d'approvisionnement prévu :

i) **Clients potentiels :** La présente ISQ est publiée par SPAC. Il est prévu que le MDN utilise le ou les contrats résultant de toute demande de soumissions subséquente pour satisfaire aux exigences du projet CD-DAR. Le contrat ou certains éléments du contrat peuvent être utilisés pour répondre à des besoins additionnels ou similaires au MDN.

ii) **Utilisation des ressources du MDN :** D'autres ressources du MDN/des FAC, d'autres ministères ou du Groupe des cinq (Gp5) et d'autres documents d'achats existants ou nouveaux pourraient être utilisés au fil de l'évolution du projet.

iii) **Nombre de contrats :** SPAC envisage actuellement d'attribuer au moins un (1) contrat.

[2] Initiative nº 65 de Protection, Sécurité, Engagement : La politique de défense du Canada.

iv) **Durée du contrat :** SPAC détermine la durée de tout contrat subséquent et des options connexes une fois que l'approvisionnement progresse jusqu'à la phase de la demande de propositions (DP). Le Canada a l'intention d'adopter une approche itérative et graduelle pour la mise en oeuvre.

v) **Soutien en service :** Le Canada demande aux soumissionnaires de répondre aux questions sur le soutien en service (SES) présentées à l'annexe E, pour l'aider à déterminer ses options contractuelles de SES au début du processus d'approvisionnement. *Remarque : Les réponses à ces questions ne font pas partie des exigences de la présente ISQ.*

1.2.4 **Programme des marchandises contrôlées :** Ce marché est assujetti au Programme des marchandises contrôlées. La *Loi sur la production de défense* définit les marchandises canadiennes contrôlées comme étant certains biens énumérés dans la Liste des marchandises d'exportation contrôlée du Canada, un règlement établi en vertu de la *Loi sur les licences d'exportation et d'importation* (LLEI). Avant d'obtenir l'accès, l'entrepreneur doit être inscrit au Programme des marchandises contrôlées de Travaux publics et Services gouvernementaux Canada (TPSGC).

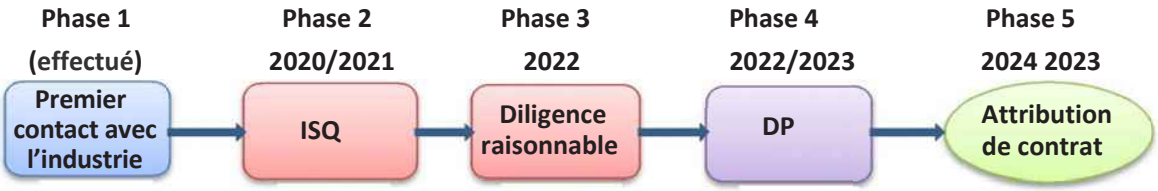
1.2.5 **Participation, contrôle et influence de l'étranger (PCIE) :** Une évaluation de PCIE sera requise avant l'attribution du contrat. Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la PCIE ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut accéder, sans en avoir l'autorisation, à des biens ou à des renseignements SECOM ou classifiés ÉTRANGERS ou DE L'OTAN.

1.2.6 **Capacité financière :** La clause A9033T (2012-07-16) du Guide des clauses et conditions uniformisées d'achat (CCUA), Capacité financière, s'appliquera à la DP.

1.3 Résumé du processus d'approvisionnement prévu

La présente ISQ constitue la deuxième étape du processus d'approvisionnement du projet. Bien que le processus d'approvisionnement puisse être modifié (et même annulé, conformément aux instructions uniformisées de TPSGC), le Canada prévoit actuellement entreprendre le processus d'approvisionnement agile et collaboratif en plusieurs phases décrites ci-dessous.

CD-DAR - Processus d'approvisionnement prévu



Les activités par phase comprennent:

LOI	**Ébauche de l'ISQ**	**Ébauche de la DP**	**DP**
RFI	**ISQ officielle**	**Conférence des soumissionnaire**	
Journée de l'industrie			
Réunions individuelles		**Réunions individuelles**	

1.3.1 Phase 1 – Premier contact avec l'industrie (effectué)

SPAC et le MDN ont commencé leurs efforts de sollicitation de l'industrie en publiant des lettres d'intérêt (LI) pour les projets de CD-AD et de SC en 2016, puis une demande de renseignements (DDR) en 2017. Une journée de l'industrie et des réunions individuelles classifiées ont eu lieu au printemps 2018. Cela a été fait dans le but d'obtenir une rétroaction sur les exigences opérationnelles et techniques, les coûts et le calendrier, et les retombées industrielles et technologiques. La rétroaction des fournisseurs découlant de ces efforts de sollicitation de l'industrie a été d'une grande utilité pour le Canada et a permis au MDN et aux FAC d'aller de l'avant avec le projet CD-DAR.

1.3.2 Phase 2 – Phase d'invitation à se qualifier

Ébauche de l'ISQ : L'ébauche de l'ISQ était le début de la deuxième phase de l'approvisionnement pour le projet CD-DAR. Les fournisseurs ont été invités à soumettre des questions et des commentaires écrits sur l'ébauche de l'ISQ. Les questions et réponses seront affichées sur le site Achats et ventes.

ISQ officielle : L'ISQ servira à préqualifier les fournisseurs pour qu'ils puissent participer aux phases subséquentes de diligence raisonnable et de la DP et à toute autre phase potentielle du processus d'approvisionnement. Les fournisseurs sont invités à se soumettre à une sélection préalable, conformément aux modalités de la présente ISQ. Seuls les fournisseurs préqualifiés seront autorisés à soumissionner lors d'une demande de soumissions subséquente publiée dans le cadre du processus d'approvisionnement.

1.3.3 Phase 3 – Diligence raisonnable

SPAC ne mènera la phase de diligence raisonnable qu'avec les fournisseurs préqualifiés, comme déterminé dans la phase de qualification (Phase 2 – Phase d'invitation à se qualifier). L'objectif de la phase de diligence raisonnable est d'améliorer davantage les exigences du projet CD-DAR en

obtenant des commentaires de la part de fournisseurs préqualifiés, en répondant aux préoccupations de l'industrie et en tenant compte des pratiques exemplaires de l'industrie avant de lancer la demande de soumissions finale. Les activités de la phase de diligence raisonnable sont les suivantes :

Ébauche de la DP : On s'attend à ce que les fournisseurs préqualifiés soient prêts à fournir de la rétroaction sur l'ébauche des documents de la DP, y compris les renseignements sur le système, l'ébauche de l'énoncé des besoins et l'ébauche des critères d'évaluation. Les éléments de l'ébauche de la DP sont classifiés et ne sont accessibles qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité de la DP décrites à l'annexe B. Les fournisseurs préqualifiés qui ne satisfont pas aux exigences de sécurité n'auront accès qu'aux éléments non classifiés de l'ébauche de la DP. Dans la mesure du possible, tout en préservant la sécurité nationale, les éléments non classifiés de l'ébauche de demande de propositions seront publiés sur Achats et ventes pour permettre aux fournisseurs non qualifiés de fournir une rétroaction. Le Canada examine et répond à ces commentaires lorsque cela est possible et publie les résultats sur le site Achats et ventes.

Conférence des soumissionnaires classifiée et réunions individuelles classifiées avec des fournisseurs préqualifiés : Une conférence des soumissionnaires et des réunions individuelles avec des fournisseurs préqualifiés sont organisées pour discuter de questions précises concernant le contenu de l'ébauche des documents de la DP. De plus amples détails concernant la phase de diligence raisonnable sont fournis aux fournisseurs préqualifiés dans le cadre du processus de l'ébauche de la DP. Enfin, la finalisation de la DP tient compte de l'examen de la rétroaction de l'industrie après le processus de l'ébauche de la DP. La participation à la conférence des soumissionnaires classifiée et à la réunion individuelle classifiée n'est offerte qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité de la DP décrites à l'annexe B.

1.3.4 Phase 4 – Demande de propositions (DP)

SPAC prévoit publier une DP à l'intention des fournisseurs préqualifiés qui demeurent qualifiés au moment de la publication de la DP et qui satisfont aux exigences de sécurité de la DP décrites à l'annexe B. Si un fournisseur ne satisfait pas aux exigences de sécurité de la DP à la date d'émission de la DP, il sera retiré de la liste des fournisseurs préqualifiés. Dans la mesure du possible, tout en préservant la sécurité nationale, les éléments non classifiés de la demande de propositions seront publiés sur Achats et ventes pour informer les fournisseurs non qualifiés. Dans la mesure du possible, le Canada examine et répond aux commentaires des fournisseurs non qualifiés et publie les résultats sur le site Achats et ventes.

1.3.5 Phase 5 – Attribution du marché

SPAC prévoit attribuer un contrat au fournisseur retenu conformément aux modalités de la DP.

1.4 Compte rendu

L'autorité contractante avisera les fournisseurs non retenus après la phase de préqualification et leur fournira un compte rendu sur demande. Les fournisseurs non retenus devraient en faire la demande à l'autorité contractante dans les 15 jours ouvrables suivant la réception des résultats du processus de qualification. Le compte rendu peut être fourni par écrit, par téléphone ou en personne. L'autorité contractante doit déterminer quelle méthode sera la plus efficace.

1.5 Exceptions relatives à la sécurité nationale

Les exceptions relatives à la sécurité nationale prévues dans les accords commerciaux ont été invoquées; ce marché est donc entièrement exclu de l'ensemble des modalités de tous les accords commerciaux.

1.6 Politique des retombées industrielles et technologiques (RIT)

La **Politique des retombées industrielles et technologiques (RIT)** s'appliquera au projet Cyberdéfense – Analyse des décisions et réponse (CD-ADR). En vertu de la Politique des RIT, les entreprises qui se voient attribuer des contrats d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada, dont la valeur équivaut à celle du contrat. La Politique des RIT comprend une proposition de valeur (PV) qui exige des soumissionnaires qu'ils se fassent concurrence sur la base des retombées économiques pour le Canada associées à chaque soumission. Les répondants retenus sont sélectionnés en fonction du prix, du mérite technique et de leur PV. Les engagements relatifs à la PV pris par le soumissionnaire retenu deviennent des obligations contractuelles dans le contrat subséquent. Afin d'optimiser l'impact économique qui peut être obtenu de la PV, le Canada cherchera à utiliser la Politique des RIT pour motiver les entrepreneurs à investir dans les Capacités industrielles clés (CIC), telles que la cyberrésilience et l'intelligence artificielle. En tant que technologies émergentes, ces CIC sont des domaines présentant un potentiel de croissance rapide et d'innovation. Par conséquent, le Canada cherchera à favoriser les débouchés dans ces technologies émergentes en motivant les partenariats et les investissements avec l'industrie et les établissements postsecondaires qui favorisent le développement des compétences et la recherche et le développement.

Le Canada collaborera avec des fournisseurs qualifiés à mesure que nous élaborerons les exigences de la proposition de valeur des RIT.

Pour de plus amples renseignements sur la Politique des RIT, y compris la PV, visitez la page http://www.canada.ca/rit.

1.7 Experts-conseils

1.7.1 Le Canada peut retenir les services d'experts-conseils dans le futur, à sa seule discrétion, pour les besoins du projet CD-DAR.

1.7.2 Le Canada transmettra aux experts-conseils, selon le besoin de savoir, les renseignements et les

documents qui lui seront fournis, y compris ceux des fournisseurs préqualifiés, dans le cadre du processus d'approvisionnement.

1.7.3 Les experts-conseils sont tenus de signer un ou des accords de non-divulgation avant d'accéder à l'information et aux documents sur le Projet dans le cadre du présent processus d'approvisionnement.

1.8 Conflit d'intérêts ou avantage indu

Conformément aux dispositions des Instructions uniformisées – Biens ou services – Besoins concurrentiels 2003 (2020-05-28), une réponse peut être rejetée en raison d'un conflit d'intérêts réel ou apparent ou d'un avantage indu.

À cet égard, le Canada indique qu'il a eu recours aux services d'un certain nombre d'entrepreneurs du secteur privé dans la préparation des stratégies et des documents se rapportant à ce processus d'approvisionnement, y compris ceux qui suivent :

Entrepreneurs :

i. Modis Canada;
ii. Veritaaq; and
iii. Procom.

Ressources (passé et présent) :

i. Marc Lessard;
ii. Paris Lampsos;
iii. Maurice Tremblay;
iv. Peter Ng;
v. Stuart Morrison; et
vi. Bethany Allen.

1.9 Surveillant de l'équité

Canada a fait appel aux services de *The Public Sector Company* comme surveillant de l'équité dans le cadre de cette acquisition. Le surveillant de l'équité observera, par exemple, l'évaluation des réponses afin de déterminer si SPAC a respecté le processus d'évaluation décrit dans la demande de soumissions. Selon son contrat avec le gouvernement du Canada, le surveillant de l'équité a l'obligation de préserver la confidentialité de tous les renseignements reçus dans le cadre de sa participation au présent processus d'approvisionnement.

2. Instructions à l'intention des fournisseurs

2.1 Instructions, clauses et conditions uniformisées

2.1.1 Toutes les instructions, clauses et conditions définies par un numéro, une date et un titre dans l'ISQ sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditionsuniformisees-d-achat) publié par TPSGC.

2.1.2 Les fournisseurs qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la présente ISQ.

2.1.3 Le document 2003 (2020-05-28), Instructions uniformisées – Biens ou services – Besoins concurrentiels, est intégré par renvoi à l'ISQ et en fait partie intégrante, sauf dans les cas suivants :

i) Chaque fois que le terme « demande de soumissions » est employé, il est remplacé par « invitation à se qualifier »;

ii) Chaque fois que le terme « soumission » est employé, il est remplacé par « réponse »;

iii) Chaque fois que le terme « soumissionnaire(s) » est employé, il est remplacé par « répondant(s) »;

2.1.4 La sous-section 5(4), qui traite de la période de validité, ne s'applique pas étant donné que l'ISQ invite les fournisseurs à se qualifier. À moins que le fournisseur n'informe l'autorité contractante de son désir de retirer sa réponse, le Canada supposera qu'il tient toujours à se qualifier.

2.1.5 Supprimer le paragraphe 01 – Dispositions relatives à l'intégrité – soumissions;

2.1.6 Supprimer le paragraphe 14 – Justification des prix;

2.1.7 Lorsqu'il soumet une réponse, le répondant s'engage à respecter les instructions, les clauses et les conditions de la présente ISQ.

2.1.8 Le processus de conformité des soumissions par étapes s'applique à ce besoin.

2.2 Terminologie pour la constitution de l'équipe

Les termes suivants sont définis afin d'aider les répondants à organiser leur équipe en réponse à la présente ISQ :

2.2.1 « Association d'entités » désigne des entités juridiques distinctes au sein d'un réseau de services professionnels officiellement organisé dont tous les membres fonctionnent en utilisant une image

de marque commune. L'accès à la propriété intellectuelle et aux ressources de talent doit être partagé et la technologie, la méthodologie, les stratégies et les politiques doivent être intégrées à l'échelle du réseau. Elle ne comprend pas les affiliés non apparentés au répondant avec qui celui-ci collabore en partenariat par l'intermédiaire de l'équipe de base du répondant ou d'une coentreprise (selon le cas).

2.2.2 « Entité » signifie un particulier, une compagnie constituée en personne morale, un partenariat, une société, une coentreprise, un syndicat, une association, une fiducie ou autre forme d'entité juridique.

2.2.3 « Coentreprise » désigne, collectivement, les participants à la coentreprise qui composent le répondant.

2.2.4 « Participant à la coentreprise » désigne une entité qui a conclu une entente avec une ou plusieurs autres entités, soit par contrat, soit en formant une nouvelle entité, afin de combiner des fonds, des biens, des connaissances, de l'expertise ou d'autres ressources dans une entreprise commune.

2.2.5 « Répondant principal » désigne le membre de l'équipe de base qui deviendra l'entrepreneur si le répondant est choisi comme entrepreneur à n'importe quelle étape du processus d'approvisionnement.

2.2.6 « Répondant » désigne l'entité, le répondant principal et les membres de son équipe de base ou la coentreprise qui soumet une réponse à la présente ISQ.

2.2.7 « Représentant du répondant » désigne la personne qui a été autorisée par le répondant à le représenter et à le lier, y compris tous les membres de l'équipe de base et les participants à la coentreprise qui composent le répondant.

2.2.8 « Équipe de base du répondant » désigne, collectivement, le répondant principal et les membres de l'équipe de base constituant le répondant.

2.2.9 « Membre de l'équipe » désigne chaque entité qui est membre de l'équipe de base du répondant.

2.2.10 « Fournisseur qualifié et fournisseur préqualifié » désigne un répondant qui a été sélectionné par le Canada en vertu de la présente ISQ.

2.3 Présentation d'une seule réponse

2.3.1 Une réponse peut être présentée par :

i) une seule entité en tant que répondant;
ii) un répondant principal et les membres de son équipe de base en tant que répondant;
iii) une coentreprise en tant que répondant.

2.3.2 Aux fins de la présente ISQ seulement, les répondants ne sont pas tenus de créer une entité juridique pour soumettre une réponse à titre d'équipe de base du répondant ou de coentreprise, mais le Canada prévoit que cela sera nécessaire avant de répondre aux demandes de soumissions subséquentes.

2.3.3 Le Canada exige que chaque réponse, à la date de clôture de la présente ISQ ou à la demande de l'autorité contractante, soit signée par le représentant du répondant, tous les membres de l'équipe de base ou les membres de la coentreprise, selon le cas. Le Canada exige que les signatures soient présentées dans le formulaire de présentation de réponse contenu à l'annexe C. Les répondants qui présentent une réponse conviennent de respecter les instructions, les clauses et les conditions de la présente ISQ

2.3.4 Chaque répondant (y compris les entités apparentées) ne pourra se qualifier qu'une seule fois. Si un répondant ou une entité apparentée participe à plusieurs réponses (participer signifie faire partie du répondant, et non pas être un sous-traitant), le gouvernement du Canada accordera deux (2) jours ouvrables à ces répondants pour indiquer la réponse unique que le gouvernement du Canada devra examiner. Si ce délai n'est pas respecté, toutes les réponses concernées pourraient être déclarées irrecevables ou le gouvernement du Canada pourrait choisir, à sa discrétion, les réponses qu'il évaluera.

2.3.5 Pour l'application du présent article, sans égard à la compétence où elle a été constituée en société ou formée juridiquement (qu'il s'agisse d'une personne, d'une société, d'une société de personnes, etc.), toute entité sera considérée comme « entité apparentée » d'un répondant :

i) s'il s'agit de la même personne morale que le répondant (c.-à-d. la même personne physique, société commerciale, société de personne, société à responsabilité limitée, etc.);

ii) si l'entité et le répondant sont des « personnes liées » ou des « personnes affiliées » aux termes de la Loi de l'impôt sur le revenu du Canada;

iii) si l'entité et le répondant entretiennent une relation fiduciaire (découlant d'un arrangement entre agences ou toute autre forme de relation fiduciaire) ou ont entretenu une telle relation au cours des deux dernières années ayant précédé la clôture de l'ISQ;

iv) si l'entité et le répondant ont tout autre lien de dépendance entre eux, ou avec le même tiers.

2.3.6 Toute personne, entreprise individuelle, société, ou tout partenariat qui est un répondant, un membre d'une équipe de base du répondant ou d'une coentreprise ne peut soumettre une autre

réponse de son propre chef ou sous l'égide d'une autre équipe de base du répondant ou une autre coentreprise.

Exemple 1 : Le fournisseur A, à lui seul, ne possède pas toute l'expérience requise par l'ISQ. Toutefois, le fournisseur B possède l'expérience qui manque au fournisseur A. Si les fournisseurs A et B décident de s'associer pour soumettre une réponse ensemble en tant que coentreprise, les deux entités seront considérées, ensemble, en tant que répondant. Les fournisseurs A et B ne peuvent pas s'associer avec un autre fournisseur pour soumettre une réponse distincte, parce qu'ils se sont associés pour former une coentreprise.

Exemple 2 : Le fournisseur X est un répondant. La filiale du fournisseur X, le fournisseur Y, décide de s'associer au fournisseur Z pour soumettre une réponse en tant que coentreprise. Les fournisseurs Y et Z, tout comme le fournisseur X, seront tous appelés à déterminer laquelle des deux réponses devra être prise en considération par le gouvernement du Canada. Les deux réponses ne peuvent pas être soumises, parce que le fournisseur Y est lié au fournisseur X en tant que société affiliée.

2.3.7 En soumettant une réponse, le répondant atteste qu'il ne se considère pas comme lié à tout autre répondant.

2.3.8 **Représentant du répondant :** Le représentant du répondant doit être nommé, et identifié par son nom dans la réponse, pour fournir des documents et des renseignements à l'autorité contractante et pour recevoir des instructions et des avis au nom du répondant ou de tout membre de l'équipe de base ou participant de la coentreprise, le cas échéant.

2.4 Lois applicables

L'ISQ sera interprétée et régie selon les lois en vigueur dans la province de l'Ontario, au Canada, et les relations entre les parties seront aussi régies par ces lois.

À leur discrétion, les répondants peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les répondants acceptent les lois applicables indiquées.

2.5 Questions, commentaires et communications

2.5.1 **Personne-ressource unique :** Afin d'assurer l'intégrité du processus d'approvisionnement concurrentiel, toutes les questions et autres communications ayant trait à l'ISQ doivent être adressées uniquement à l'autorité contractante.

Autorité contractante

Services publics et Approvisionnement Canada
Patti Wight / Laurie Stewart

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

2.5.2 **Date limite de soumission de questions :** À moins d'indication contraire dans l'ISQ, toutes les questions et observations à son sujet doivent être soumises par courriel à l'autorité contractante au plus tard dix jours avant la date de clôture. Les questions reçues après cette date pourraient ne pas recevoir de réponse.

2.5.3 **Contenu des questions :** Les répondants doivent citer le plus fidèlement possible le numéro de l'article de l'ISQ auquel se rapporte la question. Ils doivent prendre soin d'énoncer chaque question de manière suffisamment détaillée pour permettre au gouvernement du Canada de fournir une réponse. Toute question qui comporte selon le répondant des renseignements exclusifs doit afficher clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments affichant la mention « exclusif » feront l'objet d'une discrétion absolue, à moins que le gouvernement du Canada considère que la question n'a pas un caractère exclusif. Le Canada peut modifier les questions ou peut demander au répondant de le faire, afin d'en éliminer le caractère exclusif et de permettre la transmission de la question modifiée et de la réponse à l'ensemble des répondants. Le gouvernement du Canada peut ne pas répondre aux questions dont la formulation ne permet pas de les transmettre à tous les répondants.

2.5.4 **Publication des réponses :** Pour garantir l'uniformité et la qualité des renseignements communiqués aux soumissionnaires, les questions importantes ainsi que les réponses seront publiées dans le Service électronique d'appels d'offres du gouvernement sous forme de modification à l'ISQ.

2.6 Droits du gouvernement du Canada

En plus de tout autre droit décrit dans l'ISQ, le gouvernement du Canada a le droit :

a) de modifier en tout temps la présente ISQ, y compris les critères de qualification;

b) d'annuler l'ISQ à n'importe quel moment;

c) de produire à nouveau l'ISQ;

d) si aucun répondant n'est qualifié et qu'aucune modification majeure n'a été apportée au besoin, de publier de nouveau la demande de soumissions en invitant uniquement les répondants qui ont soumissionné à soumissionner de nouveau, dans un délai indiqué par le gouvernement du Canada;

e) de rejeter et de ne pas examiner une réponse davantage si, à son avis, l'une des composantes de la réponse présente des questions ou des problèmes potentiels, perçus ou réels qui pourraient nuire à la sécurité nationale du Canada;

f) d'éliminer en tout temps tout répondant qualifié s'il présente des problèmes potentiels, perçus ou réels qui pourraient porter atteinte à la sécurité nationale du Canada;

g) à tout moment pendant la phase 3 – Diligence raisonnable, d'interrompre la phase 3 et de rouvrir la phase 2 – Phase d'ISQ.

2.7 Exigences en matière de sécurité

Au fur et à mesure que le projet CD-DAR progresse au cours des différentes phases d'approvisionnement, les exigences de sécurité évoluent et augmentent de beaucoup.

2.7.1 Le répondant n'est pas tenu d'avoir une autorisation de sécurité pour devenir un fournisseur préqualifié, mais des autorisations de sécurité et d'autres exigences de sécurité sont requises aux prochaines étapes du processus d'approvisionnement.

2.7.2 Afin d'être invités à la conférence des soumissionnaires (qui est le début de la phase de diligence raisonnable) et aux réunions individuelles classifiées, les fournisseurs préqualifiés doivent satisfaire aux exigences de sécurité décrites à l'annexe B, section 1.2 Exigences en matière de sécurité relatives à la phase 3 – Diligence raisonnable.

2.7.3 Lorsque le Canada est prêt à inviter des fournisseurs préqualifiés à la conférence des soumissionnaires et à une réunion individuelle classifiée (dates à déterminer), l'autorité contractante de SPAC communiquera avec le Programme de sécurité industrielle pour vérifier les autorisations de chaque fournisseur préqualifié. Les fournisseurs préqualifiés qui ne détiennent pas les autorisations appropriées à ce moment-là seront avisés qu'ils ne peuvent pas participer.

2.7.4 Il y aura des exigences de sécurité supplémentaires pour la DP définitive et le contrat. Les exigences de sécurité prévues pour la DP finale et le contrat sont également décrites à l'annexe B. Les fournisseurs préqualifiés qui ne satisfont pas aux exigences de sécurité pour la DP définitive, telles qu'elles sont décrites à l'annexe B, section 1.2, à la date de publication de la DP finale, seront retirés de la liste des fournisseurs préqualifiés.

2.7.5 Les fournisseurs préqualifiés qui ne détiennent pas actuellement les attestations de sécurité du personnel et les attestations de sécurité de l'organisation auprès du gouvernement fédéral canadien ou de leur programme national de sécurité industrielle respectif, ou encore, les fournisseurs qui ne respectent pas les exigences relatives à la sécurité prévues qui sont décrites à l'annexe B, doivent entreprendre tôt le processus d'obtention de l'attestation de sécurité en communiquant avec les responsables du Programme de la sécurité industrielle indiqué sur le site Web de TPSGC (https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html).

3. Préparation et présentation de la réponse

3.1 Langue pour les communications à venir

Dans le formulaire de présentation de la réponse, chaque répondant doit indiquer dans laquelle des langues officielles du gouvernement du Canada il souhaite recevoir des communications futures de SPC à l'égard de son ISQ et tout au long du processus d'approvisionnement.

Si tous les fournisseurs admissibles aux termes de la présente ISQ choisissent la même langue officielle, le Canada peut décider de mener les prochaines étapes de communication et d'approvisionnement avec ces fournisseurs préqualifiés uniquement dans cette langue officielle.

3.2 Contenu de la réponse

Une réponse complète à la présente ISQ comprend tous les éléments décrits ci-après:

i. **Formulaire de présentation de la réponse (demandé à la clôture de l'ISQ)**

Les répondants doivent inclure dans leur réponse le formulaire de présentation de la réponse (Annexe C). Il s'agit d'un formulaire courant dans lequel les répondants peuvent fournir les renseignements exigés dans le cadre de l'évaluation, comme le nom d'une personne-ressource, le numéro d'entreprise – approvisionnement du répondant, la langue à utiliser lors des futures communications avec le gouvernement du Canada au sujet de ce processus d'approvisionnement, etc. L'utilisation de ce formulaire pour présenter les renseignements susmentionnés n'est pas obligatoire, mais recommandée. Si le gouvernement du Canada détermine que les renseignements exigés dans le formulaire de présentation de la réponse sont incomplets ou qu'ils doivent être corrigés, il accordera au répondant la possibilité de les compléter ou de les corriger. Il est obligatoire de fournir les informations du formulaire de présentation de la réponse lorsque demandé pendant la période d'évaluation.

ii. **Réponses aux exigences de qualification de l'annexe A – Critères d'évaluation obligatoires (obligatoire à la clôture de l'ISQ)**

La réponse obligatoire du fournisseur doit justifier sa conformité aux critères obligatoires et cotés qui font l'objet d'une évaluation à l'annexe A – Critères d'évaluation obligatoires, et traiter ces critères de façon claire et suffisamment approfondie. Chaque critère d'évaluation obligatoire et cotés doit être traité avec suffisamment de détails pour permettre à l'équipe d'évaluation de vérifier la conformité du fournisseur. Il ne suffit pas de reprendre simplement les énoncés contenus dans l'ISQ.

Afin de faciliter l'évaluation de la réponse, le gouvernement du Canada exige que les fournisseurs abordent et présentent les sujets dans le même ordre que les critères d'évaluation

et sous le même titre. Pour éviter les recoupements, les répondants peuvent faire référence aux différentes sections de leur réponse en précisant l'article et le numéro de page où le sujet visé est déjà traité.

Remarque : Les répondants sont avisés de ne pas inclure dans leur soumission des renseignements classifiés ou des renseignements distincts qui, une fois regroupés, deviennent classifiés.

3.3 Équipe de base du répondant

3.3.1 Le répondant doit nommer tous les membres de son équipe de base dans sa soumission technique.

3.3.2 À moins d'indication contraire dans les critères d'évaluation techniques, le répondant doit, dans la réponse de l'équipe de base du répondant, présenter les renseignements relatifs au répondant ou aux membres de l'équipe de base du répondant qui démontrent la façon dont ils satisfont aux critères d'évaluation techniques. Le répondant est tenu de préciser le membre de l'équipe de base du répondant auquel il fait référence dans sa réponse à chaque critère.

3.3.3 Seules les compétences et l'expérience de l'équipe de base du répondant seront prises en compte lors de l'évaluation de la réponse à la présente ISQ. Les compétences et l'expérience des sous traitants ne seront pas prises en compte à moins que les sous traitants ne soient membres de l'équipe du répondant, de la façon décrite ci-après.

3.4 Évaluation et équipe de base du répondant

3.4.1 Sauf si la présente ITQ indique clairement le contraire, un répondant peut répondre aux critères d'évaluation techniques lui-même et soumissionner en tant que société ou autre entité juridique unique, ou peut satisfaire aux critères d'évaluation techniques en tant qu'équipe de base du répondant, si le répondant principal et le reste de l'équipe de base du répondant répondent ensemble aux critères d'évaluation techniques.

3.4.2 Le répondant peut se fonder sur l'expérience de l'un des membres de son équipe de base pour satisfaire à tout critère d'évaluation technique de la présente ISQ, à moins d'indication contraire dans les critères d'évaluation techniques.

Exemple : Un répondant a une équipe de base composée de X, Y et Z. Si, dans la demande de soumissions, on exige que : a) que le répondant ait trois années d'expérience dans la prestation des services de maintenance; et b) que le répondant ait deux années d'expérience dans l'intégration de matériel dans des systèmes complexes, chacune de ces deux exigences peut alors être satisfaite par un membre différent de l'équipe de base. Cependant, pour un critère d'évaluation technique donné, comme l'exigence relative aux trois ans d'expérience en prestation de services de maintenance, le répondant ne peut pas indiquer que chaque membre de l'équipe de

base, soit X, Y et Z, possède un an d'expérience pour un total de trois ans. Cette réponse serait jugée irrecevable. Les membres de l'équipe de base ne peuvent pas mettre en commun leur expérience entre eux ou avec le soumissionnaire pour répondre à un critère d'évaluation technique de cette demande de soumissions.

Les répondants qui ont des questions concernant l'évaluation des soumissions d'une équipe de base pourront poser leurs questions dans le cadre du processus de demande de renseignements, dès que possible durant la période de demande de soumissions de l'ISQ.

3.5 Composition de l'équipe de base

3.5.1 Seul un répondant préqualifié lors de la phase de l'ISQ obtiendra le statut de fournisseur préqualifié et pourra soumissionner aux demandes subséquentes.

3.5.2 Les répondants qui obtiennent le statut de fournisseurs préqualifiés sont avisés que toute modification à leur nom, à leur structure organisationnelle ou à leur statut juridique, toute restructuration organisationnelle ou toute vente ou tout autre transfert d'actifs après la date de qualification de la présente ISQ pourrait entraîner la perte de leurs droits de soumission, y compris la perte des droits de soumission comme coentreprise.

3.5.3 Les modifications décrites ci-dessus, y compris l'incapacité de maintenir l'équipe de base du répondant pendant toute la durée du processus d'approvisionnement (sauf en cas d'approbation écrite de l'autorité contractante), pourront, à la discrétion du Canada, rendre le répondant inadmissible à continuer à participer au projet de CD-DAR

3.6 Modifications à l'équipe de base du répondant

3.6.1 Comme mentionné précédemment, le répondant doit identifier chaque membre de son équipe de base dans sa soumission technique. L'équipe de base du répondant doit demeurer la même que celle identifiée dans la réponse de la présente ISQ tout au long du processus d'approvisionnement.

3.6.2 S'il ne maintient pas l'équipe de base pendant toute la durée du processus d'approvisionnement (sauf en cas d'approbation écrite de l'autorité contractante), le répondant pourra, à la discrétion du Canada, devenir inadmissible à continuer à participer au processus d'approvisionnement du projet de CD-DAR.

3.7 Présentation électronique d'une réponse

Les soumissions doivent être présentées uniquement au Module de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) au plus tard à la date et à l'heure indiquées à la page 1 de l'ISQ.

En raison de la pandémie de COVID-19, les soumissions transmises à TPSGC par télécopie ou par tout autre service que Connexion postel ne seront pas acceptées.

Les soumissionnaires doivent présenter leur demande à l'Unité de réception des soumissions dans la région de la capitale nationale (RCN) par l'intermédiaire de Connexion postel. L'adresse courriel est la suivante :

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Il incombe au soumissionnaire de s'assurer que la demande d'ouverture d'une conversation Connexion postel est envoyée à l'adresse électronique ci-dessus au moins six jours civils avant la date de clôture de l'ISQ.

Remarque : les soumissions envoyées directement à cette adresse courriel ne seront pas acceptées. Cette adresse de courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'indiqué dans les instructions uniformisées 2003 ou pour envoyer des soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

Le répondant doit présenter sa soumission conformément à l'article 08 des instructions uniformisées de 2003. Le répondant doit transmettre sa soumission dans un seul envoi. Le service Connexion postel a la capacité de recevoir plusieurs documents, jusqu'à 1 Go par pièce jointe individuelle.

4. Processus d'évaluation des réponses

4.1 Évaluation des qualifications du répondant

Le gouvernement du Canada évaluera chacune des réponses afin de déterminer si elles satisfont à toutes les exigences obligatoires décrites dans la présente ISQ. Les dispositions relatives à l'évaluation comprises dans les Instructions uniformisées - biens ou services - besoins concurrentiels 2003 (2020-05-28) de TPSGC s'appliquent également. La réponse doit respecter toutes les exigences de l'ISQ pour être déclarée conforme.

4.2 Procédures d'évaluation

4.2.1 **Évaluation des réponses :** les réponses seront évaluées conformément aux exigences décrites dans la présente ISQ, y compris les exigences de qualification obligatoires de l'annexe A – Critères d'évaluation obligatoires.

4.2.2 **Équipe d'évaluation :** Les réponses seront évaluées par une équipe d'évaluation constituée de représentants du Canada. L'État peut faire appel à des experts-conseils ou à des personnes-ressources du gouvernement pour évaluer les réponses. Chaque membre de l'équipe chargée de l'évaluation ne participera pas nécessairement à tous les aspects de l'évaluation

4.2.3 D**emandes de précisions :** Si le Canada demande des précisions concernant une réponse ou s'il veut vérifier celle-ci, y compris les attestations, les répondants disposeront d'un délai de sept jours ouvrables (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir les renseignements nécessaires au Canada. Selon la nature de la demande, le non-respect de ce délai peut entraîner le rejet de la réponse.

4.2.4 Pr**olongation de délai :** Si le répondant a besoin de plus de temps, l'autorité contractante, à sa discrétion, peut accorder une prolongation du délai.

4.3 Processus de conformité des soumissions en phase (PCSP)

(2018-07-19) Généralités

(a) Pour ce besoin, le Canada applique le PCSP tel que décrit ci-dessous.

(b) Nonobstant tout examen par le Canada aux phases I ou II du Processus, les répondants sont et demeureront les seuls et uniques responsables de l'exactitude, de l'uniformité et de l'exhaustivité de leurs soumissions, et le Canada n'assume, en vertu de cet examen, aucune obligation ni de responsabilité envers les répondants de relever, en tout ou en partie, toute erreur ou toute omission, dans les soumissions ou en réponse à toute communication provenant d'un répondant.

LE RÉPONDANT RECONNAÎT QUE LES EXAMENS LORS DES PHASES I ET II DU PRÉSENT PROCESSUS NE SONT QUE PRÉLIMINAIRES ET N'EMPÊCHENT PAS QU'UNE SOUMISSION SOIT NÉANMOINS

JUGÉE NON RECEVABLE À LA PHASE III, ET CE, MÊME POUR LES EXIGENCES OBLIGATOIRES QUI ONT FAIT L'OBJET D'UN EXAMEN AUX PHASES I OU II, ET MÊME SI LA SOUMISSION AURAIT ÉTÉ JUGÉE RECEVABLE À UNE PHASE ANTÉRIEURE. LE CANADA PEUT DÉTERMINER À SA DISCRÉTION QU'UNE SOUMISSION NE RÉPOND PAS À UNE EXIGENCE OBLIGATOIRE À N'IMPORTE QUELLE DE CES PHASES. LE RÉPONDANT RECONNAÎT ÉGALEMENT QUE MALGRÉ LE FAIT QU'IL AIT FOURNI UNE RÉPONSE À UN AVIS OU À UN RAPPORT D'ÉVALUATION DE LA CONFORMITÉ (REC) (TEL QUE CES TERMES SONT DÉFINIS PLUS BAS) QU'IL EST POSSIBLE QUE CETTE RÉPONSE NE SUFFISE PAS POUR QUE SA SOUMISSION SOIT JUGÉE CONFORME AUX AUTRES EXIGENCES OBLIGATOIRES. (c)

(c) Le Canada peut, à sa propre discrétion et à tout moment, demander et recevoir de l'information de la part du soumissionnaire afin de corriger des erreurs ou des lacunes administratives dans sa soumission, et cette nouvelle information fera partie intégrante de sa soumission. Ces erreurs pourraient être, entre autres : une signature absente; une case non cochée dans un formulaire; une erreur de forme; l'omission d'un accusé de réception, du numéro d'entreprise d'approvisionnement ou même les coordonnées des personnes-ressources, c'est-à-dire leurs noms, leurs adresses et les numéros de téléphone; ou encore des erreurs d'inattention dans les calculs ou dans les nombres, et des erreurs qui n'affectent en rien les montants que le répondant a indiqué pour le prix ou pour tout composant du prix. Ainsi, le Canada a le droit de demander ou de recevoir toute information après la date de clôture de l'invitation à soumissionner uniquement lorsque l'invitation à soumissionner permet ce droit expressément. Le répondant disposera alors d'un délai indiqué pour fournir l'information requise. Toute information fournie hors délais sera refusée.

(d) Le PCSP ne limite pas les droits du Canada en vertu du Guide des clauses et conditions uniformisées d'achat (CCUA) 2003 (2020-05-28) Instructions uniformisées – biens ou services – besoins concurrentiels, ni le droit du Canada de demander ou d'accepter toute information pendant la période de soumission ou après la clôture de cette dernière, lorsque la demande de soumissions confère expressément ce droit au Canada, ou dans les circonstances décrites au paragraphe (c).

(e) Le Canada enverra un Avis ou un REC selon la méthode de son choix et à sa discrétion absolue. Le répondant doit soumettre sa réponse par la méthode stipulée dans l'Avis ou le REC. Les réponses sont réputées avoir été reçues par le Canada à la date et à l'heure qu'elles ont été livrées au Canada par la méthode indiquée dans l'Avis ou le REC et à l'adresse qui y figure. Un courriel de réponse autorisé dans l'Avis ou le REC est réputé reçu par le Canada à la date et à l'heure auxquelles il a été reçu dans la boîte de réception de l'adresse électronique indiquée dans l'Avis ou le REC. Un Avis, ou un REC, envoyé par le Canada au soumissionnaire à l'adresse fournie par celui-ci dans la soumission ou après l'envoi de celle-ci est réputé avoir été reçu par le répondant à la date à laquelle il a été envoyé par le Canada. Le Canada n'assume aucune responsabilité envers les répondants pours les soumissions retardataires, peu importe la cause.

Phase I: Soumission financière – Pas applicable

Phase II: Soumission technique

(a) L'examen par le Canada au cours de la phase II se limitera à une évaluation de la soumission technique afin de vérifier si le répondant a respecté toutes les exigences obligatoires d'admissibilité. Cet examen n'évalue pas si la soumission technique répond à une norme ou répond à toutes les exigences de la soumission. Les exigences obligatoires d'admissibilité sont les critères techniques obligatoires tels qu'ainsi décrits dans la présente demande de soumissions comme faisant partie du Processus de conformité des soumissions en phases. Les critères techniques obligatoires qui ne sont pas identifiés dans la demande de soumissions comme faisant partie du PCSP ne seront pas évalués avant la phase III.

(b) Le Canada enverra un avis écrit au soumissionnaire REC précisant les exigences obligatoires d'admissibilité que la soumission n'a pas respectée. Un soumissionnaire dont la soumission a été jugée recevable au regard des exigences examinées au cours de la phase II recevra un REC qui précisera que sa soumission a été jugée recevable au regard des exigences examinées au cours de la phase II. Le répondant en question ne sera pas autorisé à soumettre des informations supplémentaires en réponse au REC.

(c) Le répondant disposera de la période de temps précisée dans le REC (« période de grâce ») pour remédier à l'omission de répondre à l'une ou l'autre des exigences obligatoires d'admissibilité inscrites dans le REC en fournissant au Canada, par écrit, des informations supplémentaires ou des clarifications en réponse au REC. Les réponses reçues après la fin de la période de grâce ne seront pas prises en considération par le canada sauf, dans les circonstances et conditions expressément prévues par le REC.

(d) La réponse du soumissionnaire doit adresser uniquement les exigences obligatoires d'admissibilité énumérées dans le rapport d'évaluation de conformité (REC) et considérées comme non accomplies, et doit inclure uniquement les renseignements nécessaires pour ainsi se conformer aux exigences. Toutefois, dans le cas où une réponse aux exigences obligatoires d'admissibilité énumérées dans le REC entraînera nécessairement la modification d'autres renseignements qui sont déjà présents dans la soumission, les rajustements nécessaires devront être mis en évidence par le répondant. La réponse au REC ne doit pas inclure de changement à la soumission financière. Toute autre information supplémentaire qui n'est pas requise pour se conformer aux exigences ne sera pas prise en considération par le Canada.

(e) La réponse du soumissionnaire au REC devra spécifier, pour chaque cas, l'exigence obligatoire d'admissibilité du REC à laquelle elle répond, notamment en identifiant le changement effectué dans la section correspondante de la soumission initiale, et en identifiant dans la soumission initiale les modifications nécessaires qui en découlent. Pour chaque modification découlant de la réponse aux exigences obligatoires d'admissibilité énumérées dans le REC, le répondant doit

expliquer pourquoi une telle modification est nécessaire. Il n'incombe pas au Canada de réviser la soumission du soumissionnaire; il incombe plutôt au soumissionnaire d'assumer les conséquences si sa réponse au REC n'est pas effectuée conformément au présent paragraphe. Toutes les informations fournies doivent satisfaire aux exigences de la demande de soumissions.

(f) Tout changement apporté à la soumission par le répondant en dehors de ce qui est demandé, sera considéré comme étant de l'information nouvelle et ne sera pas prise en considération. L'information soumise selon les exigences de cette demande de soumissions en réponse au REC remplacera, intégralement et uniquement la partie de la soumission originale telle qu'elle est autorisée dans cette section.

(g) Les informations supplémentaires soumises pendant la phase II et permises par la présente section seront considérées comme faisant partie de la soumission et seront prises en compte par le Canada dans l'évaluation de la soumission lors de la phase II que pour déterminer si la soumission respecte les exigences obligatoires admissibles. Celles-ci ne seront utilisées à aucune autre phase de l'évaluation pour augmenter les notes que la soumission originale pourrait obtenir sans les avantages de telles informations additionnelles. Par exemple, un critère obligatoire admissible qui exige l'obtention d'un nombre minimum de points pour être considéré conforme sera évalué à la phase II afin de déterminer si cette note minimum obligatoire aurait été obtenue si le répondant n'avait pas soumis les renseignements supplémentaires en réponse au REC. Dans ce cas, la soumission sera considérée comme étant conforme par rapport à ce critère obligatoire admissible et les renseignements supplémentaires soumis par le répondant lieront le répondant dans le cadre de sa soumission, mais la note originale du soumissionnaire, qui était inférieure à la note minimum obligatoire pour ce critère obligatoire admissible, ne changera pas, et c'est cette note originale qui sera utilisée pour calculer les notes pour la soumission.

(h) Le Canada déterminera si la soumission est recevable pour les exigences examinées à la phase II, en tenant compte de l'information supplémentaire ou de la clarification fournie par le répondant conformément à la présente section. Si la soumission n'est pas jugée recevable selon des exigences examinées à la phase II à la satisfaction du Canada, la soumission financière sera jugée non recevable et rejetée.

(i) Uniquement les soumissions jugées recevables selon les exigences examinées à la phase II et à la satisfaction du Canada seront ensuite évaluées à la phase III.

4.4 Évaluation technique

Critères techniques obligatoires

Le processus de conformité des soumissions en phases s'appliquera à tous les critères techniques obligatoires. Les critères techniques obligatoires sont présentés dans le tableau 1 de l'annexe A – Critères d'évaluation techniques.

Critères techniques cotés

Le processus de conformité en phases s'appliquera à tous les critères techniques cotés et aux exigences obligatoires comportant une note avec un seuil minimal. Les critères techniques cotés et les exigences obligatoires comportant une note avec un seuil minimal sont présentés dans le tableau 2 de l'annexe A — Critères d'évaluation techniques.

La cotation de chaque soumission se fera par l'attribution d'une note aux exigences cotées, qui sont précisées dans la demande de soumissions par le terme « cotées » ou par la mention d'une note. Les soumissionnaires qui ne présentent pas une soumission complète (contenant tous les renseignements exigés dans la demande de soumissions) verront leurs soumissions cotées en conséquence.

4.5 Critères de qualification de base

4.5.1 Lorsque la réponse

i. respecter toutes les exigences de la ISQ; et

ii. satisfaire à tous les critères d'évaluation techniques obligatoires à l'Annexe A; et

iii. obtenir au moins 80 points pour l'ensemble des critères d'évaluation techniques qui sont cotés de l'annexe A. L'échelle de cotation compte 180 points.

deviendra un fournisseur préqualifié pour la prochaine phase du processus d'approvisionnement

4.5.2 Les soumissions ne répondant pas aux exigences de (i) ou (ii) ou (iii) seront déclarées non recevables.

4.5.3 Le gouvernement du Canada se réserve le droit de réévaluer la qualification de tout répondant qualifié, et ce, à tout moment durant le processus d'approvisionnement. Par exemple, dans une situation où une attestation de sécurité en particulier est une des exigences de l'ISQ et que celle du répondant change ou vient à échéance, le gouvernement du Canada pourrait disqualifier ce répondant qualifié, étant donné qu'il ne répond plus aux exigences de l'ISQ. De même, si des informations sont signalées au Canada et qu'elles mettent en question les qualifications du répondant qualifié dans le cadre de la présente ISQ, le Canada peut évaluer de nouveau ce répondant. Le cas échéant, il pourrait demander plus d'information. Si le répondant qualifié ne les fournit pas dans les cinq (5) jours ouvrables (ou plus longtemps, selon l'autorité contractante), le Canada peut disqualifier le fournisseur préqualifié.

4.5.4 Les répondants non retenus ne pourront pas participer aux étapes ultérieures du processus d'approvisionnement ni être évalués de nouveau à cette fin, à moins que le

Canada décide, à sa seule discrétion, que les circonstances nécessitent une nouvelle évaluation.

4.5.5 Le Canada avisera par écrit chaque répondant de son statut de qualification.

4.6 Seconde vague de qualification de l'ISQ

4.6.1 Si le gouvernement du Canada fournit aux répondants non retenus une deuxième occasion de se qualifier, il leur fera tous parvenir par écrit, la même journée, les raisons pour lesquelles ils ne se sont pas qualifiés au cours de la première vague de qualification.

4.6.2 Si le gouvernement du Canada fournit aux répondants non retenus une deuxième occasion de se qualifier, il leur fera tous parvenir par écrit, la même journée, les raisons pour lesquelles ils ne se sont pas qualifiés au cours de la première vague de qualification.

4.6.3 Les répondants qui ne se qualifient pas à la suite de la seconde vague effectuée par le Canada ne pourront pas participer ou être évalués de nouveau pour les étapes ultérieures du processus d'approvisionnement.

Annexe A: Critères d'évaluation obligatoires

1. Critères d'évaluation technique

1.1 Critères techniques obligatoires

Le répondant doit satisfaire aux critères d'évaluation technique obligatoires précisés dans le tableau 1 de l'annexe A de l'ISQ. Tous les critères d'évaluation énumérés dans le tableau 1 sont obligatoires et sont tous assujettis au processus de conformité des soumissions par étapes. Le répondant doit fournir les documents nécessaires afin de démontrer le respect de ces exigences. Chaque critère technique obligatoire doit être traité séparément.

1.2 Critères techniques cotés

Les réponses qui satisfont à toutes les exigences techniques obligatoires seront évaluées et cotées selon les critères d'évaluation cotés par points spécifiés au tableau 2. Le processus de conformité des soumissions en phases s'appliquera à tous les critères d'évaluation énumérés dans le tableau 2 de l'annexe A. Le répondant doit fournir la documentation nécessaire afin de démontrer qu'il se conforme à cette exigence. Chaque critère technique coté doit être traité séparément.

1.3 Projets

1.3.1 Dans les cas où le répondant doit inclure une description de projets :

(i) le projet doit avoir été réalisé par le répondant lui-même : l'expérience acquise par un sous-traitant proposé ou une société affiliée au répondant qui ne fait pas partie de l'équipe de base ne compte pas;

(ii) un projet doit avoir mis en œuvre avec succès au cours des sept (7) dernières années suivant la date de clôture de l'IQ;

(iii) plus d'un (1) projet de référence peut être utilisé pour satisfaire à tous les critères d'évaluation, toutefois, pas plus d'un (1) projet de référence ne peut être utilisé pour satisfaire à un critère d'évaluation individuel;

(iv) un projet doit être opérationnel et non pas dans des environnements de recherche et développement (R et D) ou d'essai;

(v) un projet peut avoir été réalisé dans le cadre d'une coentreprise, mais le répondant doit alors indiquer les éléments pour lesquels il était responsable;

(vi) un même projet peut être utilisé pour satisfaire à plusieurs critères;

(vii) le répondant doit indiquer clairement et de la façon la plus détaillée possible son rôle, ses responsabilités et les produits livrables dans le cadre du contrat;

(viii) le répondant doit présenter les résultats obtenus et les livrables atteints dans le cadre de

leur contrat et préciser s'ils ont respecté la portée, le budget et l'échéancier.

1.3.2 Les répondants sont avisés de ne pas inclure dans leur soumission des renseignements classifiés ou des renseignements distincts qui, une fois regroupés, deviennent classifiés.

1.3.3 Les répondants doivent fournir le formulaire 2 – Formulaire de vérification des projets cités en référence, pour chaque projet déclaré en réponse aux exigences obligatoires et cotées correspondantes.

Les répondants devraient seulement fournir les projets cités en référence demandés, comme indiqué dans chaque exigence obligatoire. Si le nombre de projets cités en référence est supérieur au nombre demandé, les répondants devront préciser les projets cités en référence qui s'appliquent aux exigences obligatoires correspondantes.

1.3.4 Le répondant **doit** fournir les renseignements suivants pour chaque projet cité en référence :

a. nom du projet
b. une brève description de l'objectif du projet
c. la valeur du projet
d. en coentreprise ou à titre de fournisseur unique
e. la valeur du contrat (avec le fournisseur)
f. la durée du projet (mois/année)
g. la durée du contrat (mois/année)
h. le niveau d'effort du projet (année-personne – bureau de projet et expert en la matière)
i. le niveau d'effort du contrat (année-personne – bureau de projet et expert en la matière)
j. la portée de la capacité (nombre d'usagers et points terminaux)
k. l'énoncé des besoins du projet et sa portée
l. la classification du projet
m. les références et coordonnées

2. Expérience au sein de projets classifiés

Si l'expérience de projet requise pour satisfaire à un critère obligatoire ou coté a été acquise dans un environnement classifié, et pour lequel une entente de confidentialité ou une entente visée par la *Loi sur la protection de l'information* (LPI) a été signée, il pourrait être impossible de divulguer certains détails nécessaires pour confirmer l'expérience exigée. Si le répondant choisit d'inclure ces projets classifiés, il devra suivre la procédure suivante :

Le cas échéant, le répondant doit nommer le projet classifié « Projet A », « Projet B », et ainsi de suite. Il doit préciser les dates de début et de fin et la durée du projet. Le répondant doit également citer un client en référence, par exemple le responsable de projet, et fournir ses coordonnées. Le client doit être en mesure de fournir l'information qui est nécessaire pour permettre de vérifier la conformité au critère d'évaluation.

L'équipe d'évaluation, qui comprend une autorité contractante avec une cote de sécurité appropriée, vérifiera auprès des responsables de projet que le projet a été complété conformément aux exigences.

Les résultats de cette vérification des références seront utilisés pour l'évaluation des critères obligatoires et cotés. Si la référence du répondant est incapable de fournir les informations nécessaires pour vérifier que l'expérience est conforme au critère d'évaluation, la réponse sera jugée insatisfaisante pour ce critère.

3. Formulaire 2 – Formulaire de vérification des projets cités en référence

Instructions à l'intention des fournisseurs :

(a) Les répondants doivent fournir un formulaire de vérification pour chaque projet mis en référence, en réponse à chacun des critères obligatoires et cotés des tableaux 1 et 2 de l'annexe A de la présente ISQ.

(b) Si les renseignements demandés dans le présent formulaire n'accompagnent pas la réponse du répondant à l'ISQ, ils doivent être fournis sur demande de l'autorité contractante dans le délai précisé.

(c) Le Canada peut communiquer avec la personne-ressource du client, indiquée pour le projet cité en référence, afin de valider les renseignements fournis.

Formulaire 2 – Formulaire de vérification des projets cités en référence

#	Response		
(a)	Numéro du critère obligatoire (voir table 1 et 2 de l'annexe A)		
(b)	Nom légal complet du répondant ou membre de l'équipe (si le répondant est une coentreprise, le nom légal complet du membre de la coentreprise pour le projet référencé)		
(c)	Description du projet et du contrat (spécifique au répondant), la valeur en dollars canadiens, la durée (indiquer le mois et l'année) et la cote de sécurité du projet référencé		
(d)	Nom de l'organisation cliente pour le projet référencé		
(e)	Nom du contact client et ses coordonnées pour le projet référencé		
(f)	Organisation cliente et affiliation du contact client avec le répondant (ou membre de la coentreprise). Veuillez indiquer: Ne sont pas affiliés Sont affiliés		
	Veuillez indiquer:	Ne sont pas affiliés	Sont affiliés
(g)	Nom de l'organisation pour laquelle le contact client travaille actuellement (si le contact client ne travaille plus pour l'organisation cliente identifiée pour le projet référencé)		
(h)	Titre du contact client (lorsqu'il travaillait pour le projet référencé)		
(i)	Numéro de téléphone actuel du contact client		
(j)	Adresse courriel actuelle du contact client		
(k)	Rôle du contact client dans le projet référencé		
(l)	Indiquez le nombre maximal d'utilisateurs et de points terminaux du projet référencé sur lequel seul le répondant a travaillé.		
	Nombre d'utilisateurs:	Nombre de points terminaux:	
(m)	Identifiez les composants dont vous étiez responsable: (Si le projet référencé était une coentreprise, veuillez identifier uniquement les composants pour lesquels le répondant était responsable)		
(n)	Identifier le niveau d'effort (année-personne – bureau de projet et expert en la matière) pour les composants du projet référencé dont vous étiez responsable		
(o)	Confirmer que le projet référencé se trouve dans un environnement d'exploitation (Oui/Non)		
(p)	Si le projet référencé est utilisé pour satisfaire plusieurs critères, veuillez fournir une ventilation du pourcentage pour les critères donnés alloués dans le cadre de l'échéancier du projet		
(q)	Pour le contrat dont relève le projet référencé, indiquer clairement le rôle, les responsabilités et les produits livrables du répondant de la façon la plus détaillée possible		

Table 1 - Critères d'évaluation technique obligatoires

Les termes ou mots en italique sont définis dans Table 3 - Définitions

No de l'exigence	Critères obligatoires	Evaluation	**Preuves exigées** (dans les sept années précédant la date de clôture de l'ISQ)
O1	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de gestion de l'information et de technologie de l'information (GI-TI) complexe* au cours des sept (7) dernières années, qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de solutions commerciales, gouvernementales ou militaires standard intégrées de *cybersécurité* et *d'analyse des décisions et réponse*, ainsi que la prestation *d'aide à la stabilisation* pendant au moins douze (12) mois pour : **a. *des réseaux de GI-TI complexes* composés d'au moins 8000 *points terminaux; et*** **b. au moins une des nations du Groupe des cinq (Gp5), à savoir l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Unis ou les États-Unis.**	Réussite / échec	Pour le critère 1, le *répondant* doit fournir pas plus d'un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions commerciales, gouvernementales ou militaires standard intégrées *de cybersécurité* et *d'analyse des décisions et réponses* au sein de nations du Gp5.
O2	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* au cours des sept (7) dernières années, qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de solutions commerciales, gouvernementales ou militaires standard intégrées de *cybersécurité* et *d'analyse des décisions et réponse* pour **au moins 8000 *points terminaux*** au sein de nations du Gp5. Ces solutions doivent avoir fourni les capacités indiquées aux points (a) et (b) ci-dessous, ainsi qu'au moins cinq (5) des capacités indiquées aux points (c) à (h). **a. Fournir *l'analyse des décisions et réponse relatives au milieu cybernétique* des *réseaux de commandement et contrôle (C2)* par l'entremise d'une *image commune de la situation opérationnelle (ICSO)* intégrée.** b. **Fournir *l'analyse des décisions et réponses relatives au milieu cybernétique* des *réseaux de C2* par l'entremise de la sécurité infonuagique**. **c. Identifier et suivre tous les actifs de GI-TI (autorisés et non autorisés).** **d. Évaluer les actifs relativement aux vulnérabilités, à la configuration, au risque et à la conformité aux correctifs.** **e. Recueillir, conserver et analyser les renseignements sur les menaces**	Réussite / échec	Pour le critère 2, le *répondant* doit fournir pas plus d'un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.

	cybernétiques. **f. Détecter et évaluer les activités suspectes, et fournir du contexte pour les évaluations du risque et des vulnérabilités.** **g. Exécuter en *temps quasi réel* la prévention des menaces et la réponse à celles-ci, et prendre les mesures d'atténuation appropriées.** h. **Fournir au moins de *l'aide à la stabilisation* pendant au moins douze (12) mois.**		
O3	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de multiples (au moins 5) solutions commerciales, gouvernementales ou militaires standard de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5. Ce projet doit **démontrer TOUS les éléments suivants au sein d'un environnement *réseau de GI-TI complexe* d'au moins 8000 *points terminaux*, ainsi que la prestation *d'aide à la stabilisation* pendant au moins douze (12) cours des sept (7) dernières années.** **a. Recueillir, conserver, détecter et analyser les données de façon continue (et en *temps quasi réel*), et présenter du contexte pour les évaluations des risques et des vulnérabilités.** b. **Les transmissions de données sur les cybermenaces et de renseignements analytiques en provenance de multiples sources et fournis en divers formats doivent être normalisées et intégrées en un format commun en vue de l'analyse, en plus de fournir une *Image commune de la situation opérationnelle (ICSO).***	Réussite / échec	Pour le critère 3, le *répondant* doit fournir pas plus d'un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.
O4	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de multiples (au moins 5) solutions commerciales, gouvernementales ou militaires standard intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5. Ce projet doit **démontrer TOUS les éléments suivants au sein d'un environnement *réseau de GI-TI complexe* d'au moins 8000 *points terminaux*, ainsi que la prestation *d'aide à la stabilisation* pendant au moins douze (12) mois au cours des sept (7) dernières années**. **a. L'analyse des incidents de *cybersécurité* en provenance des sources suivantes :**	Réussite / échec	Pour le critère 4, le *répondant* doit fournir pas plus d'un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.

	i. le renseignement sur les menaces; **ii. les incidents antérieurs:** **iii. les incidents similaires qui ont eu lieu sur les réseaux;** **iv. la détection fondée sur les signatures et sur les connaissances heuristiques.** **b. L'analyse des données sur les incidents de cybersécurité en provenance des sources suivantes :** **i. le système de gestion des événements et des incidents de sécurité (SGEIS);** **ii. la détection et l'intervention aux points terminaux;** **iii. la saisie intégrale des paquets;** **iv. le système de détection d'intrusion et de prévention d'intrusion.** **v. les évaluations des vulnérabilités;** **la gestion du flux des travaux.** **c. Alertes de *cybersécurité* intégrées provenant de trois (3) des six (6) sources suivantes :** **i. le renseignement sur les menaces;** **ii. l'information d'une entité externe;** **iii. l'information sur l'actif interne;** **iv. l'information provenant du réseau et des points terminaux;** **v. l'historique des activités;** **vi. l'information de l'analyse du trafic réseau.**		
O5	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de solutions commerciales, gouvernementales ou militaires standard intégrées de *cybersécurité* et *d'analyse des décisions et réponse*, ainsi que la prestation *d'aide à la stabilisation pendant au moins douze (12) mois au cours des sept (7) dernières années.* Ce projet devait comprendre **l'identification, le confinement et l'éradication *souples* et *dynamiques* des menaces (internes et externes) à l'aide de capacités de cyberdéfense avancées en *temps quasi réel*.**	Réussite / échec	Pour le critère 5, le *répondant* doit fournir pas plus d'un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.

	effectuées par l'entremise de plateformes normalisées au sein d'un *réseau de GI-TI complexe* comptant au moins 8000 *points terminaux*.		
O6	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* au cours des sept (7) dernières années, qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de solutions commerciales, gouvernementales ou militaires standard intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5, ainsi que la prestation *d'aide à la stabilisation* pendant au moins douze (12) mois**. Ce projet devait comprendre l'établissement d'un dépôt de données en appui au stockage, au chiffrement, à l'analyse, à la récupération et au traitement de données structurées et non structurées (y compris la capture de paquets [PCAP], les données Netflow et le format d'événement commun [CEF]) sur un réseau dispersé sur le plan géographique (au moins 10 nœuds). Il devait également comprendre la réalisation d'une *analyse de 2e niveau* en vue de permettre le soutien à la prise de décisions par l'entremise de l'exécution automatisée et assistée de mesures d'intervention pour un *réseau de GI-TI complexe* composé d'au moins 8000 *points terminaux*.**	Réussite / échec	Pour le critère 6, le *répondant* doit fournir pas plus d'un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.
O7	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de solutions commerciales, gouvernementales ou militaires standard de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5, ainsi que la prestation *d'aide à la stabilisation* pendant au moins douze (12) mois **pour des *réseaux de GI-TI complexes*, composés d'au moins 8000 *points terminaux*. En outre, il doit avoir fourni, dans le cadre de ce projet, toutes les fonctionnalités d'interopérabilité décrites ci-dessous au sein de nations du Gp5 au cours des sept (7) dernières années**. **a. La capacité d'intégrer en toute facilité divers flux, comme des vecteurs de menace, des renseignements analytiques et autres, auprès de partenaires principaux tels que les autres ministères gouvernementaux, les nations du Gp5 ou l'industrie.** **b. La collecte centralisée de renseignements sur les menaces.** **c. La fusion et la déduplication de renseignements sur les menaces.**	Réussite / échec	Pour le critère 7, le *répondant* doit fournir pas plus d'un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.

	d. La recherche et l'analyse graphique d'indicateurs. **e. Le stockage de renseignements sur les menaces structurés et non structurés, lisibles par machine.** **f. La diffusion de renseignements sur les menaces vers des outils externes.** **g. Des interfaces et mécanismes de partage de renseignements sur les menaces avec d'autres organisations (notamment en formats SCAP, STIX et JSON).**		
O8	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* **au cours des sept (7) dernières années**, qui comprenait **la conception, le développement et la livraison de solutions intégrées d'exercice et de formation à l'intention des exploitants et spécialistes de la maintenance de solutions de *cybersécurité* et *d'analyse des décisions et réponse* pour des systèmes (ensembles du matériel et des logiciels) d'un *réseau de GI-TI complexe* composé d'au moins 8000 *points terminaux*** au sein de nations du Gp5. Ce projet devait inclure l'élaboration de scénarios opérationnels et de soutien, qui peuvent être créés, modifiés, tenus à jour et exécutés par les cyberexploitants dans un environnement d'exercice et de formation.	Réussite / échec	Pour le critère 8, le *répondant* ne doit pas fournir plus d'un (1) projet de référence exécuté au cours des sept (7) dernières années dans le cadre duquel *il* a élaboré et livré des solutions d'exercice et de formation à des nations du Gp5.
O9	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe*, qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la livraison de solutions commerciales, gouvernementales ou militaires standard intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5, ainsi que la prestation *d'aide à la stabilisation* pendant au moins douze (12) mois. **Ce projet, réalisé au cours des sept (7) dernières années, devait inclure l'administration et la gestion de la collecte de données (notamment sur les actifs cybernétiques de TI, sur la configuration, etc.) en provenance de sources *hétérogènes*, et le développement de solutions de gestion de la configuration pour des ensembles de données importants, hébergés sur des *réseaux de GI-TI complexes* composés d'au moins 8000 *points terminaux*.**	Réussite / échec	Pour le critère 9, le *répondant* doit fournir au moins un (1) projet de référence réalisé au cours des sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.
O10	Le *répondant* doit avoir *mis en œuvre avec succès* un (1) *projet de GI-TI complexe* qui comprenait la conception, le développement, l'intégration, la mise en œuvre et la	Réussite / échec	Pour le critère 10, le *répondant* doit fournir au moins un (1) projet de référence réalisé au cours des

	livraison de solutions commerciales, gouvernementales ou militaires standard intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5. **En outre, le répondant doit avoir fourni du soutien technique pour ces solutions pendant une période continue d'au moins douze (12) mois au cours des sept (7) dernières années, qui satisfait aux critères suivants ou les dépasse :** **a. offert cinq (5) jours par semaine;** **b. huit (8) heures par jour;** **c. 52 semaines par année.**		sept (7) dernières années dans le cadre duquel *il* a *mis en œuvre avec succès* des solutions *commerciales, gouvernementales ou militaires standard* intégrées de *cybersécurité* et *d'analyse des décisions et réponse* au sein de nations du Gp5.

Tableau 2 – Critères d'évaluation techniques cotés

Les réponses qui répondent à tous les critères techniques obligatoires seront évaluées et notées en fonction des critères cotés par points ci-après.

No de l'exigence	Critères d'évaluation cotés	Pointage	Note	Preuves exigées (dans les sept années précédant la date de clôture de l'ISQ)
C1	Le *répondant* a *mis en place correctement* au cours des sept (7) dernières années un (1) projet de GI/TI complexe comportant la conception, le développement, l'intégration et la mise en place d'une solution d'*analyse et de réponse de cybersécurité et de cyberdécision* intégrée de matériel commercial, gouvernemental et militaire courant et de resynchronisation dans des pays du Groupe des cinq, et de services de *soutien à la stabilisation* pendant au moins douze (12) mois pour une solution d'*analyse et de réponse de cybersécurité et de cyberdécision* en intégrant à cette solution les technologies émergentes suivantes : a) Détection des anomalies et analyse de données par apprentissage automatique; i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) plus de 8000 dispositifs terminaux; b) Analyse de mégadonnées; i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) plus de 8000 dispositifs terminaux; c) Orchestration et automatisation de la sécurité et intervention (OASI); i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) plus de 8000 dispositifs terminaux	Les points seront accordés en fonction du nombre de dispositifs terminaux du projet. Les points ne seront accordés qu'une fois pour chaque rubrique (a) à (e). Somme des points ci-dessous, **jusqu'à concurrence de cent dix (110) points** 10 points 20 points 30 points 40 points 5 points 10 points 15 points 20 points 5 points 10 points 15 points 20 points		Pour <u>chacune</u> des sous-catégories des critères cotés C1 le *répondant* doit fournir au plus une (1) référence d'un projet exécuté au cours des sept (7) dernières années où il a mis en place une solution d'*analyse et de réponse de cybersécurité et de cyberdécision* intégrée de matériel commercial, gouvernemental et militaire courant dans des pays du Groupe des cinq. Le répondant peut présenter plus d'un projet pour répondre aux critères cotés C1 (a) à (e), mais pas pour un des sous-critères (a) à (e).

	d) Détection des menaces et des vulnérabilités à l'aide de l'intelligence artificielle; i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) plus de 8000 dispositifs terminaux e) Analyse du comportement des utilisateurs et des entités; i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) pus de 8000 dispositifs terminaux	5 points 10 points 15 points 20 points 4 points 6 points 8 points 10 points		
C2	Le *répondant* a *mis en place correctement* au cours des sept (7) dernières années un (1) projet de GI/TI complexe comportant la conception, le développement, l'intégration et la mise en place d'une solution d'*analyse et de réponse de cybersécurité et de cyberdécision* intégrée de matériel commercial, gouvernemental et militaire courant dans des pays du Groupe des cinq, et de services de *soutien à la stabilisation* pendant au moins douze (12) mois pour des systèmes intégrant des environnements à niveaux de sécurité multiples et comportant une *passerelle entre chaque domaine* : i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) plus de 8000 dispositifs terminaux	Les points seront accordés en fonction du nombre de dispositifs terminaux du projet. Nombre maximal : Vingt (20) points 5 points 10 points 15 points 20 points		Le *répondant* doit fournir au plus une (1) référence d'un projet exécuté au cours des sept (7) dernières années où il a mis en place une solution d'analyse et de réponse de cybersécurité et de cyberdécision intégrée de matériel commercial, gouvernemental et militaire courant dans des pays du Groupe des cinq correspondant au critère coté C2
C3	Le *répondant* a *mis en place correctement* au cours des sept (7) dernières années un projet de GI/TI complexe comportant la conception, le développement, l'intégration et la mise en place d'une solution d'analyse et de réponse de cybersécurité et de cyberdécision intégrée de matériel commercial, gouvernemental et militaire courant et de resynchronisation dans des pays du Groupe des cinq, et de services de *soutien à la stabilisation* pendant au moins douze (12) mois pour tous les aspects suivants d'un seul réseau : (a) éléments d'un réseau étendu à au moins deux (2) continents comportant au moins dix (10) nœuds fonctionnels distincts, (b) interconnecté à distance à une vitesse défavorable (liens de moins de 1,544 Mbps) en environnements hostiles à un	Les points seront accordés en fonction du nombre de dispositifs terminaux du projet. Nombre maximal : Vingt (20) points		Le répondant doit fournir au plus une (1) référence d'un projet exécuté au cours des sept (7) dernières années où il a mis en place une solution d'analyse et de réponse de cybersécurité et de cyberdécision intégrée de matériel commercial, gouvernemental et militaire courant dans des pays du Groupe des cinq correspondant au critère coté C3

	réseau central haute vitesse (100 Mbps ou plus), et (c) pour la transmission de données liées aux critères obligatoires 1 à 6 dans un réseau de : i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) plus de 8000 dispositifs terminaux	5 points 10 points 15 points 20 points		
C4	Le *répondant* a *mis en place correctement* au cours des sept (7) dernières années un (1) projet de GI/TI complexe comportant la conception, le développement, l'intégration et la mise en place d'une solution d'*analyse et de réponse de cybersécurité et de cyberdécision* intégrée de matériel commercial, gouvernemental et militaire courant et de resynchronisation dans des pays du Groupe des cinq en environnement militaire, et de services de *soutien à la stabilisation* pendant au moins douze (12) mois : i) 2001 to 4000 dispositifs terminaux; ii) 4001 to 6000 dispositifs terminaux; iii) 6001 to 8000 dispositifs terminaux; iv) plus de 8000 dispositifs terminaux;	Les points seront accordés en fonction du nombre de dispositifs terminaux du projet. Nombre maximal : Vingt (10) points 2 points 4 points 6 points 10 points		Le *répondant* doit fournir au plus une (1) référence d'un projet exécuté au cours des sept (7) dernières années où il a mis en place une solution d'*analyse et de réponse de cybersécurité et de cyberdécision* intégrée de matériel commercial, gouvernemental et militaire courant dans des pays du Groupe des cinq correspondant au critère coté C4.
Total des points (maximum 160; note de passage 80)				

* Remarque : Pour tous les critères cotés C1 à C4, 2000 dispositifs terminaux ou moins obtiennent zéro (0) point.

Table 3 - Définitions

Terme	Définition
Aide à la stabilisation	L'aide à la stabilisation désigne un soutien continu pendant au moins douze (12) mois, à partir du moment où le ou les groupes de clients ont commencé à utiliser la capacité cybernétique jusqu'au moment où la capacité cybernétique a été entièrement mise en œuvre, au minimum.
Analyse de deuxième (2e) niveau	L'analyse de 2e niveau offre une analyse encore plus approfondie et se concentre sur le soutien aux incidents et sur le traitement des alertes découlant de l'analyse de 1er niveau. Les analystes de 2e niveau coordonnent la transmission des conclusions sur la surveillance de sécurité avec l'équipe du renseignement sur les menaces, les fournisseurs partenaires et avec des personnes-ressources particulières afin d'obtenir une analyse plus globale des données des événements et de leur incidence sur des environnements donnés.
Analyse des décisions et réponse	Il s'agit de produire une description exacte des cyber ressources, individuellement et ensemble comme réseau, en ce qui a trait aux vulnérabilités, aux points faibles liés à l'utilisation et aux menaces, d'après des données recueillies pendant des mois ou des années, puis de mettre en œuvre les plans d'action approuvés pour la sécurité et la cyber défense dans le but de préserver la liberté d'action.
Analyse des modèles de comportement	L'analyse comportementale fait appel à l'apprentissage machine, à l'intelligence artificielle, aux mégadonnées et à l'analytique pour détecter des comportements furtifs malveillants en analysant les différences subtiles dans les activités courantes normales, dans le but de stopper de façon proactive les attaques cybernétiques avant que les attaquants ne soient en mesure de mettre pleinement en œuvre leurs plans destructeurs. L'analyse des modèles de comportement commence par la surveillance comportementale qui, dans le contexte de la cybersécurité, consiste en la consignation des événements et activités d'un système et de ses utilisateurs. Les événements consignés sont comparés à des comportements et politiques de sécurité de base afin de vérifier leur conformité ou de relever des infractions. La surveillance comportementale peut comprendre le suivi des tendances, l'établissement de seuils et la définition de mesures d'intervention. Le suivi des menaces peut révéler une augmentation du nombre d'erreurs nécessitant des services de soutien technique, des niveaux de charge anormaux qui indiquent la présence de code malveillant, ou encore une augmentation des travaux de production, ce qui démontre la nécessité d'augmenter la capacité. Les seuils servent à définir les niveaux d'activités ou d'événements qui, une fois dépassés, constituent une source d'inquiétude et requièrent la prise de mesures d'intervention. Les niveaux inférieurs à ces seuils sont consignés, mais ne

Terme	Définition
	déclenchent pas l'exécution de mesures d'intervention. Celles-ci peuvent servir à résoudre des conflits, à traiter des infractions, à prévenir les périodes d'indisponibilité ou à améliorer des capacités.
Analyse du comportement de l'utilisateur et de l'entité (ACUE)	Les solutions d'analyse du comportement de l'utilisateur et de l'entité (ACUE) font appel à l'analytique pour établir des profils et comportements standard des utilisateurs et des entités (hôtes, applications, trafic réseau et dépôts de données) au fil du temps et à travers les groupes de paires. Toute activité anormale comparativement à ces références de base est présentée comme suspecte et des ensembles d'analyses sont appliqués à ces anomalies peuvent aider à repérer des menaces et des incidents potentiels. La plupart des cas d'utilisation que les entreprises souhaitent obtenir concernent la détection d'attaquants malveillants internes et externes qui s'infiltrent dans leur organisation (employés compromis).
Analytique avancée des données	L'examen autonome ou semi-autonome des données ou du contenu à l'aide de techniques et d'outils de pointe, habituellement autres que ceux du renseignement d'affaires habituel, afin d'accroître la compréhension, de faire des prévisions ou de formuler des recommandations.
Apprentissage machine	La capacité composée de nombreuses technologies (comme l'apprentissage en profondeur, les réseaux neuronaux et le traitement du langage naturel), utilisée dans le cadre de l'apprentissage non supervisé et supervisé, qui est guidée par les leçons tirées des informations existantes.
Autoréparateur	Dans l'univers de la TI, les systèmes autoréparateurs sont décrits comme tout dispositif ou système qui a la capacité de détecter s'il ne fonctionne pas correctement et d'apporter, sans aide, les rectifications nécessaires pour restaurer son bon fonctionnement. Un système pour lequel on s'attend qu'il fonctionne toujours comme prévu.
Connaissance de la situation	Connaissance des éléments de l'environnement opérationnel nécessaire pour prendre des décisions éclairées.
Cyberactif	Tous les actifs (les logiciels, le matériel et les utilisateurs, autorisés et non autorisés) connectés au réseau de commandement (ce qui exclut la gestion de l'identité, des justificatifs et de l'accès dans le cas des utilisateurs).
Cybersécurité	La cybersécurité est un ensemble de technologies et de processus intégrés qui se situent à tous les niveaux conceptuels d'une entreprise – le périmètre, le réseau interne, les divers points terminaux, les applications et les données – et qui servent à analyser l'information, à défendre le réseau et à réagir aux agresseurs et aux menaces qu'ils mettent en œuvre. Assurer la cybersécurité implique en outre d'élaborer des solutions pour réagir aux éventuelles menaces que poseront les

Terme	Définition
	concepts et processus de la nouvelle génération, afin de garantir une protection optimale à chaque niveau. Il importe d'établir des mécanismes qui s'appuient mutuellement et qui s'appliquent là où ils conviennent le mieux dans l'architecture (et la structure), pour être en mesure de s'en servir afin de produire une solide capacité d'analyse, de défense et de réaction en cas de cybermenace.
Déployé	Capacité en appui à une base expéditionnaire (dispersé sur le plan géographique, le plus souvent exploitée dans un contexte de menace) qui emploie et maintient des forces opérationnelles pour réaliser des missions.
Dynamique	Se rapporte à un attribut de données dont les valeurs peuvent uniquement être établies lors de l'exécution d'une partie ou de la totalité d'un programme.
État des actifs	État déterminé en évaluant les attributs des actifs en ce qui a trait à la vulnérabilité, à la configuration, au risque et à la conformité en matière de correctifs.
Évaluation des vulnérabilités	L'évaluation des vulnérabilités est la capacité de relever, de catégoriser et de gérer les vulnérabilités. Parmi les vulnérabilités, comptons des configurations système non sécurisées, des problèmes logiciels ou matériels qui rendent ces derniers vulnérables à l'intrusion cybernétique et aux attaques internes ou externes, le manquement à l'installation de correctifs ainsi que d'autres mises à jour relatives à la sécurité dans des systèmes connectés au réseau de l'entreprise directement, à distance ou à l'aide de l'infonuagique.
Hétérogène	• Équipement réseau de générations technologiques différentes (anciennes et modernes) ou provenant de divers fournisseurs. • Dans le cas des logiciels, il s'agit de logiciels de versions ou de niveaux de correctif différents, ou encore provenant de divers fournisseurs. • Diverses sources de données structurées et non structurées.
Image commune de la situation opérationnelle (ICSO)	L'ICSO est un outil de C2 qui offre une connaissance de la situation et des options d'intervention, ce qui permet aux utilisateurs de prendre des décisions éclairées et précises. Les données sont recueillies de multiples sources afin d'appuyer toutes les fonctions d'une réponse à partir d'une seule plateforme de données spatiales. L'ICSO offre à l'équipe de gestion des incidents en fonction un portrait exhaustif de la situation, ce qui lui permet d'apporter des rectifications à toute activité en cours et de planifier la prochaine période opérationnelle.
Infonuagique	L'infonuagique désigne un type de traitement dans lequel des capacités de TI évolutives et souples sont fournies en tant que service par l'entremise de services externes à l'organisation figurant dans un bassin commun de ressources informatiques configurables (p. ex. des réseaux, des serveurs, des composants de stockage, des applications ou des services), qui peuvent être rapidement fournies

Terme	Définition
	et distribuées en exigeant très peu d'efforts de gestion ou d'interaction avec les fournisseurs de services.
Intelligence artificielle	La capacité souvent utilisée pour décrire les machines (ou ordinateurs) qui reproduisent les fonctions « cognitives », c'est-à-dire la capacité d'une unité fonctionnelle de s'améliorer et d'exécuter des fonctions généralement associées à l'intelligence humaine (en d'autres mots, qui reproduisent des fonctions « cognitives » que l'être humain associe à l'esprit humain, comme le raisonnement, l'apprentissage et la résolution de problème) sans intervention humaine.
Liberté d'action	Une fois la tâche ou la mission établie et les ordres nécessaires transmis, les commandants subordonnés doivent pouvoir jouir d'un maximum de liberté pour prendre l'initiative, exercer leur savoir-faire et mettre en application leur connaissance de la situation locale dans le cadre de la planification et de la conduite d'une opération avec peu de contraintes, voire aucune.
Lignes de communication	Ensemble des voies terrestres, maritimes, fluviales ou aériennes qui relient une force en opération à une ou plusieurs bases d'opérations, et par lesquelles le matériel et les renforts sont acheminés.
Mégadonnées	Par « mégadonnées », on entend des ressources d'information très volumineuses, à grande vitesse ou très variées qui nécessitent des formes rentables et novatrices de traitement de l'information pour permettre l'amélioration des connaissances, de la prise de décisions et de l'automatisation des processus.
Mis en œuvre avec succès	On emploie l'expression « mis en œuvre avec succès » lorsque le Répondant a conçu, développé, intégré, mise en œuvre et livré Aide à la stabilisation des éléments pour un projet mené à terme avec succès ou dans le cadre duquel on a pleinement mis en œuvre une capacité (il peut s'agir d'un projet échelonné sur plusieurs phases), où toutes les exigences ont été respectées et pour lequel il a fourni une preuve d'acceptation des clients. À noter qu'une lettre de soutien d'un client (fédéral) est jugée acceptable.
Passerelle interdomaine	Une forme d'interface contrôlée qui permet de transférer automatiquement des renseignements sur la cybersécurité entre divers domaines de sécurité.
Point terminal	Un point terminal est un appareil informatique à distance qui effectue des transmissions bilatérales avec un réseau auquel il est connecté. Les ordinateurs portatifs et de bureau, les téléphones mobiles, les tablettes électroniques, les serveurs et les environnements virtuels peuvent tous être considérés comme des points terminaux.

Terme	Définition
Projet complexe	Les projets complexes se distinguent par leurs nombreux éléments sociaux et techniques de niveaux différents, qui sont interconnectés et interdépendants. Contrairement aux projets plus simples, qui constituent des entreprises normalisées et clairement définies au sein d'environnements prévisibles et stables, les projets complexes comportent généralement un degré important d'incertitude quant à la définition des objectifs ultimes. De plus, ils sont souvent réalisés au sein d'un environnement changeant et peuvent nécessiter l'apport de multiples intervenants.
Relation contractuelle	Une lettre de soutien d'un membre d'une coentreprise serait une preuve acceptable d'une relation contractuelle.
Réseau de GI-TI complexe	Les réseaux de GI-TI dits « complexes » ont des propriétés distinctes qui découlent des interactions des *systèmes complexes* qu'ils comprennent, comme de l'équipement d'envergure, réparti à travers le monde, *dynamique*, *souple* et *hétérogène* (combinaison d'équipement ancien et moderne, divers fournisseurs), des applications *hétérogènes* (versions, licences et fournisseurs différents), des sources de données *hétérogènes* (structurées et non structurées), de systèmes *autoréparateurs* (conçus pour être toujours en ligne et fonctionnel), une connectivité intermittente, une faible latence et une bande passante étroite (p. ex. des communications satellites [mbit/s], navires [kbit/s], etc.).
Réseaux de commandement et contrôle (C2)	De façon générique, le terme « commandement et contrôle (C2) » désigne un processus (mais non pas les systèmes, contrairement à la croyance répandue) que les preneurs de décisions de cybersécurité, y compris les organisations responsables de la prise de décisions, emploient pour planifier, diriger, coordonner et commander les actifs cybernétiques et les ressources de leurs propres équipes en vue d'assurer le fonctionnement organisationnel sans heurts ainsi que la continuité et le succès de leur mission.
Sécurité multiniveaux	Le concept du traitement de l'information selon diverses classifications et catégories qui permettent l'accès par des utilisateurs possédant des autorisations de sécurité différentes tout en interdisant l'accès à ceux qui ne possèdent pas une telle autorisation.
Souplesse	La capacité de s'adapter, ou d'apporter des rectifications ou des modifications selon la situation.
Soutien de troisième (3^{e}) ligne	Capacités de soutien fournies à une force militaire au sein d'un théâtre d'opérations ou à des installations établies le long des lignes de communication stratégiques.

Terme	Définition
Système complexe	Les systèmes complexes sont des systèmes dont le comportement est intrinsèquement difficile à modéliser en raison des dépendances, de la concurrence, des liens ou d'autres types d'interactions entre leurs composants ou entre un système donné et son environnement. Les systèmes dits « complexes » ont des propriétés distinctes qui découlent de ces liens, comme la non-linéarité, l'émergence d'éléments, le classement spontané, l'adaptation, des boucles de commandes, etc.
Système de détection des intrusions	Un service de sécurité qui surveille et analyse les événements réseau ou système dans le but de détecter des tentatives d'accès non autorisées aux ressources du système réalisées par l'entremise d'un logiciel ou d'un dispositif matériel, et de fournir des avertissements à cet égard, le tout en temps réel ou quasi réel. Ce service est mis en œuvre sur l'hôte ou sur le réseau conjointement à une activité de surveillance qui est associée à l'intrusion ou à l'utilisation interne malveillante, ou les deux.
Système de protection contre les intrusions	Logiciel ou dispositif matériel qui possède toutes les capacités d'un système de détection des intrusions, mais qui tente également de prévenir les incidents possibles tels que des activités indésirables qui perturbent les opérations.
Temps quasi réel	Qualificatif appliqué à l'acheminement des données ou des informations qui s'effectue sans délai si ce n'est celui du traitement automatique et de la transmission électronique. Par conséquent, le délai dépend des capacités du support employé pour transmettre les données.

Annexe B : Exigences relatives à la sécurité

Les trois sections suivantes décrivent en détail les exigences de sécurité pour chaque étape du processus d'achat, y compris le contrat. Il s'agit des exigences de sécurité prévues en fonction des listes de vérification des exigences relatives à la sécurité (LVERS) incluses dans la présente annexe. Le Canada se réserve le droit de modifier les exigences de sécurité, au besoin.

1.1 Exigences de sécurité pour l'ISQ

a) L'ISQ ne comporte aucune exigence relative à la sécurité.

b) Il n'est pas nécessaire qu'un fournisseur détienne une cote de sécurité pour devenir un fournisseur qualifié.

c) Il y a des exigences de sécurité pour la phase de diligence raisonnable, la DP et le contrat.

d) À titre d'information, les fournisseurs doivent prendre note que le processus d'obtention des niveaux d'autorisation de sécurité exigés peut être long et qu'il dépend du niveau de sécurité requis. La responsabilité d'obtenir ces attestations de sécurité incombe entièrement aux fournisseurs.

Les fournisseurs qui ne détiennent pas actuellement les attestations de sécurité du personnel et les attestations de sécurité de l'organisation auprès du gouvernement fédéral canadien, ou encore, les fournisseurs qui ne respectent pas les exigences relatives à la sécurité prévues qui sont décrites dans les sections 1.2 et 1.3 devraient entreprendre tôt le processus d'obtention de l'attestation de sécurité en communiquant avec les responsables du Programme de la sécurité industrielle indiqué sur le site Web de TPSGC (https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html).

1.2 Exigences de sécurité pour la phase 3 – Diligence raisonnable et la phase 4 – DP

Les exigences de sécurité suivantes (listes de vérification des exigences relatives à la sécurité [LVERS] et les clauses connexes prévues par le Programme de sécurité des contrats) s'appliquent à la phase de diligence raisonnable et à la phase de la DP et sont requises pour y participer pleinement. Les fournisseurs préqualifiés qui ne satisfont pas à ces exigences en matière de sécurité à la date de publication de la DP définitive seront retirés de la liste des fournisseurs qualifiés.

1.2.1 EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:

DOSSIER TPSGC Nº W6369-20-CY06 / DP

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une cote de sécurité d'installation valable au niveau NATO SECRET, ainsi qu'une: cote de protection des documents approuvée au niveau SECRET et NATO SECRET, délivrées par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC).
2. Ce contrat comprend un accès à des marchandises contrôlées. Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées de Travaux publics et Services gouvernementaux Canada (TPSGC).
3. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ en vigueur, délivrée ou approuvée par le PSC, TPSGC
4. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS ou PROTEGÉS portant la mention "CITOYENS CANADIENS SEULEMENT", dont l'accès est réglementé, **doivent être citoyens du Canada** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.
5. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS CANADIENS RESTREINTS ou PROTÉGÉS CANADIENS RESTREINTS, ou à des établissements dont l'accès est réglementé, **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande**, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.
6. Les membres du personnel de l'entreprise qui doivent avoir accès aux biens ou aux renseignements OTAN NON-CLASSIFIÉS **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande**, mais n'ont pas besoin d'avoir une attestation de sécurité ; toutefois,

l'entrepreneur doit s'assurer que de tiers n'auront pas accès aux renseignements OTAN NON-CLASSIFIÉS et que le principe du « besoin de savoir », sera appliqué.

7. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens NATO DIFFUSION RESTREINTE **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande** et doivent TOUS détenir une cote de FIABILITÉ ou son équivalent en vigueur, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

8. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS OTAN, ou à des établissements dont l'accès est réglementé **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande**, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau NATO SECRET, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

9. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS ÉTRANGERS ou PROTÉGÉS ÉTRANGERS, ou à des établissements dont l'accès est réglementé, **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande,** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

10. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens COMSEC**, doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande** et détenir une cote de sécurité du personnel valable proportionné avec les renseignements ou les biens qui seront accédés, avoir un besoin de connaitre et ont été soumis à une séance d'information COMSEC et ont signé un certificat de séance d'information COMSEC. L'accès par des étrangers, nationaux ou des résidents étrangers doit être approuvé par les Services à la Clientèle Chef de TI à CSTC sur une base de cas-par-cas.

11. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données au niveau CLASSIFIÉS/PROTÉGÉS tant que le PSC, TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau NATO SECRET et compris un lien électronique au niveau NATO SECRET.

12. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent pas être attribués sans l'autorisation écrite préalable du PSC, TPSGC

13. Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la **Participation, le contrôle et l'influence étrangers (PCIE)** ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut accéder, sans en avoir l'autorisation, à des biens ou à des renseignements **COMSEC, CLASSIFÉS DE**

L'OTAN ou CLASSIFÉS ÉTRANGERS. Travaux publics et Services gouvernementaux Canada (TPSGC) déterminera si le statut « Sans PCIE » ou « Avec PCIE » doit être attribué à l'entreprise de l'entrepreneur. Si le statut « Avec PCIE » est attribué à l'entreprise, TPSGC déterminera si des mesures d'atténuation existent ou doivent être prises par l'entreprise afin qu'elle puisse obtenir le statut « Sans PCIE par atténuation ».

14. En permanence pendant l'exécution du contrat, l'entrepreneur doit détenir une lettre de TPSGC indiquant les résultats de l'évaluation de la PCIE ainsi que le statut attribué à son entreprise, c'est-à-dire « Sans PCIE » ou « Sans PCIE par atténuation ».

15. Tout changement au questionnaire et aux facteurs connexes d'évaluation de la PCIE doit être immédiatement signalé au Secteur de la sécurité industrielle (SSI) aux fins de détermination de l'incidence du changement sur le statut lié à la PCIE.

16. L'entrepreneur ou l'offrant doit respecter les dispositions :

    a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe B;
    b) du Manuel de la sécurité industrielle (dernière édition).

1.2.2 EXIGENCES EN MATIÈRE DE SÉCURITÉ POUR LES ENTREPRENEURS POUR UN DP

NUMERO DE DOSSIER DE SPAC : W6369-20-CY06 / RFP

Pour l'échange d'informations classifiées du Canada, L'entrepreneur et les sous-traitants doivent être dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational, ou qui possèderont un tel instrument avec le Canada avant la fin de la période de soumission. Le programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de SPAC: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-fra.html Pour l'échange d'information de l'OTAN **l'entrepreneur / offrant / sous-traitant** doit être un membre de l'OTAN en règle.

Tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis **à l'entrepreneur / à l'offrant / au sous-traitant** étranger destinataire doivent être protégés comme suit:

1. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution **du contrat/de l'offre à commandes/du contrat de sous-traitance**, détenir une Attestation de sécurité d'installation valide, délivrée par l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur**, d'un niveau équivalent à **SECRET et NATO SECRET**, et posséder une Cote de protection de documents de niveau **SECRET et NATO SECRET** conformément aux législations, règlements, et politiques nationales **du pays du fournisseur.**

2. Dans l'éventualité du retrait de la partie destinataire ou à la fin **du contrat/de l'offre à commandes/du contrat de sous-traitance**, tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis ou produits en vertu **du présent contrat/de la présente offre à commandes/du présent contrat de sous-traitance** continueront d'être protégés, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

3. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire assurera une protection des renseignements et des biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'Autorité nationale de sécurité (ANS) ou par l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur**.

4. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit attribuer à tous les renseignements et biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** qui lui sont fournis par le gouvernement du Canada en vertu **du présent contrat/de la présente offre à commandes/du présent contrat de sous-traitance** la cote de sécurité équivalente utilisée par **le pays du fournisseur**, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

5. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution **du contrat/de l'offre à commandes/du contrat de sous-traitance** veiller à ce que le transfert des renseignements et des biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** soit effectué conformément aux législations, règlements, et politiques nationales **du pays du fournisseur** et aux dispositions du Protocole d'entente bilatérale sur la sécurité industrielle signé par **le pays du fournisseur** et le Canada.

6. À la fin des travaux, **l'entrepreneur/l'offrant/le sous-traitant** étranger destinataire doit restituer au gouvernement du Canada, par l'entremise des circuits officiels, tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** qu'il aura reçu ou produit en vertu **du présent contrat/de la présente offre à commandes/du présent contrat de sous-traitance**, y compris tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** remis à ses sous-traitants ou produits par eux **sauf autrement autorisé au préalable écrite par l'ADS du Canada**.

7. Les Canadiens qui examinent, possèdent ou transfèrent des marchandises contrôlées (*voir la remarque) qui sont soumises à un contrôle domestique par Services publics et Approvisionnement Canada (SPAC) dans le cadre de marchés ou de marchés de sous-traitance doivent s'inscrire auprès du Programme des marchandises contrôlées (PMC) de SPAC avant d'avoir accès aux marchandises contrôlées, sauf s'ils sont exemptés de l'inscription auprès du PMC en vertu du *Règlement sur les*

marchandises contrôlées.

Pendant toute la durée du présent **contrat et du présent contrat de sous-traitance, l'entrepreneur et le sous-traitant étrangers** destinataires doivent se conformer à leurs politiques nationales respectives concernant l'examen, la possession ou le transfert des marchandises contrôlées et doivent immédiatement signaler à leur Autorité nationale de sécurité (ANS) responsable tous les cas dans lesquels ils savent ou ont lieu de croire que des marchandises contrôlées fournies ou produites aux termes **de ce contrat et de ce contrat** de sous-traitance ont été perdues ou divulguées à des personnes non autorisées (entités non inscrites auprès du PMC ou entités non exemptées de l'inscription auprès du PMC), notamment à une entité tierce, qu'il s'agisse d'un gouvernement, d'un individu d'une entreprise ou de ses représentants. La perte ou la compromission de marchandises contrôlées lors de leur traitement à l'extérieur du Canada devrait être signalée immédiatement, conformément aux exigences de la Directive sur les marchandises contrôlées et de la Directive sur la gestion du matériel du Secrétariat du Conseil du Trésor du Canada, et à l'autorité gouvernementale canadienne propriétaire des marchandises contrôlées, par exemple le ministère canadien qui a émis les marchandises contrôlées à l'entrepreneur et au sous-traitant étranger destinataire dans le cadre **de ce contrat et de ce contrat** de sous-traitance. De plus, si des marchandises contrôlées sont perdues ou divulguées à des personnes non autorisées qui sont assujetties à l'International Traffic in Arms Regulations des États-Unis, l'ANS ou l'autorité gouvernementale canadienne propriétaire des marchandises contrôlées devra signaler la situation à l'exportateur américain ou au Directorate of Defense Trade Controls (DDTC) du département d'État des États-Unis de l'Amerique.

* Remarque : Les marchandises contrôlées sont des marchandises, y compris les composants et les technologies connexes (p. ex. les plans, les spécifications techniques, etc.), qui revêtent une importance militaire ou pour la sécurité nationale, y compris les « articles de défense » qui sont régis par l'International Traffic in Arms Regulations des États-Unis. La Liste des marchandises contrôlées figurant à l'Annexe de la Loi sur la production de défense (article 35) détaille les marchandises contrôlées particulières qui font l'objet d'un contrôle interne par SPAC.

8. Les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** doivent être divulgués uniquement aux **de l'Australie, des États-Unis d'Amérique, du Royaume Uni, de Nouvelle Zélande, et du Canada,** doivent être divulgués uniquement aux membres du personnel employés par le destinataire étranger dans le cadre **du contrat / de l'offre à commandes / du contrat de sous-traitance** qui en ont besoin pour exécuter **le contrat / l'offre à commandes / le contrat de sous-traitance**. Ces membres du personnel doivent être des citoyens **de l'Australie, des États-Unis d'Amérique, du Royaume Uni, de Nouvelle Zélande, et/ou un citoyen canadien,** et doivent tous être titulaires d'une Attestation de sécurité du personnel valide de niveau **SECRET OU NATO SECRET**, exigée, délivrée ou approuvée par l'Autorité nationale de sécurité (ANS) ou par

l'Autorité désignée en matière de sécurité (ADS) de leur pays respectif, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

9. Les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** doivent être divulgués uniquement aux membres du personnel **de l'entrepreneur / de l'offrant / du sous-traitant** étranger destinataire qui en ont besoin pour exécuter **le contrat / l'offre à commandes / le contrat de sous-traitance** et qui sont titulaires d'une Attestation de sécurité du personnel de niveau **SECRET OU NATO SECRET**, accordée par l'Autorité nationale de sécurité (ANS) ou par l'Autorité désignée en matière de sécurité (ADS) du pays du fournisseur, conformément aux législations, règlements, et politiques nationales du {nom du pays}.

10. **L'entrepreneur / L'offrant / Le sous-traitant** étrangers destinataires ne doivent pas accéder aux renseignements et aux biens appartenant à la catégorie NATO DIFFUSION RESTREINTE, sans avoir au préalable consulté leur administration nationale de la sécurité ou leur Autorité désignée en matière de sécurité respective, au sujet des mesures de protection qu'il convient de prendre conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

11. Les membres du personnel **de l'entrepreneur / de l'offrant / du sous-traitant** étranger destinataire qui doivent avoir accès aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN**, n'ont pas besoin de cote de sécurité accordée par leur Autorité nationale de sécurité (ANS) ou leur Autorité désignée en matière de sécurité (ADS). Toutefois, **l'entrepreneur / l'offrant / le sous-traitant** étranger destinataire doit s'assurer qu'aucun tiers n'aura accès aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN** et que le principe du « besoin de savoir » sera appliqué au personnel accédant à l'information/bien. Aux fins de cette disposition, le principe du « besoin de savoir » signifie que l'ANS ou que l'ADS a établi hors de tout doute qu'un éventuel destinataire de renseignements/biens **NON-CLASSIFIÉS de l'OTAN** doit avoir accès aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN**, en avoir connaissance ou les posséder afin d'exécuter les services et les tâches requises en vertu **du contrat / de l'offre à commandes / du contrat de sous-traitance**. **Les contrats / Les offres à commandes / Les contrats de sous-traitance** comportant des exigences relatives aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN** NE DOIVENT PAS être attribués **sans l'autorisation écrite de l'ADS du Canada**.

12. Les membres du personnel **de l'entrepreneur / de l'offrant / du sous-traitant** étranger destinataire devant avoir accès à des renseignements/biens de niveau **OTAN CONFIDENTIEL ou plus haut** ou à des établissements de travail dont l'accès est réglementé doivent tous détenir une cote de sécurité du personnel valable au niveau **NATO SECRET** doivent avoir été autorisés, informés et approuvés par leur autorité de sécurité compétente de l'OTAN respective.

13. Les renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis ou produits dans le cadre **du présent contrat/de la présente offre à commandes/du présent contrat**

de sous-traitance ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:

a. l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) de l'autre sous-traitant étranger destinataire atteste par écrit que ce dernier a obtenu l'approbation d'accès aux renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** par l'intermédiaire de son ANS ou de son ADS;

b. l'ANS ou l'ADS **du pays du fournisseur** donne son autorisation écrite lorsque l'autre sous-traitant destinataire étranger est situé dans un autre pays.

14. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) concernée, conformément aux législations, règlements, et politiques nationales du {nom du pays} / ADS canadienne}.

15. Un compte de Sécurité des communications (SÉCOM) de niveau **SECRET** doit être octroyé et approuvé par l'Autorité nationale de la sécurité des communications (ANSC) **du pays du fournisseur. L'entrepreneur / L'offrant / Le sous-traitant** qui a besoin d'accéder à du matériel SÉCOM responsable (MSR) et/ou à des renseignements ou à des biens SÉCOM doit être citoyen **du pays du fournisseur**, être titulaire d'une Attestation de sécurité du personnel valide correspondant aux renseignements ou aux biens auxquels il aura accès, avoir un « besoin de connaître », avoir assisté à un exposé sur la SÉCOM et avoir signé une attestation d'initiation SÉCOM. L'accès par des ressortissants étrangers ou **« étrangers résidants »** doit être approuvé par l'ANSC du pays du fournisseur, au cas par cas. Ces approbations doivent être transmises par écrit à l'administration désignée en matière de sécurité (ADS) du Canada.

16. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou conserver dans un système informatique des renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** avant que l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur** lui en donne le droit. Une fois que **l'entrepreneur / l'offrant / le sous-traitant** étranger destinataire a reçu cette approbation écrite, il peut effectuer ces tâches jusqu'au niveau **SECRET ET NATO SECRET**.

17. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements /biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** pour répondre à des besoins distincts de l'exécution **du contrat/de l'offre à commandes/du contrat de sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS du Canada.

18. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire visitant des sites gouvernementaux ou industriels canadiens dans le cadre du contrat doit soumettre pour approbation une demande

de visite à l'administration désignée en matière de sécurité (ADS) du Canada, par l'entremise de son Autorité nationale de la sécurité (ANS) ou son Autorité désignée en matière de sécurité (ADS).

19. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait ou il a lieu de croire que des renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** obtenus dans le cadre **du présent contrat / de la présente offre à commandes / du présent contrat de sous-traitance** ont été compromis.

20. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit immédiatement signaler à son Autorité nationale de la sécurité (ANS) ou à son Autorité désignée en matière de sécurité (ADS) tous les cas dans lesquels il sait ou il a lieu de croire que des renseignements /biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis ou produits par **l'entrepreneur / l'offrant / le sous-traitant** étranger destinataire conformément **au présent contrat / à la présente offre à commandes / au présent contrat de sous-traitance** ont été perdus ou divulgués à des personnes non autorisées.

21. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'intermédiaire de l'Autorité nationale de la sécurité (ANS) ou de l'Autorité désignée en matière de sécurité (ADS) du destinataire.

22. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit respecter les dispositions énoncées dans le protocole d'entente bilatéral en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational conclu entre **du pays du fournisseur** et le Canada pour déterminer les niveaux d'équivalence.

23. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'Annexe B.

24. Si un **entrepreneur / offrant / sous-traitant** étranger destinataire est choisi comme fournisseur dans le cadre de ce contrat, des clauses de sécurité propres a son pays seront établies et mises on œuvre par l'ADS canadienne; ces clauses seront fournies à l'autorité contractante du gouvernement du Canada, afin de respecter les dispositions de sécurité relatives aux équivalences établies par l'ADS canadienne.

1.3 Exigences de sécurité pour la phase 5 – Contrat

a) Les exigences de sécurité suivantes (listes de vérification des exigences relatives à la sécurité [LVERS] et les clauses connexes prévues par le Programme de sécurité des contrats) s'appliquent au contrat.

1.3.1 EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:

DOSSIER TPSGC No W6369-20-CY06 / CONTRACT

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une cote de sécurité d'installation valable au niveau TRÈS SECRET et NATO SECRET, ainsi qu'une cote de protection des documents au niveau TOP SECRET et NATO SECRET délivrés par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC) et un compte COMSEC au niveau TOP SECRET, délivrée par la Centre de la sécurité des télécommunications Canada (CSTC).

2. Ce contrat comprend un accès à des marchandises contrôlées. Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées de Travaux publics et Services gouvernementaux Canada (TPSGC).

3. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTEGÉS CANADIENS NON RESTREINTS, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ, délivrée ou approuvée par le PSC, TPSGC.

4. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTEGÉS portant la mention "CITOYENS CANADIENS SEULEMENT", dont l'accès est réglementé, **doivent être citoyens du Canada** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITÉ, délivrée ou approuvée par le PSC, TPSGC.

5. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS CANADIENS RESTREINTS ou PROTÉGÉS CANADIENS RESTREINTS, ou à des établissements dont l'accès est réglementé, **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande, et** doivent TOUS détenir une cote de sécurité du personnel valable au niveau TRÈS SECRET, SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

6. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens TRÈS SECRET SIGINT, ou à des établissements dont l'accès est réglementé, **doivent être citoyens du Canada** et doivent TOUS détenir une cote de sécurité du personnel valable au niveau TRÈS SECRET SIGINT, délivrée par le Programme de sécurité des contrats (PSC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

7. Les membres du personnel de l'entreprise qui doivent avoir accès aux biens ou aux renseignements

OTAN NON-CLASSIFIÉS **doivent être citoyens du Canada, États-Unis ou Royaume-Unis**, mais n'ont pas besoin d'avoir une attestation de sécurité ; toutefois, l'entrepreneur doit s'assurer que de tiers n'auront pas accès aux renseignements OTAN NON-CLASSIFIÉS et que le principe du « besoin de savoir », sera appliqué.

8. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens **NATO DIFFUSION RESTREINTE**, **doivent être citoyens du Canada, États-Unis ou Royaume-Unis,** et doivent TOUS détenir une cote de FIABILITÉ ou son équivalent en vigueur, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

9. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens **CLASSIFIÉS OTAN**, ou à des établissements dont l'accès est réglementé, **doivent être citoyens du Canada, États-Unis ou Royaume-Unis**, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau NATO SECRET, délivrée ou approuvée par l'autorité de sécurité compétente déléguée par l'OTAN.

10. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens CLASSIFIÉS ÉTRANGERS ou PROTÉGÉS ÉTRANGERS, ou à des établissements dont l'accès est réglementé, **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande**, et doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITÉ, tel que requis, délivrée ou approuvée par le PSC, TPSGC.

11. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens COMSEC, **doivent être citoyens du Canada, États-Unis, Royaume-Uni, Australie ou Nouvelle Zélande** et détenir une cote de sécurité du personnel valable proportionné avec les renseignements ou les biens qui seront accédés, avoir un besoin de connaitre et ont été soumis à une séance d'information COMSEC et ont signé un certificat de séance d'information COMSEC. L'accès par des étrangers, nationaux ou des résidents étrangers doit être approuvé par les Services à la Clientèle Chef de TI à CSTC sur une base de cas-par-cas.

12. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données au niveau CLASSIFIÉS/PROTÉGÉS tant que le PSC, TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau NATO SECRET et compris un lien électronique au niveau NATO SECRET.

13. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent pas être attribués sans l'autorisation écrite préalable du PSC, TPSGC.

14. Avant l'attribution du contrat, l'entrepreneur doit remplir un questionnaire sur la **Participation, le contrôle et l'influence étrangers (PCIE)** ainsi que les documents connexes indiqués dans les lignes directrices sur la PCIE destinées aux organisations. L'entrepreneur doit soumettre ces documents dûment remplis afin d'indiquer si une tierce partie (personne, entreprise ou gouvernement) peut

accéder, sans en avoir l'autorisation, à des biens ou à des renseignements **COMSEC, CLASSIFÉS DE L'OTAN ou CLASSIFÉS ÉTRANGERS**. Travaux publics et Services gouvernementaux Canada (TPSGC) déterminera si le statut « Sans PCIE » ou « Avec PCIE » doit être attribué à l'entreprise de l'entrepreneur. Si le statut « Avec PCIE » est attribué à l'entreprise, TPSGC déterminera si des mesures d'atténuation existent ou doivent être prises par l'entreprise afin qu'elle puisse obtenir le statut « Sans PCIE par atténuation ».

15. En permanence pendant l'exécution du contrat, l'entrepreneur doit détenir une lettre de TPSGC indiquant les résultats de l'évaluation de la PCIE ainsi que le statut attribué à son entreprise, c'est-à-dire « Sans PCIE » ou « Sans PCIE par atténuation ».

16. Tout changement au questionnaire et aux facteurs connexes d'évaluation de la PCIE doit être immédiatement signalé au Secteur de la sécurité industrielle (SSI) aux fins de détermination de l'incidence du changement sur le statut lié à la PCIE.

17. L'entrepreneur ou l'offrant doit respecter les dispositions :

    a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe B;

    b) du Manuel de la sécurité industrielle (dernière édition) et du Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein des entreprises du secteur privé canadien (ITSD-06A).

1.3.2 EXIGENCES EN MATIÈRE DE SÉCURITÉ POUR LES ENTREPRENEURS

NUMERO DE DOSSIER DE SPAC : W6369-20-CY06 / CONTRACT

Pour l'échange d'informations classifiées du Canada, L'entrepreneur et les sous-traitants doivent être dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational, ou qui possèderont un tel instrument avec le Canada avant la fin de la période de soumission. Le programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de SPAC: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-fra.html Pour l'échange d'information de l'OTAN **l'entrepreneur / offrant / sous-traitant** doit être un membre de l'OTAN en règle.

Tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis **à l'entrepreneur / à l'offrant / au sous-traitant** étranger destinataire doivent être protégés comme suit:

1. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution **du contrat/de l'offre à commandes/du contrat de sous-traitance**, détenir une Attestation de sécurité d'installation valide, délivrée par l'Autorité nationale de la sécurité (ANS) ou

l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur**, d'un niveau équivalent à **SECRET et NATO SECRET**, et posséder une Cote de protection de documents de niveau **SECRET, TOP SECRET, TOP SECRET SIGINT et NATO SECRET** conformément aux législations, règlements, et politiques nationales **du pays du fournisseur.**

2. Dans l'éventualité du retrait de la partie destinataire ou à la fin **du contrat/de l'offre à commandes/du contrat de sous-traitance**, tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis ou produits en vertu **du présent contrat/de la présente offre à commandes/du présent contrat de sous-traitance** continueront d'être protégés, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

3. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire assurera une protection des renseignements et des biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'Autorité nationale de sécurité (ANS) ou par l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur**.

4. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit attribuer à tous les renseignements et biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** qui lui sont fournis par le gouvernement du Canada en vertu **du présent contrat/de la présente offre à commandes/du présent contrat de sous-traitance** la cote de sécurité équivalente utilisée par **le pays du fournisseur**, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

5. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution **du contrat/de l'offre à commandes/du contrat de sous-traitance** veiller à ce que le transfert des renseignements et des biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** soit effectué conformément aux législations, règlements, et politiques nationales **du pays du fournisseur** et aux dispositions du Protocole d'entente bilatérale sur la sécurité industrielle signé par **le pays du fournisseur** et le Canada.

6. À la fin des travaux, **l'entrepreneur/l'offrant/le sous-traitant** étranger destinataire doit restituer au gouvernement du Canada, par l'entremise des circuits officiels, tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** qu'il aura reçu ou produit en vertu **du présent contrat/de la présente offre à commandes/du présent contrat de sous-traitance**, y compris tous les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** remis à ses sous-traitants ou produits par eux **sauf autrement autorisé au préalable écrite par l'ADS du Canada**.

7. Les Canadiens qui examinent, possèdent ou transfèrent des marchandises contrôlées (*voir la remarque) qui sont soumises à un contrôle domestique par Services publics et Approvisionnement Canada (SPAC) dans le cadre de marchés ou de marchés de sous-traitance doivent s'inscrire auprès du Programme des marchandises contrôlées (PMC) de SPAC avant d'avoir accès aux marchandises contrôlées, sauf s'ils sont exemptés de l'inscription auprès du PMC en vertu du *Règlement sur les marchandises contrôlées*.

   Pendant toute la durée du présent **contrat et du présent contrat de sous-traitance, l'entrepreneur et le sous-traitant étrangers** destinataires doivent se conformer à leurs politiques nationales respectives concernant l'examen, la possession ou le transfert des marchandises contrôlées et doivent immédiatement signaler à leur Autorité nationale de sécurité (ANS) responsable tous les cas dans lesquels ils savent ou ont lieu de croire que des marchandises contrôlées fournies ou produites aux termes **de ce contrat et de ce contrat** de sous-traitance ont été perdues ou divulguées à des personnes non autorisées (entités non inscrites auprès du PMC ou entités non exemptées de l'inscription auprès du PMC), notamment à une entité tierce, qu'il s'agisse d'un gouvernement, d'un individu d'une entreprise ou de ses représentants. La perte ou la compromission de marchandises contrôlées lors de leur traitement à l'extérieur du Canada devrait être signalée immédiatement, conformément aux exigences de la Directive sur les marchandises contrôlées et de la Directive sur la gestion du matériel du Secrétariat du Conseil du Trésor du Canada, et à l'autorité gouvernementale canadienne propriétaire des marchandises contrôlées, par exemple le ministère canadien qui a émis les marchandises contrôlées à l'entrepreneur et au sous-traitant étranger destinataire dans le cadre **de ce contrat et de ce contrat** de sous-traitance. De plus, si des marchandises contrôlées sont perdues ou divulguées à des personnes non autorisées qui sont assujetties à l'International Traffic in Arms Regulations des États-Unis, l'ANS ou l'autorité gouvernementale canadienne propriétaire des marchandises contrôlées devra signaler la situation à l'exportateur américain ou au Directorate of Defense Trade Controls (DDTC) du département d'État des États-Unis de l'Amerique.

   * Remarque : Les marchandises contrôlées sont des marchandises, y compris les composants et les technologies connexes (p. ex. les plans, les spécifications techniques, etc.), qui revêtent une importance militaire ou pour la sécurité nationale, y compris les « articles de défense » qui sont régis par l'International Traffic in Arms Regulations des États-Unis. La Liste des marchandises contrôlées figurant à l'Annexe de la Loi sur la production de défense (article 35) détaille les marchandises contrôlées particulières qui font l'objet d'un contrôle interne par SPAC.

8. Les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** doivent être divulgués uniquement aux **de l'Australie, des États-Unis d'Amérique, du Royaume Uni, de Nouvelle Zélande, et du Canada,** doivent être divulgués uniquement aux membres du personnel employés par le destinataire étranger dans le cadre **du contrat / de l'offre à commandes / du contrat de sous-traitance** qui en ont besoin pour exécuter **le contrat / l'offre à commandes / le**

contrat de sous-traitance. Ces membres du personnel doivent être des citoyens **de l'Australie, des États-Unis d'Amérique, du Royaume Uni, de Nouvelle Zélande, et/ou un citoyen canadien,** et doivent tous être titulaires d'une Attestation de sécurité du personnel valide de niveau **SECRET OU NATO SECRET**, exigée, délivrée ou approuvée par l'Autorité nationale de sécurité (ANS) ou par l'Autorité désignée en matière de sécurité (ADS) de leur pays respectif, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

9. Les renseignements et les biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** doivent être divulgués uniquement aux membres du personnel **de l'entrepreneur / de l'offrant / du sous-traitant** étranger destinataire qui en ont besoin pour exécuter **le contrat / l'offre à commandes / le contrat de sous-traitance** et qui sont titulaires d'une Attestation de sécurité du personnel de niveau **SECRET OU NATO SECRET**, accordée par l'Autorité nationale de sécurité (ANS) ou par l'Autorité désignée en matière de sécurité (ADS) du pays du fournisseur, conformément aux législations, règlements, et politiques nationales du {nom du pays}.

10. **L'entrepreneur / L'offrant / Le sous-traitant** étrangers destinataires ne doivent pas accéder aux renseignements et aux biens appartenant à la catégorie NATO DIFFUSION RESTREINTE, sans avoir au préalable consulté leur administration nationale de la sécurité ou leur Autorité désignée en matière de sécurité respective, au sujet des mesures de protection qu'il convient de prendre conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.

11. Les membres du personnel **de l'entrepreneur / de l'offrant / du sous-traitant** étranger destinataire qui doivent avoir accès aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN**, n'ont pas besoin de cote de sécurité accordée par leur Autorité nationale de sécurité (ANS) ou leur Autorité désignée en matière de sécurité (ADS). Toutefois, **l'entrepreneur / l'offrant / le sous-traitant** étranger destinataire doit s'assurer qu'aucun tiers n'aura accès aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN** et que le principe du « besoin de savoir » sera appliqué au personnel accédant à l'information/bien. Aux fins de cette disposition, le principe du « besoin de savoir » signifie que l'ANS ou que l'ADS a établi hors de tout doute qu'un éventuel destinataire de renseignements/biens **NON-CLASSIFIÉS de l'OTAN** doit avoir accès aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN**, en avoir connaissance ou les posséder afin d'exécuter les services et les tâches requises en vertu **du contrat / de l'offre à commandes / du contrat de sous-traitance**. **Les contrats / Les offres à commandes / Les contrats de sous-traitance** comportant des exigences relatives aux renseignements/biens **NON-CLASSIFIÉS de l'OTAN** NE DOIVENT PAS être attribués **sans l'autorisation écrite de l'ADS du Canada**.

12. Les membres du personnel **de l'entrepreneur / de l'offrant / du sous-traitant** étranger destinataire devant avoir accès à des renseignements/biens de niveau **OTAN CONFIDENTIEL ou plus haut** ou à des établissements de travail dont l'accès est réglementé doivent tous détenir une cote de sécurité du personnel valable au niveau **NATO SECRET** doivent avoir été autorisés, informés et approuvés par leur autorité de sécurité compétente de l'OTAN respective.

13. Les renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis ou produits dans le cadre **du présent contrat/de la présente offre à commandes/du présent contrat de sous-traitance** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:

    a. l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) de l'autre sous-traitant étranger destinataire atteste par écrit que ce dernier a obtenu l'approbation d'accès aux renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** par l'intermédiaire de son ANS ou de son ADS;

    b. l'ANS ou l'ADS **du pays du fournisseur** donne son autorisation écrite lorsque l'autre sous-traitant destinataire étranger est situé dans un autre pays.

14. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) concernée, conformément aux législations, règlements, et politiques nationales du {nom du pays} / ADS canadienne}.

15. Un compte de Sécurité des communications (SÉCOM) de niveau **SECRET** doit être octroyé et approuvé par l'Autorité nationale de la sécurité des communications (ANSC) **du pays du fournisseur. L'entrepreneur / L'offrant / Le sous-traitant** qui a besoin d'accéder à du matériel SÉCOM responsable (MSR) et/ou à des renseignements ou à des biens SÉCOM doit être citoyen **du pays du fournisseur**, être titulaire d'une Attestation de sécurité du personnel valide correspondant aux renseignements ou aux biens auxquels il aura accès, avoir un « besoin de connaître », avoir assisté à un exposé sur la SÉCOM et avoir signé une attestation d'initiation SÉCOM. L'accès par des ressortissants étrangers ou **« étrangers résidants »** doit être approuvé par l'ANSC du pays du fournisseur, au cas par cas. Ces approbations doivent être transmises par écrit à l'administration désignée en matière de sécurité (ADS) du Canada.

16. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou conserver dans un système informatique des renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** avant que l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur** lui en donne le droit. Une fois que **l'entrepreneur / l'offrant / le sous-traitant** étranger destinataire a reçu cette approbation écrite, il peut effectuer ces tâches jusqu'au niveau **SECRET, TOP SECRET, TOP SECRET SIGINT ET NATO SECRET**.

17. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements /biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** pour répondre à des besoins distincts de l'exécution **du contrat/de l'offre à commandes/du contrat de sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS du Canada.

18. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire visitant des sites gouvernementaux ou industriels canadiens dans le cadre du contrat doit soumettre pour approbation une demande de visite à l'administration désignée en matière de sécurité (ADS) du Canada, par l'entremise de son Autorité nationale de la sécurité (ANS) ou son Autorité désignée en matière de sécurité (ADS).

19. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait ou il a lieu de croire que des renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** obtenus dans le cadre **du présent contrat / de la présente offre à commandes / du présent contrat de sous-traitance** ont été compromis.

20. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit immédiatement signaler à son Autorité nationale de la sécurité (ANS) ou à son Autorité désignée en matière de sécurité (ADS) tous les cas dans lesquels il sait ou il a lieu de croire que des renseignements /biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** fournis ou produits par **l'entrepreneur / l'offrant / le sous-traitant** étranger destinataire conformément **au présent contrat / à la présente offre à commandes / au présent contrat de sous-traitance** ont été perdus ou divulgués à des personnes non autorisées.

21. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **ÉTRANGER, NATO, CANADA PROTÉGÉ et CLASSIFIÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'intermédiaire de l'Autorité nationale de la sécurité (ANS) ou de l'Autorité désignée en matière de sécurité (ADS) du destinataire.

22. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit respecter les dispositions énoncées dans le protocole d'entente bilatéral en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational conclu entre **du pays du fournisseur** et le Canada pour déterminer les niveaux d'équivalence.

23. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'Annexe C.

24. Si un **entrepreneur / offrant / sous-traitant** étranger destinataire est choisi comme fournisseur dans le cadre de ce contrat, des clauses de sécurité propres a son pays seront établies et mises en œuvre par l'ADS canadienne; ces clauses seront fournies à l'autorité contractante du gouvernement du Canada, afin de respecter les dispositions de sécurité relatives aux équivalences établies par l'ADS canadienne.

25. Un compte de Sécurité des communications (SÉCOM) de niveau {insérer le niveau requis} doit être octroyé et approuvé par l'autorité nationale de la sécurité des communications (ANSC) du {nom du pays}. {L'entrepreneur / L'offrant / Le sous-traitant} qui a besoin d'accéder à du matériel SÉCOM

responsable (MSR) et/ou à des renseignements ou à des biens SÉCOM doit être citoyen de {nom du pays}, être titulaire d'une Attestation de sécurité du personnel valide correspondant aux renseignements ou aux biens auxquels il aura accès, avoir un « besoin de connaître », avoir assisté à un exposé sur la SÉCOM et avoir signé une attestation d'initiation SÉCOM. L'accès par des ressortissants étrangers ou {les agents de négociation des contrats doivent utiliser l'expression « étrangers résidants » dans le cas où le pays de l'entrepreneur étranger destinataire est les États-Unis} doit être approuvé par l'ANSC du {nom du pays}, au cas par cas. Ces approbations doivent être transmises par écrit à l'administration désignée en matière de sécurité (ADS) du Canada.

1.4 Listes de vérification des exigences relatives à la sécurité [LVERS]

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contra:
W6369-20-CY06-RFP

Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1 Originating Government Department or Organizati Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD/DPDCC
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

In this RFP phase, qualified suppliers will be required to access and store one or more classified Annexes that will be provided; information is classified up to SECRET and releasable only to Canadian citizens.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non	Yes / Oui ✓
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	No / Non ✓	Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non	Yes / Oui ✓
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	No / Non ✓	Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	No / Non ✓	Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ✓	NATO / OTAN ✓	Foreign / Étranger ✓

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion ✓	All NATO countries / Tous les pays de l'OTAN	No release restrictions / Aucune restriction relative à la diffusion
Not releasable / À ne pas diffuser ✓		
Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
FVEYs members only as applicable	FVEYs members only as applicable	FVEYs members only as applicable

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ✓	PROTECTED A / PROTÉGÉ A ✓
PROTECTED B / PROTÉGÉ B ✓	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ✓	PROTECTED B / PROTÉGÉ B ✓
PROTECTED C / PROTÉGÉ C	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET ✓	CONFIDENTIAL / CONFIDENTIEL
SECRET / SECRET ✓	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET ✓
TOP SECRET / TRÈS SECRET		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-RFP

Security Classification / Classification de sécurité
UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No / Non: ; Yes / Oui: ✓
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité: SECRET

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No / Non: ✓; Yes / Oui: ___
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel:
Document Number / Numéro du document:

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

✓ RELIABILITY STATUS / COTE DE FIABILITÉ	CONFIDENTIAL / CONFIDENTIEL	✓ SECRET / SECRET	TOP SECRET / TRÈS SECRET
TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	NATO CONFIDENTIAL / NATO CONFIDENTIEL	✓ NATO SECRET / NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET
SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux: _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No / Non: ✓; Yes / Oui:
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non:; Yes / Oui:
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No / Non:; Yes / Oui: ✓
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No / Non: ✓; Yes / Oui:
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No / Non: ✓; Yes / Oui:
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No / Non:; Yes / Oui: ✓
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No / Non: ✓; Yes / Oui:
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC				
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens	✓	✓		✓	✓		✓	✓	✓							
Production																
IT Media / Support TI					✓		✓		✓							
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

✓ No / Non — Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

✓ No / Non — Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-CONTRACT
Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD/DPDCC
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

In this Contract Award phase, the winning Bidder may require access to information that is collectively classified up to TOP SECRET - SIGINT as well as access to COMSEC assets, releasable to Canadian citizens only. The winning Bidder will also be required to store, process and exchange information with DND/CAF up to SECRET. Selected supplier personnel may also require access to designated restricted/classified areas and equipment to perform work as part of the contract fulfillment.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non	✓ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	✓ No / Non	Yes / Oui

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non	✓ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	✓ No / Non	Yes / Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?	✓ No / Non	Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ✓	NATO / OTAN ✓	Foreign / Étranger ✓

7. b) Release restrictions / Restrictions relatives à la diffusion

Canada	NATO / OTAN	Foreign / Étranger
No release restrictions / Aucune restriction relative à la diffusion ✓	All NATO countries / Tous les pays de l'OTAN	No release restrictions / Aucune restriction relative à la diffusion
Not releasable / À ne pas diffuser ✓		
Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓	Restricted to: / Limité à : ✓
Specify country(ies): / Préciser le(s) pays : FVEYS members only as applicable	Specify country(ies): / Préciser le(s) pays : CAN/UK/US members only as applicable	Specify country(ies): / Préciser le(s) pays : FVEYS members only as applicable

7. c) Level of information / Niveau d'information

Canada	NATO / OTAN	Foreign / Étranger
PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ✓	PROTECTED A / PROTÉGÉ A ✓
PROTECTED B / PROTÉGÉ B ✓	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ✓	PROTECTED B / PROTÉGÉ B ✓
PROTECTED C / PROTÉGÉ C	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET ✓	CONFIDENTIAL / CONFIDENTIEL
SECRET / SECRET ✓	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET ✓
TOP SECRET / TRÈS SECRET ✓		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ✓		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-CONTRACT
Security Classification / Classification de sécurité
UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No ☐ Yes ✓
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ Oui ✓
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité : TOP SECRET - SIGINT, SECRET

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No ✓ Yes ☐
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? — Non ✓ Oui ☐

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

✓ RELIABILITY STATUS / COTE DE FIABILITÉ	CONFIDENTIAL / CONFIDENTIEL	✓ SECRET / SECRET	✓ TOP SECRET / TRÈS SECRET
✓ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	NATO CONFIDENTIAL / NATO CONFIDENTIEL	✓ NATO SECRET / NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET
SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No ✓ Yes ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? — Non ✓ Oui ☐
If Yes, will unscreened personnel be escorted? — No ☐ Yes ☐
Dans l'affirmative, le personnel en question sera-t-il escorté? — Non ☐ Oui ☐

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No ☐ Yes ✓
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ Oui ✓

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No ☐ Yes ✓
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? — Non ☐ Oui ✓

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No ✓ Yes ☐
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? — Non ✓ Oui ☐

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No ☐ Yes ✓
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ Oui ✓

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No ☐ Yes ✓
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? — Non ☐ Oui ✓

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens	✓	✓			✓	✓	✓		✓		✓	✓			✓	✓
Production																
IT Media / Support TI	✓	✓			✓		✓		✓							
IT Link / Lien électronique	✓	✓			✓		✓		✓						✓	

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

✓ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

✓ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Annexe C: Formulaire de présentation de la réponse

<table>
<tr><th colspan="4">Invitation à se qualifier No. W6369-20CY06/A
Formulaire de présentation de la réponse</th></tr>
<tr><td>Dénomination sociale complète du répondant principal
Dans le cas d'une coentreprise, veuillez identifier tous les participants.</td><td colspan="3"></td></tr>
<tr><td rowspan="5">Représentant autorisé du répondant aux fins d'évaluation
(p. ex., pour des précisions)</td><td>Nom</td><td colspan="2"></td></tr>
<tr><td>Titre</td><td colspan="2"></td></tr>
<tr><td>Adress</td><td colspan="2"></td></tr>
<tr><td>Téléphone</td><td colspan="2"></td></tr>
<tr><td>Courriel</td><td colspan="2"></td></tr>
<tr><td colspan="4">Numéro d'entreprise – approvisionnement (NEA) du répondant principal _____

Veuillez consulter les instructions uniformisées de SPC. Il est à noter que le NEA donné doit correspondre à la dénomination sociale utilisée dans la réponse. Si ce n'est pas le cas, le répondant sera déterminé en fonction de la dénomination sociale fournie, et le répondant devra fournir le NEA qui correspond à cette dernière.</td></tr>
<tr><td rowspan="4">Si le répondant fournit une réponse à l'ISQ à titre de coentreprise, il doit en indiquer la dénomination sociale complète, l'adresse et le numéro d'entreprise – approvisionnement (le cas échant) de la coentreprise. [Le répondant ajoutera des lignes si la coentreprise compte plus de deux membres].</td><td colspan="3">Dénomination sociale complète du membre de la coentreprise :</td></tr>
<tr><td colspan="3">Adresse du membre de la coentreprise :</td></tr>
<tr><td colspan="3">Dénomination sociale complète du membre de la coentreprise :</td></tr>
<tr><td colspan="3">Adresse du membre de la coentreprise :</td></tr>
<tr><td rowspan="4">Anciens fonctionnaires

Pour en savoir davantage, veuillez consulter l'article des instructions uniformisées de SPC intitulé « Ancien fonctionnaire ».

Si la réponse provient d'une coentreprise, veuillez fournir cette information pour chacun des participants.</td><td rowspan="2">Le répondant est-il un ancien fonctionnaire recevant une pension selon la définition des instructions uniformisées de SPC? Si oui, veuillez fournir les renseignements requis à la section des instructions uniformisées de SPC intitulée « Ancien fonctionnaire ».</td><td>Oui</td><td></td></tr>
<tr><td>Non</td><td></td></tr>
<tr><td rowspan="2">Le répondant est-il un ancien fonctionnaire ayant reçu une somme forfaitaire en vertu de la Directive sur le réaménagement des effectifs? Si oui, veuillez fournir les renseignements requis à la section des instructions uniformisées de SPC intitulée « Ancien fonctionnaire ».</td><td>Oui</td><td></td></tr>
<tr><td>Non</td><td></td></tr>
<tr><td rowspan="8">Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation

Pour en savoir davantage, veuillez consulter la section des Instructions uniformisées de SPC intitulée « Programme de contrats fédéraux pour l'équité en matière d'emploi ».

Veuillez cocher l'une des cases ou fournir l'information demandée. S'il s'agit d'une réponse d'un consortium, veuillez fournir cette information pour chacun des membres.</td><td colspan="2">Le répondant atteste qu'il n'a aucun effectif au Canada.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il est un employeur du secteur public.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il est un employeur sous réglementation fédérale, assujetti à la Loi sur l'équité en matière d'emploi.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il a un effectif combiné de moins de 100 employés (à temps plein, temps partiel ou temporaires) au Canada.</td><td></td></tr>
<tr><td colspan="2">Le répondant a un effectif combiné de 100 employés (à temps plein, temps partiel ou temporaires) ou plus au Canada.</td><td></td></tr>
<tr><td colspan="2">Le numéro de certificat est valide et à jour.</td><td></td></tr>
<tr><td colspan="2">Le répondant atteste qu'il a présenté l'accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168) aux responsables du Programme du travail d'Emploi et Développement social Canada</td><td></td></tr>
<tr><td>Langue de communication future dans le cadre du processus d'approvisionnement – veuillez indiquer le français ou l'anglais</td><td colspan="3"></td></tr>
<tr><td>Province ou territoire canadien visé par la demande selon les lois en vigueur</td><td colspan="3"></td></tr>
</table>

Niveau de cote de sécurité du répondant Le nom dans l'attestation de sécurité doit correspondre à la dénomination sociale du répondant. Si ce n'est pas le cas, la cote de sécurité n'est pas valide pour le répondant.	Cote de sécurité	
	Date d'attribution	
	Entité émettrice (TPSGC, GRC, etc.)	
	Dénomination sociale de l'entité à qui la cote de sécurité a été attribuée	

En apposant ma signature ci-dessous, je confirme, au nom du répondant, que j'ai lu l'invitation à se qualifier en entier, y compris les documents intégrés par renvoi. J'atteste également ceci : 1. Le répondant considère qu'il possède les compétences et qu'il offre des produits répondant aux exigences obligatoires décrites dans l'IQ; 2. Tous les renseignements fournis sont exacts et complets; 3. Le répondant accepte de se conformer à toutes les modalités et conditions de la présente IQ, documents intégrés par renvoi compris.
Respondent Principal Authorization: Représentant autorisé du répondant
Nom:
Adresse:
Courriel:
Signature du représentant autorisé du répondant :
Téléphone:
Date:
Si le répondant fournit une réponse à l'ISQ à titre de coentreprise, il doit en indiquer la dénomination sociale complète, l'adresse et le numéro d'entreprise – approvisionnement (le cas échant) de la coentreprise. [Le répondant ajoutera des lignes si la coentreprise compte plus de deux membres].
Nom:
Adresse:
Courriel:
Signature du représentant autorisé du répondant :
Téléphone:
Date:
Si le répondant fournit une réponse à l'ISQ en tant qu'équipe de base du répondant, chaque membre de l'équipe de base doit remplir la section ci-dessous [Le répondant doit ajouter plus de lignes s'il y a plus de deux (2) membres de l'équipe de base]
Nom légal complet du membre de l'équipe de base:
Adresse de l'équipe de base:
Nom du représentant du membre de l'équipe de base:
Nom:
Adresse:
Courriel:
Signature du représentant autorisé du répondant :
Téléphone:
Date:

Annexe D : Processus d'approvisionnement agile et collaboratif

1.1 Introduction

a) Le Canada adopte une approche agile et collaborative relative au processus d'approvisionnement pour le projet CD-DAR en réunissant le gouvernement et l'industrie pour concevoir et améliorer l'approvisionnement de façon itérative afin d'obtenir des résultats.

b) La phase d'ISQ du projet CD-DAR ainsi que la phase de diligence raisonnable continueront de suivre un processus d'approvisionnement agile et collaboratif qui facilite un dialogue solide et une communication bilatérale, une rétroaction de qualité et la divulgation de renseignements jusqu'à la publication de la DP.

c) Le Canada reconnaît que la consultation et la collaboration tout au long d'un processus d'approvisionnement peuvent aider à réduire le fardeau global du retravail des soumissionnaires potentiels et aider les fournisseurs à obtenir un rendement raisonnable de leurs investissements, et que le processus global offre de généreuses retombées aux Canadiens.

1.2 Avant cette ISQ

a) Avant l'ISQ, le processus de collaboration au sein de l'industrie a commencé par la publication de lettres d'intérêt (LI) sur le site Achats et ventes en décembre 2016 pour les projets de sensibilisation à la cybersécurité (SC) et de cyberopérations défensives - aide à la décision (CD-AD) pour déterminer si une solution existante était disponible sur le marché. Les résultats des LI indiquaient qu'il n'existait pas de solution disponible dans le commerce, mais ils démontraient que l'industrie souhaitait vivement collaborer avec le MDN et les FAC pour répondre à ses besoins. Comme les résultats de la LI n'ont pas fourni suffisamment d'information au MDN pour faire avancer le projet, il a été déterminé qu'une demande de renseignements plus détaillée était nécessaire. Les numéros de dossier de CD-AD et de SC sont indiqués ci-dessous. Bien qu'ils soient maintenant inactifs, les deux sont accessibles sur le site Achats et ventes.

LI de CD-AD

Numéro de référence sur le site Achats et ventes : PW-$$QE-049-26100
Numéro de la demande de soumissions : W6369-17DE25/A

LI de SC

Numéro de référence sur le site Achats et ventes : PW-$$QE-049-26099
Numéro de la demande de soumissions : W6369-17DE26/A

b) Une DDR a été publiée en décembre 2017 sur le site achatsetventes.gc.ca dans le cadre du projet de CD-AD et a fourni davantage de renseignements sur le projet à l'industrie et a sollicité des

commentaires détaillés de l'industrie sur les exigences opérationnelles et techniques, les coûts, et le calendrier.

DDR de CD-AD

Numéro de référence sur le site Achats et ventes : PW-$$QE-049-26594
Numéro de la demande de soumissions : W6369-17DE25/B

c) Une journée de l'industrie non classifiée a été tenue en février 2018 pour présenter à l'industrie un aperçu des exigences et du processus de consultation prévu, et solliciter les commentaires de l'industrie. Les questions posées et les réponses données, et les commentaires découlant de ce dialogue avec les participants ont été affichés sur le site Achats et ventes.

d) À la suite de la journée de l'industrie, des réunions individuelles classifiées ont eu lieu en mars 2018 pour présenter et discuter l'annexe classifiée de la DDR de CD-AD. Tous les fournisseurs ont été invités à présenter une demande de réunion individuelle, les seuls critères étant qu'ils répondaient aux exigences de sécurité détaillées dans la DDR. Les questions et réponses classifiées ont été distribuées sur demande aux fournisseurs qui ont assisté aux réunions ou qui ont satisfait aux exigences de sécurité et ont demandé une copie dans les délais précisés dans la DDR. Toutes les questions et réponses non classifiées provenant des réunions individuelles ont été affichées sur le site Achats et ventes.

1.3 Pendant la phase d'ISQ

a) Ébauche de l'ISQ : Une ébauche de l'ISQ a été publié sur le site Achats et ventes, ce qui permettra à l'industrie de fournir des commentaires avant l'émission de l'ISQ finale. Les fournisseurs ont été invités à formuler des commentaires et à poser des questions par écrit sur l'ébauche de l'ISQ. Les réponses seront affichées sur le site Achats et ventes.

b) ISQ officielle : L'ISQ officielle sera affichée sur le site Achats et ventes. Il s'agit de la première étape du processus de qualification pour être admissible à soumissionner pour la DP dans le cadre du projet CD-DAR.

c) Les répondants devront soumettre leurs réponses avant l'heure et la date indiquées dans l'ISQ.

d) Le gouvernement du Canada (GC) informera les fournisseurs des résultats de l'évaluation.

1.4 Pendant la phase de diligence raisonnable

a) Le GC a l'intention de publier une ébauche complète de la DP, qui comprend un élément classifié, à l'intention des fournisseurs préqualifiés.

b) A l'intention de publier (tout en respectant les contraintes de la sécurité nationale) les éléments non classifiés de l'ébauche de la DP sur Achats et ventes au moyen d'une demande d'information (DI).

c) Afin d'obtenir des commentaires sur l'ébauche de la DP, le GC peut organiser une conférence des soumissionnaires classifiée et des réunions individuelles classifiées avec des fournisseurs préqualifiés.

d) Le cas échéant, le GC fournira de la rétroaction sur la façon dont il utilise ou non les commentaires reçus.

e) Le GC peut apporter des modifications aux exigences et aux modalités de la DP en fonction des commentaires de l'industrie.

f) Dans la mesure du possible, tout au long du processus, le GC prévoit répondre et publier les questions et réponses soumises par d'autres fournisseurs (et non par des fournisseurs préqualifiés) sur le site Achats et ventes.

g) Dans la mesure du possible, tout au long du processus, on répondra aux questions non classifiées posées par des fournisseurs préqualifiés et on les affichera sur le site Achats et ventes.

h) Les questions et réponses classifiées ne seront fournies qu'aux fournisseurs préqualifiés qui satisfont aux exigences de sécurité requises.

j) Le GC prévoit publier les questions posées et les réponses données, dans la mesure du possible, tout au long du processus.

1.5 Demande de propositions (DP)

a) Le GC fournira la DP complète, qui comprend des éléments classifiés, aux fournisseurs préqualifiés et invitera les fournisseurs préqualifiés à soumissionner sur la demande.

b) Afin de tenir l'industrie informée, le GC a l'intention de publier (tout en respectant les contraintes de la sécurité nationale) les éléments non classifiés de l'ébauche de la DP sur Achats et ventes. Toutefois, seuls les fournisseurs préqualifiés seront invités à soumissionner à la demande.

Annexe E : Questions sur le soutien en service

Pour l'aider à étudier ses options contractuelles de SES au début du processus d'approvisionnement, le Canada demande aux soumissionnaires de répondre aux questions suivantes. Veuillez noter que les réponses à ces questions ne sont PAS obligatoires et ne joueront PAS un rôle dans l'évaluation de la soumission du répondant.

1. Quel soutien initial est inclus avec la solution potentielle?
2. Quel type de soutien est requis avec la solution après le soutien initial (nombre d'années, nombre d'années d'option, etc.)?
3. Quel type d'entente de niveau de service serait requis (paramètres de soutien, p. ex.)?
4. Quelle structure de paiement (mensuellement, selon les services rendus, etc.) serait requise?
5. Votre solution proposée contiendrait-elle des droits de PI qui pourraient restreindre les futurs contrats de SES?
6. Est-ce qu'une tierce partie aurait accès ou serait autorisée à utiliser les droits de PI que vous détenez pour réaliser des fonctions de SES? Si ce n'est pas le cas, quelle en est la raison?

Pièce jointe 1: Ébauche de l’énoncé des besoins opérationnels (EBO)

Pièce jointe 2: Ébauche de Concept d’opération (CONOPS)

Énoncé des besoins

Cyberdéfense – Décision, analyse et réponse (CD-DAR)

C.000707

Ébauche

DOCUMENTS D’APPROBATION DE PROJET

VERSION [1.0]

EMPLACEMENT DE GESTION DES DOCUMENTS : [INSÉRER OÙ LE DOCUMENT À JOUR EST CLASSÉ (GCDOCS/SGDDI/ETC.)]

Ébauche

TABLE DES MATIÈRES

Ébauche

Ébauche

TABLE DES FIGURES

LISTE DES TABLEAUX

Ébauche

Recommandé par l'équipe du projet :
Signature _____ Date _____ Directeur de projet (DP)
Signature _____ Date _____ Gestionnaire de projet principal (GP)
Approuvé par le comité supérieur de révision :
Signature _____ Date _____ Chef - Développement des Forces
Approuvé par le responsable du projet :
Signature _____ Date _____ Responsable du projet

Ébauche

1 INTRODUCTION

1.1 Contexte

Le paysage des cybermenaces a grandement évolué depuis les vingt dernières années. De nos jours, les cybercriminels sont beaucoup plus sophistiqués et organisés et ont des objectifs et/ou des intentions bien précis. Ils disposent de plus de ressources et peuvent être dirigés et financés par des États-nations, des syndicats du crime organisé et des groupes terroristes. Les cyberattaquants et leurs parrains veulent acquérir illégitimement des informations, des comptes et des données, qu'ils peuvent utiliser à des fins criminelles, politiques ou militaires contre le Canada et ses alliés.

En réponse, les organisations déploient de nombreuses stratégies et technologies qui mettent l'accent sur une défense du réseau périmétrique ou des appareils des utilisateurs (ordinateurs portatifs, imprimantes, tablettes, etc.) fondées sur les méthodes d'attaque répertoriées (virus, maliciels, etc.). Ces solutions s'avèrent trop souvent inefficaces puisque susceptibles de produire une grande quantité d'alertes pour la plupart fausses. Impossibles à traiter automatiquement par un système, il faut donc évaluer ces alertes à la main, ce qui nécessite beaucoup de temps et un important bassin d'experts. Parce que ces alertes sont très nombreuses, le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) ne disposent pas du temps nécessaire et de ressources pour intervenir chaque fois qu'une alerte est déclenchée, et doivent se résigner à ne pas les traiter toutes. Malgré les efforts déployés par le gouvernement, les attaquants font continuellement évoluer leurs méthodes pour contourner les cyberdéfenses et exploiter les changements technologiques, ce qui constitue une menace constante à la sécurité nationale et au bien-être du Canada et des Canadiens.

Le projet Cyberdéfense – Décision, analyse et réponse (CD-DAR), C.000707, fera en sorte d'acquérir des capacités de cyberdéfense dans le but de surveiller et de défendre les réseaux du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'intervenir en conséquence. La capacité CD-DAR fournira également une analyse contextuelle fiable à l'appui des décisions et des mesures du MDN et des FAC à l'intérieur d'extensions et d'interfaces désignées du réseau de commandement[1] (R comd) ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables à l'appui de la conduite d'opérations de cyberdéfense (OCD). L'infrastructure du réseau secret consolidé (IRSC) fait partie du R comd du MDN et des FAC et une partie importante de la portée de ce projet sera appliquée à l'IRSC.

[1] Le réseau de commandement est un réseau de communications qui relie un échelon de commandement à certains ou à tous ses échelons subordonnés aux fins de commandement et contrôle.

1.2 Énoncé des besoins opérationnels et résultats

1.2.1 Énoncé des besoins opérationnels

Le MDN et les FAC ont besoin d'une capacité de cyberdéfense applicable aux domaines stratégiques, opérationnels et propres à la mission. La capacité doit fournir une découverte du réseau, des outils de cyberdéfense logicielle intégrés, un dépôt de base de données de confiance et une image commune de la situation opérationnelle (ICSO), tenir compte des facteurs humains et permettre la criminalistique cybernétique à distance. Le MDN/les FAC a besoin d'une surveillance intégrée de son architecture de réseau et de l'information pertinente qu'elle contient, ainsi que d'une connaissance complète de la situation, de la détection, de l'analyse et de la formulation d'une réponse aux cybermenaces en temps opportun dans les domaines stratégique, opérationnel et tactique.

1.2.2 Facteurs de changement

Il est actuellement difficile de découvrir et de suivre tous les actifs de réseau et de distinguer les éléments connus des éléments nouveaux (et inconnus). Des logiciels mal conçus et des composants du système mal configurés constituent des vulnérabilités importantes des systèmes d'information qui permettent leur exploitation. Afin de fournir des pratiques exemplaires en matière de sécurité des réseaux, telles qu'elles sont décrites par le Centre canadien pour la cybersécurité, le MDN et les FAC doivent commencer par comprendre la composition du réseau et disposer d'une solide capacité à en découvrir les actifs. Les analystes du Centre d'opérations des réseaux des Forces canadiennes (CORFC) travaillent souvent avec plusieurs trousses d'outils; ils doivent surveiller de nombreuses consoles pour être informés de nouvelles alertes, divers portails de services de renseignement sur les menaces pour obtenir de l'information sur les entités en cause et un éventail d'outils de détection et de réponse installés aux points d'extrémité pour comprendre ce qui se passe lorsque ces derniers sont touchés. Le CORFC utilise des outils de flux de travail pour contrôler les processus de triage et d'enquête; ce travail exige souvent que l'analyste copie et colle des données d'un outil à un autre, qu'il remplisse des formulaires et soumette des demandes de recherche ou qu'il téléverse des artéfacts aux fins d'analyse et d'entreposage. L'automatisation assurée par la solution CD-DAR élimine bon nombre de ces tâches, simplifie les processus et assure une qualité et une cohérence reproductibles, même si les processus demeurent essentiellement les mêmes. L'élimination partielle ou complète de ce type de processus manuel répétitif aura une incidence directe sur la productivité des analystes de la sécurité. Ceux-ci pourront alors consacrer plus de temps à des problèmes plus épineux et davantage prioritaires qui exigent une expertise humaine.

De plus, on sait que les systèmes de surveillance de la sécurité génèrent un grand nombre d'alertes pour la plupart considérées comme de « faux résultats positifs » (ou tout simplement non pertinentes) après une enquête plus poussée. Le triage des alertes se fait souvent de façon manuelle par les analystes dont les erreurs toujours possibles se traduisent par l'omission d'incidents. De nombreux rapports dans les organismes de référence des médias sont tombés

Ébauche

entre mauvaises mains même si les outils de sécurité ont généré une alerte à ce sujet, parce qu'un analyste l'a rejetée par erreur (probablement en raison d'une surcharge de travail). Le MDN et les FAC font face à des menaces de plus en plus agressives, comme des rançongiciels[2], où l'intervention efficace se mesure en secondes. Ce scénario oblige les organisations à réduire le temps qu'il leur faut pour réagir à ces incidents, habituellement en déléguant plus de tâches à des machines. La réduction du délai d'intervention, y compris le confinement des incidents et les mesures correctives, est l'un des moyens les plus efficaces de maîtriser les répercussions des incidents de sécurité. La solution CD-DAR fournissent automatiquement un contexte aux alertes et ajoutent des renseignements clés pour permettre un triage manuel automatisé ou, à tout le moins, plus facile et plus rapide.

Le CORFC peut tirer parti de la capacité CD-DAR pour réduire le temps nécessaire à la formation des nouveaux analystes cybernétiques. L'automatisation élimine la nécessité pour l'analyste de connaître les détails des étapes manuelles à suivre pour chaque scénario. Les connaissances sont stockées et gérées dans la capacité CD-DAR, ce qui réduira le besoin pour l'analyste de mémoriser le déroulement du processus et de le répéter constamment. Les analystes peuvent extraire des détails précis pour de nombreux scénarios, si le besoin se présente. Comme la solution CD-DAR combinera la fonctionnalité des outils existants et nouveaux et procurera une image commune de la situation opérationnelle intégrée, il ne sera plus autant nécessaire de donner de la formation à chaque analyste de la sécurité sur chacun des outils.

On a conscience aujourd'hui que le nombre d'événements cybernétiques et d'alertes de sécurité surpasse facilement le nombre de cyberopérateurs ayant l'expérience et les qualifications nécessaires disponibles pour enquêter sur ces événements et protéger l'intégrité du réseau de TI. Par conséquent, le MDN a de plus en plus de mal à rester à jour sur ce front en constante évolution. Si l'on ajoute à cela les capacités de cyberdéfense actuelles, dépassées et inefficaces, la sécurité et la défense du MDN et des FAC demeurent vulnérables à une cybermenace sans cesse croissante, ce qui augmente considérablement le risque pour les missions et les opérations.

1.2.3 Lacunes en matière de capacité

Comme il est expliqué plus en détail à la section 2.4, les lacunes en matière de capacité sont des lacunes ou un manque de ce qui suit :

a. découverte du réseau;
b. outils de cyberdéfense logicielle intégrés;
c. dépôt de base de données fiable;
d. image commune de la situation opérationnelle;

[2] Un type de logiciel malveillant conçu pour bloquer l'accès à un système informatique jusqu'à ce qu'une somme d'argent soit versée.

Ébauche

e. facteurs humains;

f. analyse judiciaire.

1.2.4 Résultats opérationnels

La solution CD-DAR apportera un changement fondamental à la cybersécurité du MDN et des FAC en mettant en œuvre la capacité d'intervention complète en cas d'événements de cybersécurité complexes et en évolution. Elle répondra aux besoins immédiats et à long terme, tout en maintenant et en permettant l'application des exigences en matière de cybersécurité.

Dans le cadre de ce projet, on livrera et mettra en œuvre un système complexe comprenant du matériel informatique et des logiciels, exploité par du personnel qualifié et suivant les processus connexes, qui assurera une surveillance fiable de la sécurité en temps quasi réel et exécutera une fonction d'intervention en cas d'événement sur les réseaux désignés.

Les résultats ***immédiats*** du projet feront du CORFC un centre moderne de cyberopérations doté d'une solution CD-DAR qui sera exploité par une cyberforce. La capacité qui sera mise en œuvre dans le cadre du projet aura une forte incidence sur la façon dont les cyberopérateurs sont sensibilisés, formés, équipés et mènent leurs activités quotidiennes. L'amélioration de l'aide à la décision et de réponse, analyse et réponse (DAR) permettra de s'assurer qu'ils sont prêts à fonctionner dans le cyberespace pour protéger les extensions et les interfaces du réseau de commandant du MDN et des FAC, ainsi que les systèmes du RED déployés.

Les résultats ***intermédiaires*** comprendront des indicateurs de rendement, des mesures de production de rapports et des systèmes de production de rapports (s'ils sont jugés essentiels), ainsi que des processus opérationnels perfectionnés et/ou nouvellement définis mis en place au besoin. Ces processus opérationnels utiliseront davantage le matériel et les outils logiciels pour établir une connaissance fiable, pertinente et significative de la situation de la cybersécurité de l'infrastructure des technologies de l'information (ITI), ainsi qu'une aide à la décision concernant les COD qui touchent tous les aspects des opérations du MDN et des FAC.

Les résultats ***ultimes*** de l'investissement proposé permettront au MDN et aux FAC d'avoir une cyberforce équipée, formée et prête à mener efficacement des activités de COD fondées sur une solide capacité cybernétique de base qui permettra de développer la croissance pour des années à venir. De plus, grâce à l'application de la politique de la Stratégie d'approvisionnement en matière de défense, ce projet contribuera au développement et au maintien d'une cyberindustrie viable au Canada qui est prête à soutenir le gouvernement du Canada (GC) et l'Équipe de la Défense en offrant des technologies novatrices et avancées sur le plan scientifique ainsi qu'en dotation de personnel pour l'avenir.

Ébauche

2 EXIGENCES OBLIGATOIRES DE HAUT NIVEAU (EOHN)

Les principaux facteurs opérationnels de la capacité requise sont abordés par les exigences obligatoires de haut niveau (EOHN). Les EOHN décrivent un ensemble de capacités que le projet de CD-DAR doit permettre d'atteindre. Essentiellement, ils définissent les résultats, les effets ou les services attendus du projet.
Les exigences obligatoires de haut niveau pour l'investissement sont décrites au tableau 1 ci-dessous. Ces EOHN seront raffinés pour en faire un énoncé détaillé des besoins opérationnels (EBO).

Aux fins de l'EBO, la portée du projet de CD-DAR est le « réseau de commandement ». Un réseau de commandement est un réseau de communication qui relie un échelon de commandement à une partie ou à la totalité de ses échelons subalternes aux fins de commandement et de contrôle (C2). L'infrastructure du réseau secret consolidé (IRSC) fait partie du réseau de commandement du MDN et des FAC et une partie importante de la portée de ce projet sera appliquée à l'IRSC. Le réseau de commandement comprend les extensions et les interfaces du R comd et les systèmes du RED déployables. Tout au long de cet énoncé des besoins opérationnels, le terme « réseau de commandement » sera utilisé pour inclure les termes ci-dessus.

Tableau 1 – Exigences obligatoires de haut niveau

N°	Capacité	EOHN
1	Cyberactifs (découverte du réseau)	La capacité d'identifier et de suivre rapidement tous les biens (autorisés et non autorisés) connectés au réseau de commandement et d'évaluer leurs attributs en matière de vulnérabilité, de configuration, de risque et de conformité aux correctifs.
2	Cyberanalyse	La capacité de recueillir, de conserver et d'analyser continuellement des renseignements sur les cybermenaces dans l'environnement du réseau de commandement et de détecter et de caractériser les activités suspectes, ainsi que de fournir un contexte pour les évaluations des risques et des vulnérabilités en temps quasi réel.
3	Intervention cybernétique	Capacité d'identifier de façon adaptative et dynamique une menace et de la contenir et de l'éradiquer.
4	Commandement et contrôle	La capacité de maintenir la connaissance de la situation, au moyen d'une image commune de la situation opérationnelle, des alertes, des menaces et des mesures correctives dans l'ensemble du réseau de commandement du MDN et des FAC, et d'alimenter la connaissance de la situation aux fins de prise de décisions et l'exécution des réponses par des interfaces normalisées et des flux de travail automatisés à l'appui du soutien à la décision de l'élément de commandement, et la mise en œuvre des interventions selon les directives.
5	Intégration de la solution CD-DAR	La capacité d'être intégrée (hébergée et exploitée avec des applications et un dépôt fiable) au réseau de commandement assigné en tant que système cohésif.

Ébauche

Nº	Capacité	EOHN
6	Cyberinteropérabilité	La capacité d'échanger de l'information sur les vecteurs et l'analyse des cybermenaces pour répondre aux exigences internes en matière de compatibilité ainsi qu'aux systèmes et à l'environnement réseau assigné d'autres ministères (AM) et des nations faisant partie du Groupe des cinq (Gp5), pays membres de l'Organisation du traité de l'Atlantique Nord (OTAN) et autres organisations externes.
7	Cyberrésilience	La capacité d'effectuer une surveillance localisée de l'architecture de réseau, des biens et de l'information sur les menaces, l'analyse et la prise de décisions d'intervention dans des environnements déployés où la connectivité n'est pas disponible, n'est pas fiable ou a une capacité limitée.
8	Évolution et développement continus des cybercapacités	La capacité d'évoluer continuellement en tant que réponse au changement (menace, politique, technologie) de l'infrastructure de réseau du MDN et des FAC (la criminalistique à distance et le confinement/l'assainissement font partie de cette intervention) avec une incidence minimale sur les systèmes connectés ou la modification de l'infrastructure de TI sous-jacente, des normes de base et des politiques.
9	Cyberflexibilité	La capacité de la solution CD-DAR à être évolutive, modulaire et facilement élargie, indépendamment de l'emplacement ou de la durée des actifs statiques ou opérationnels déployés.

2.1 Hypothèses clés

À la suite d'un examen interne et externe, les hypothèses touchant ce projet sont énumérées au tableau 2 ci-dessous.

Tableau 2 – Hypothèses

Nº	Catégorie	Hypothèses utilisées	Effets sur le projet	Niveau de fiabilité faible/moyen/élevé	Stratégies si l'hypothèse ne se concrétise pas
1	Infrastructure	Le projet utilisera l'infrastructure physique et le réseau existant, mais pourrait nécessiter des réseaux enclavés particuliers à des fins de sécurité et d'essai.	Si l'infrastructure physique et le réseau existant ne peuvent pas être réutilisés, les coûts du projet augmenteront.	Élevé	Une réévaluation aura lieu et les fonds seront réaffectés.
2	Génie des systèmes	La bande passante actuelle au sein de l'ITI permettra de tenir compte des mises à jour des données sur la connaissance de la situation (CS) que requiert la solution CD-DAR, particulièrement	Un manque de bande passante disponible peut surcharger le cyberenvironnement opérationnel et nuire à l'assurance de la mission. Le besoin d'une bande passante	Élevé	S'il y a un manque de bande passante suffisante, il sera traité par les organismes appropriés (Directeur - Ingénierie et intégration (Gestion

Nº	Catégorie	Hypothèses utilisées	Effets sur le projet	Niveau de fiabilité faible/moyen/élevé	Stratégies si l'hypothèse ne se concrétise pas
		dans les emplacements déployés.	supplémentaire augmenterait les coûts d'exploitation.		de l'information) [DIIGI], Services partagés Canada [SPC]) pour formuler une résolution.

2.2 Capacité opérationnelle initiale (COI) (haut niveau)

La capacité opérationnelle initiale (COI) permettra d'atteindre les capacités des EOHN au tableau 1 dans l'infrastructure limitée du R comd et déployée du RED. Cela comprendra l'installation et la configuration de l'infrastructure de soutien aux sites concernés, où certains employés clés seront également formés sur les systèmes précis CD-DAR. Le perfectionnement des indicateurs de rendement, des systèmes de rapport et des processus opérationnels sera également atteint à la COI.

2.3 Capacité opérationnelle finale (COF) (haut niveau)

La COF verra l'atteinte des capacités de toutes les EOHN, décrites au tableau 1, sur le reste des infrastructures du réseau de commandement et de l'infrastructure du RED déployée. Les réseaux seront désignés dans l'EBO produit au cours de la phase de définition du projet. La COF permettra également d'atteindre le résultat énoncé dans l'analyse de rentabilisation (AR) : une force cybernétique équipée, entraînée et préparée pour mener efficacement des COD et une cybercapacité qui soutiendra le développement futur.

2.4 Insuffisance en capacité

Le domaine cybernétique du MDN et des FAC fait actuellement face à des menaces persistantes, constantes et croissantes de la part de ses adversaires. Il est essentiel que la solution CD-DAR remplace les systèmes multiples et les processus manuels d'aujourd'hui par une plateforme unique et moderne, dotée de processus opérationnels corrélés et automatisés. Le projet de CD-DAR est un important pas en avant dans la défense et la protection du domaine cybernétique du MDN et des FAC avec un objectif axé sur le Groupe des opérations d'information des Forces canadiennes (GOIFC) et le Centre d'opérations des réseaux des Forces canadiennes (CORFC).

En collaboration avec des intervenants (c.-à-d. ceux ayant des intérêts particuliers dans le fonctionnement du réseau décrit ci-dessous, principalement au sein du MDN, ce qui comprend d'autres ministères ou organismes du gouvernement comme le Centre de la sécurité des télécommunications (CST) et SPC, ainsi que le Groupe des cinq et les alliés de l'OTAN), le projet de CD-DAR a évalué les capacités cybernétiques du MDN et des FAC, et a conclu qu'elles sont

Ébauche

insuffisantes pour les besoins actuels. Elles se fondent sur des solutions à court terme avec des injections irrégulières de nouvelles technologies qui permettent d'atteindre un effet limité. Au sein du MDN, le Centre d'opérations de réseaux des Forces canadiennes (CORFC) constitue l'organisation principale de cyberdéfense. Leur mission est d'obtenir et de maintenir la cybersupériorité au sein de la zone de responsabilité cybernétique (ZResp) du MDN et des FAC afin d'assurer la « liberté d'action des forces amies ». Concentrés sur les opérations, hautement motivés et possédant des compétences uniques en technologies et techniques spécialisées, ils sont proactifs, dynamiques, disponibles 24 heures sur 24, 7 jours sur 7 et se consacrent au maintien des services de TI dans toutes les conditions. Le CORFC est l'unité nationale opérationnelle de cyberdéfense qui se voit attribuer en permanence des tâches essentielles à la mission pour représenter le chef d'état-major de la Défense (CEMD) et les autorités opérationnelles de réseau (AO) applicables. Le CORFC dirige les opérations courantes et la défense de tous les réseaux du MDN et des FC pour le compte du Sous-ministre adjoint (Gestion de l'information) (SMA[GI]).

Au sein du CORFC, les équipes suivantes présentent des lacunes en matière de capacité :

a. Opération de cyberdéfense – coordonne les cyberopérations défensives du MDN et des FAC et l'intervention en cas d'incident avec les organisations internes et externes du Ministère;

b. Cellule de renseignement sur les cybermenaces – fonctionne à l'heure actuelle de 8 à 17 h (avec une capacité de pointe) pour fournir des renseignements proactifs et réactifs afin d'améliorer les opérations de cyberdéfense;

c. Équipe de surveillance – analyse du trafic réseau du domaine cybernétique du MDN et des FAC afin d'identifier les dispositifs potentiellement compromis en vue d'une enquête plus approfondie;

d. Équipe de reconnaissance – fournit des évaluations réalistes et en direct de la vulnérabilité et de l'exploitation avancée des systèmes et des procédures d'information pour évaluer la posture de sécurité du client et effectuer des démonstrations contrôlées de ce qu'un attaquant pourrait accomplir dans l'infrastructure de TI d'un client;

e. Équipe de gestion des incidents – assume le rôle de chef de file national en matière de gestion des incidents dans le cadre établi pour une approche d'entreprise coordonnée;

f. Soutien du système de détection des intrusions d'entreprise – responsable de fournir un soutien 24 heures sur 24, 7 jours sur 7, des éléments suivants : (i) la configuration, la mise à l'essai, le déploiement de divers SDI et outils analytiques sur les capteurs/serveurs de SDI du CORFC pour tous les réseaux surveillés des FAC; (ii) la configuration, la mise à l'essai et le déploiement de divers capteurs/serveurs SDI sur tous les réseaux; (iii) les correctifs et les mises à niveau des suites de SDI

Ébauche

nécessaires; et (iv) le soutien matériel et logiciel et la maintenance du matériel SDI (Security Onion[3], Sourcefire[4], conçus spécifiquement pour le CORFC);

g. Équipe de soutien de l'évaluation des vulnérabilités de l'entreprise – s'occupe de la gestion des vulnérabilités et des risques dans certains réseaux;

h. Section de la criminalistique – fournit des services d'analyse numérique spécialisés au MDN et aux FAC. Elle fournit également une analyse technique des cybermenaces et des techniques de logiciels malveillants utilisées par les adversaires pour pénétrer le domaine cybernétique du MDN et des FAC.

Comme il est expliqué brièvement à la section 1.2.3, les lacunes en matière de capacité sont des lacunes ou un manque de ce qui suit :

a. Découverte du réseau – Afin de protéger un réseau, il doit y avoir un inventaire complet de tous les dispositifs matériels du réseau, comme les serveurs, les routeurs, les commutateurs, les passerelles et bien plus encore, et les logiciels, y compris les versions ou les correctifs[5] les plus récents qui se trouvent sur le réseau spécifié. À l'heure actuelle, la surveillance du réseau et la découverte d'appareils sont limitées pour le MDN et les FAC. Il y a des plates-formes capables d'effectuer la découverte de réseaux qui sont mises à l'essai et utilisées de façon ponctuelle, couvrant des parties des réseaux du MDN et des FAC, mais pas le réseau complet. Des logiciels comme Nessus, Cyber Information and Incident Sharing System (CIICS) et Malware Information Sharing Platform (MISP)[6] se sont révélés capables de fournir une solution, mais ne sont pas utilisés de façon cohérente. La solution CD-DAR trouvera les meilleures réponses possibles, assurera l'interopérabilité des plates-formes de découverte de réseau et couvrira toute la gamme des capacités de conception de produits;

b. Outils de cyberdéfense logicielle intégrés – L'ensemble d'outils actuels n'est pas intégré et nécessite des compétences d'opérateur extrêmement spécialisées pour utiliser ces outils logiciels afin d'isoler tout problème, exporter de l'information et

[3] Security Onion est une distribution Linux gratuite et libre pour la détection des intrusions, la surveillance de la sécurité des entreprises et la gestion des journaux.

[4] Sourcefire, Inc (rachetée par Cisco) était une entreprise technologique qui développait du matériel et des logiciels de sécurité réseau. Les appareils de sécurité réseau Firepower de la société sont fondés sur Snort, un système de détection d'intrusion (SDI) à code source ouvert.

[5] Un correctif est un ensemble de modifications à un programme informatique ou ses données connexes pour les corriger ou les améliorer). Cela comprend la correction des vulnérabilités en matière de sécurité (une faiblesse qui peut être exploitée par un auteur de menaces, comme un attaquant, pour exécuter des actions non autorisées dans un système informatique).

[6] Nessus est un analyseur de vulnérabilités propriétaire élaboré par Tenable Network Security; Cyber Information and Incident Coordination System (CIICS) est une application Web qui permet aux pays d'échanger de l'information sur la cyberdéfense au sein d'une communauté de confiance; cette communauté est appelée Fédération CIICS de l'OTAN; Malware Information Sharing Platform (MISP) est un logiciel libre et gratuit qui facilite l'échange du renseignement sur les menaces, notamment les indicateurs de cybersécurité.

Ébauche

faire des comparaisons manuelles avec de l'information extraite d'autres outils logiciels. Voici deux exemples :

i. Équipe de surveillance – À l'heure actuelle, l'analyste de la surveillance utilise des ensembles d'outils isolés qui ne sont pas reliés. Toutefois, cela ne nous donne pas un portrait complet du contexte des cybermenaces. Pour automatiser plus efficacement la détection des menaces, il faut utiliser l'apprentissage automatique et les algorithmes automatisés pour observer les tendances afin de détecter les menaces jusque-là inconnues. Cela aidera à maintenir la robustesse du réseau, ce qui permettra au MDN et aux FAC de maintenir une meilleure cybersécurité;

ii. Équipe de gestion des incidents – Le traitement des incidents est un processus très lourd. Il y a peu de plates-formes qui ont de bons flux de travail qui permettent la traçabilité de la façon dont un incident est traité et/ou qui assurent la responsabilisation des mesures prises tout au long du processus. À ce moment-là, une analyse est effectuée sur une plate-forme, puis les données d'analyse doivent être transférées physiquement à d'autres applications pour bien gérer l'incident;

c. Un dépôt de base de données fiable – La Cellule de renseignements sur les cybermenaces fournit des renseignements proactifs et réactifs pour améliorer les opérations de cyberdéfense. Pour effectuer une analyse, le MDN et les FAC doivent tirer des renseignements de différents systèmes. Un dépôt central permettra aux commandants de prendre des décisions éclairées sur les mesures défensives requises. À l'heure actuelle, le Centre national de transfert de données de l'État-major interarmées stratégique (EMIS) a la capacité de transférer de l'information à partir de 29 réseaux différents pour l'ensemble du MDN et des FAC. Toutefois, comme il ne s'agit pas d'une cybercapacité, cette information est hors de portée pour la solution CD-DAR et limite la façon dont l'information est stockée et transférée à des fins de cyberrenseignement. Il est nécessaire d'avoir des renseignements sur les cybermenaces adaptés à la tâche dans un dépôt central et robuste avec une grande quantité d'automatisation pour les sources fiables et connues, du niveau de classification faible au niveau de classification élevé (et vice versa), de l'information et des données de base du système et du réseau. Cela permettra la surveillance de la sécurité et des mécanismes comme l'analyse des liens, l'analyse des vulnérabilités, la détection des intrusions, l'analyse criminalistique, la collecte et l'analyse de journaux et d'autres données provenant des réseaux de l'organisation. Cela permettrait également d'effectuer des examens d'analyse de sécurité et de donner des conseils et des directives pour les interventions aux alertes de sécurité;

Ébauche

d. Image commune de la situation opérationnelle (ICSO) – La capacité de partager l'information nécessaire à l'élaboration d'une ICSO est étroitement associée aux outils de défense logicielle intégrée. Les capacités actuelles du MDN et des FAC ne disposent pas d'un point de vue central pour évaluer les répercussions des cyberactivités. Ces capacités sont insuffisamment intégrées, moins réactives et considérées comme déficientes pour ce qui est de fournir de l'information opérationnelle à l'appui des processus décisionnels efficaces du commandement. Une ICSO doit être souple et adaptée aux besoins de chaque commandant, qu'ils soient stratégiques, opérationnels ou tactiques. À l'heure actuelle, le CORFC utilise le programme interne et n'a aucune marge de manœuvre dans les points de vue opérationnels pour consolider l'information pour le commandant. Il est également impossible d'utiliser ce programme sur des réseaux qui ne sont pas disponibles, qui ne sont pas fiables ou qui ont une capacité limitée (épisodique);

e. Facteurs humains – La solution CD-DAR abordera deux aspects particuliers des facteurs humains. Le premier est qu'il faut trop de spécialisation de la part des analystes cybernétiques, et le deuxième est la surcharge cognitive pour les cyberopérateurs. Pour régler ces problèmes, le projet de CD-DAR fournira une solution intégrée de cyberdéfense qui allégera le fardeau de comparer manuellement l'information d'un outil à celle d'un autre; cela réduira les connaissances détaillées et la spécialisation nécessaires pour maîtriser les divers outils de cyberdéfense. La solution CD-DAR atténuera la surcharge cognitive en gérant le volume de détection manuelle des menaces en recueillant automatiquement des renseignements de sécurité à partir du réseau. Elle analysera ces renseignements afin de cerner les menaces et de mettre en corrélation les renseignements provenant de sources multiples (GC et alliés). Les alertes de sécurité seront alors automatiquement classées par ordre de priorité avec des recommandations sur la façon de remédier aux menaces. La solution CD-DAR fera appel à des analyses de sécurité avancées qui vont bien au-delà des approches fondées sur la signature actuellement utilisées. Les technologies d'apprentissage automatique seront mises à profit pour évaluer les événements dans l'ensemble du réseau de commandement et détecter les menaces et prévoir l'évolution d'attaques qui seraient impossibles à réaliser au moyen d'approches manuelles. Ces analyses de sécurité comprennent :

    i. des renseignements intégrés sur les menaces qui ciblent les mauvais acteurs connus en tirant parti des renseignements sur les menaces mondiales,

    ii. une analyse comportementale qui applique des modèles connus pour découvrir des comportements malveillants,

Ébauche

iii. la détection d'anomalies au moyen du profilage statistique pour établir une base de référence historique afin de fournir des alertes sur les écarts par rapport aux bases de référence établies qui sont conformes aux vecteurs d'attaque potentiels;

f. Capacité de mener des enquêtes judiciaires – La Section de la criminalistique fournit des services d'analyse numérique spécialisés au MDN et aux FAC. Elle fournit également une analyse technique des cybermenaces et des techniques de logiciels malveillants utilisées par les adversaires pour pénétrer le domaine cybernétique du MDN et des FAC. En plus de l'analyse des logiciels malveillants, la Section de la criminalistique est chargée de tenir à jour les événements de cybersécurité et de collaborer avec d'autres organismes. À l'heure actuelle, lorsqu'une fuite de données se produit, l'enlèvement physique et le remplacement du matériel peuvent coûter des milliers, voire des millions de dollars au MDN et aux FAC. Avec le projet CD-DAR comme solution de rechange au remplacement du matériel physique, l'image d'un disque dur touché pourrait être envoyée à distance à un environnement de bac à sable[7] où la Section de la criminalistique peut faire des analyses et des enquêtes tout en permettant d'effacer le disque dur. Lorsque l'équipement est situé dans différentes régions géographiques sans l'expertise d'un analyste, les disques durs et autres équipements doivent être expédiés à une installation locale aux fins d'analyse. Ces disques sont sujets à être endommagés au cours de l'expédition, ce qui entraîne des retards supplémentaires ou peut empêcher la mise en place d'une procédure appropriée et l'examen de preuves potentielles. La solution CD-DAR permettra d'économiser du temps et de l'argent, car la Section de la criminalistique n'aura pas à attendre que l'équipement soit transporté d'un bout à l'autre du pays à des fins d'analyse.

2.5 Contraintes liées au projet

Tableau 3 – Contraintes

Nº	Catégorie	Description
1	Security Clearance	En raison de la nature du domaine, ce projet doit nécessiter du personnel et des membres de l'industrie ayant des cotes de sécurité allant jusqu'à TRÈS SECRET - Renseignement d'origine électromagnétique (SIGINT) et avec des restrictions de citoyenneté de l'Australie / la Nouvelle-Zélande / le Royaume-Uni / les États-Unis (AUS/NZ/UK/US) ou aux citoyens CANADIENS seulement.

[7] En sécurité informatique, un "bac à sable" est un mécanisme de sécurité permettant de séparer les programmes en cours d'exécution, généralement dans le but d'atténuer les défaillances du système ou les vulnérabilités des logiciels, sans risquer de nuire à la machine hôte ou au système d'exploitation.

2	Exigences de conception	Le système de processus, de logiciels et de matériel doit pouvoir être utilisé par le personnel opérationnel existant du MDN et des FAC, y compris le personnel qui produit et utilise actuellement de l'information sur la connaissance de la situation. Pour être efficace, la capacité CD-DAR ne doit pas exiger une formation excessive qui modifie fondamentalement les compétences et les métiers ou professions disponibles pour remplir ces rôles.

2.6 Situation actuelle

Le 28 mars 2019, le Comité des capacités de la Défense (CCD) a passé en revue le projet de CD-DAR. Il a approuvé l'option préférée qui consiste à regrouper l'analyse de rentabilisation (projets de sensibilisation à la cybersécurité (SCS) et d'Aide à la décision pour les cyberopérations défensives (AD-COD). Le CCD a également convenu que le projet devrait être acheminé au Conseil de gestion du programme (CGP) pour qu'il appuie la phase de définition, à la suite de l'examen de la portée, de l'extensibilité et des calendriers du projet.

Une demande d'information (DI) a été publiée en décembre 2017 dans le but de consulter l'industrie en ce qui concerne la faisabilité de la solution, le coût et les délais. Les soumissions de l'industrie en réponse à la demande d'information ont mis en évidence les progrès technologiques importants réalisés au cours des dernières années, et une estimation des coûts a été fournie pour la SCS et la capacité intégrée AD-COD, pour le calendrier donné. Le dernier examen d'avancement du comité de révision supérieur (CRS) a eu lieu en février 2020 et le prochain est prévu pour février 2021. En juin 2020, le Secrétariat du Conseil du Trésor du Canada (CT) a approuvé le passage du projet à la phase de définition. De plus, une modification de la DI et une ébauche d'invitation à se qualifier (IQ) ont été préparées et publiées en juillet 2020. L'IQ, mise à jour selon les recommandations de l'industrie, sera publiée sur Achatsetventes en avril 2021.

L'équipe du projet CD-DAR a réalisé d'importantes activités en vue de respecter les étapes critiques, comme l'établissement détaillé des coûts pour les phases de définition et de mise en œuvre, le document d'architecture technique (DAT), le plan de transformation des activités, en plus des documents de projet comme la charte de projet (approbation de la phase d'analyse des options (AO) en octobre 2020), le plan de gestion du projet et le plan de gestion des risques, etc. Le projet a fait appel à des intervenants clés du MDN (DIIGI, Directeur général - Opérations de gestion de l'information (DGOGI), CORFC, Centre des opérations des services de défense (COSD), Recherche et développement pour la défense Canada (RDDC), etc.), du GC (SPC et CST) et des partenaires alliés pour s'assurer que l'interopérabilité et les dépendances sont bien comprises compte tenu de la taille et de la complexité du projet. En collaboration avec le Directeur - Achat de systèmes électroniques (DASE) et Services publics et Approvisionnement Canada (SPAC), l'équipe de projet élabore également une stratégie et un calendrier

Ébauche

d'approvisionnement global et, dans la mesure du possible, des activités d'approvisionnement préparatoires à l'avance afin de respecter les délais prévus pour les phases de définition et de mise en œuvre.

2.7 Interdépendances du projet

Les interdépendances qui pourraient nuire à la réussite de la mise en œuvre de la solution CD-DAR sont énumérées au tableau 4 ci-dessous.

Tableau 4 – Interdépendances de la solution CD-DAR

Titre du projet	N° du projet	Description des interdépendances	Incidence si non livré	Réponse au risque	Date requise
Infrastructure de technologie de l'information à l'appui du commandement et du contrôle (ITI à l'appui du C2)	C.000698	L'ITI à l'appui du C2 transformera et améliorera l'ITI du MDN et des FAC afin de combler les lacunes cernées et de positionner l'entreprise pour relever les défis futurs. Il permettra une exécution plus efficace du C2 à tous les niveaux. L'ITI à l'appui du C2 dépend de la solution CD-DAR pour améliorer la sécurité du réseau secret intégré.	Aucune	Le projet CD-DAR sera très probablement livré avant le projet d'ITI à l'appui du C2, par conséquent la solution CD-DAR devra s'adapter facilement pour servir le nouvel environnement.	À déterminer
Commandement et contrôle de réseau – Capacité intégrée de connaissance de la situation (C2 réseau CICS)	C.000375	Le C2 réseau CICS fournira une vue priorisée des services de technologie de l'information (TI) dont les opérations dépendent.	La portée du projet CD-DAR pourrait devoir être étendue pour inclure la connaissance de la situation des services de TI.	Engagement précoce avec la haute direction et le CDF pour augmenter le financement et ajuster le calendrier au moyen d'une proposition de modification du plan d'investissement - évaluation des répercussions (PMPI-ER).	À déterminer

Ébauche

2.7.1 Dépendances

Le projet CD-DAR est tourné vers l'avenir et fournira des capacités futures. Sa conception et ses produits livrables devront probablement faire preuve d'une certaine souplesse pour s'aligner sur les fonctionnalités et les capacités actuelles et prévues fournies par d'autres projets. En outre, les changements imposés par diverses autorités opérationnelles et techniques, au cours de la durée de vie du projet, ainsi que les directives et politiques inconnues à l'heure actuelle, peuvent créer des dépendances supplémentaires pour la solution.

2.7.2 Contributions

Le projet espère tirer parti des capacités existantes et prévues en dehors de la portée du projet et qui sont fournies par d'autres parties, que ce soit au sein du MDN/des FAC (p. ex. COMRENSFC), par d'autres ministères ou des partenaires de sécurité externes, dans le but de maximiser la nature intégrée de la solution CD-DAR. Ces éléments incluent, mais ne sont pas limités à :

a. le renseignement sur les menaces provenant d'autres ministères et de partenaires de sécurité de confiance;

b. Sources supplémentaires d'authentification, d'autorisation, d'audit et d'éléments d'infrastructure connexes.

Ébauche

3 FONCTIONNEMENT DU SYSTÈME

3.1 Missions et scénarios

La **mission** de la cyberforce des FAC est d'imaginer et de concevoir les cybercapacités des FAC, puis de les construire et de les mettre en œuvre avec les forces existantes pour mener des cyberopérations complètes. Étant donné le domaine cybernétique constant, intégré, mondial et technologiquement dépendant dans lequel les FAC opèrent dans l'ensemble, la cyberforce joue un rôle crucial dans la défense quotidienne du Canada, maintenant et à l'avenir.

La **mission principale** du projet de CD-DAR consistera à acquérir des cybercapacités défensives pour améliorer la CS de la cybersécurité et les décisions, analyses et réponses (DAR). Celles-ci doivent être intégrées dans une solution pour fournir une analyse contextuelle fiable afin d'appuyer les décisions et les mesures d'intervention du personnel du réseau de commandement dans la conduite des COD.

Le MDN et des FAC sont chargés du renseignement militaire à des fins d'évaluation de la menace et des risques. En tout temps, le MDN et des FAC peuvent être tenus d'entreprendre des missions pour assurer la protection du Canada et des Canadiens ainsi que le maintien de la paix et de la stabilité internationales.

Les capacités de CD-DAR seront disponibles et actives, peu importe le but, l'emplacement ou la durée de la mission. Étant donné que la solution CD-DAR surveille le R comd et ses extensions, les opérations utilisant ces extensions bénéficieront de la même capacité de cyberdéfense à l'appui de leur mission.

Une cyberopération est l'application de cybercapacités coordonnées pour atteindre un objectif dans le cyberespace ou par son intermédiaire. Les cyberopérations sont pertinentes dans tout le spectre des opérations militaires, qu'il s'agisse du soutien à l'autorité civile, la recherche et le sauvetage, les opérations de soutien de la paix et de combat. Comme pour toutes les opérations militaires, les effets opérationnels sont produits par l'intermédiaire de relations de C2 officialisées, de groupements opérationnels, de besoins en matière d'information déterminés par le commandement, d'une planification délibérée, de procédures d'état-major et d'une force entraînée et préparée capable de produire les effets opérationnels souhaités.

L'objectif des COD est de contrer activement les menaces et de restaurer l'état de fonctionnement sécuritaire initial du réseau. Les COD sont l'ensemble des mesures prises pour défendre la disponibilité, l'intégrité et la confidentialité du système de C2 et des données des FAC de manière qu'un commandant puisse se prévaloir de ses pouvoirs opérationnels. Les actions associées aux COD comprennent les activités de soutien du renseignement (protection), les tâches de surveillance et de reconnaissance (détection et orientation), les décisions de commandement (décision) et le déploiement de contre-mesures (action).

Ébauche

Le diagramme de la figure 1 ci-dessous présente un modèle d'action et de décision type pour les COD. IL montre également montre les relations et les plans servant à revenir à un état de fonctionnement sécuritaire.

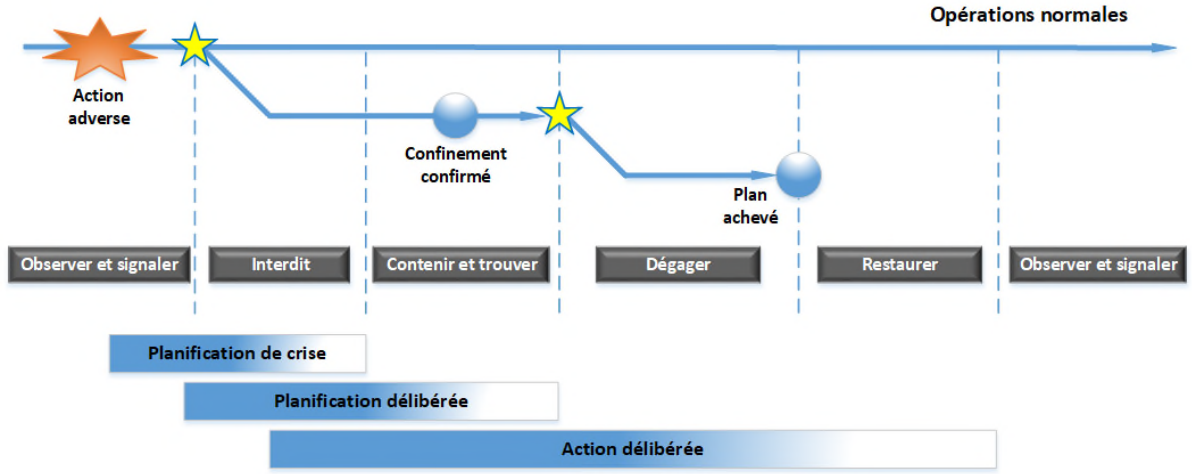


Figure 1 – Modèle d'action et de décision des COD

Une fois la solution CD-DAR mise en œuvre, le rôle du CORFC comprendra la détection, la reconnaissance et l'identification d'entités cybernétiques (humaines et non humaines) hostiles ou autrement non autorisées dans un secteur de responsabilité cybernétique défini et désigné et, selon sa disposition, préviendra sa destruction ou sa perte par les actions de l'ennemi.

Cybermission du CORFC : « La mission du CORFC consiste à obtenir et à maintenir la cybersupériorité à l'intérieur de la zone de responsabilité cyberspatiale du MDN et des FAC afin d'assurer la liberté d'action des forces amies. »

Le projet de CD-DAR fournira une capacité qui améliorera la position du MDN et des FAC en matière de cybersécurité, réduira le délai d'intervention en cas d'incidents cybernétiques et aidera à atténuer la menace d'attaque cybernétique en fournissant à l'utilisateur d'une force un moyen de fonctionner efficacement dans un domaine cybernétique contesté. La visibilité accrue en matière de sécurité et la normalisation assurée par la solution CD-DAR constitueront le fondement sur lequel des capacités plus avancées de gestion, de sécurité et de défense du Canada et des Canadiens pourront être construites.

3.2 Environnement

Étant donné qu'une partie importante de la population mondiale est maintenant connectée à l'échelle mondiale grâce à l'évolution d'Internet, les défis que pose le cyberespace en matière de sécurité et de défense sont importants. En outre, une connectivité accrue a permis et continuera de permettre aux adversaires de se connecter à des groupes idéologiques et à des individus et de les motiver grâce à une gamme de plates-formes Internet, de devises et de sources de pouvoir financier. La protection du renseignement, de la défense et de l'information

sur la sécurité nationale, l'accès garanti et l'utilisation des systèmes et de l'infrastructure des technologies de l'information du Canada et des pays alliés; et la capacité d'exploiter le cyberespace pour atteindre les objectifs de sécurité nationale est une nécessité et continuera d'être essentielle à la sécurité de la plupart des pays.

L'importance de l'ITI mondiale continue de s'étendre à de nouveaux domaines de la vie moderne et de la société. Les avancées technologiques ont ouvert le domaine cybernétique à une variété d'acteurs étatiques et non étatiques; ce qui donne lieu à l'augmentation de menaces importantes. Dans le contexte militaire, les adversaires potentiels développent rapidement des moyens cybernétiques pour exploiter les vulnérabilités inhérentes aux systèmes de commandement, de contrôle, de communications, de l'informatique, de renseignement, de surveillance et de reconnaissance (C4ISR) ainsi que les systèmes de combat. Cette exigence militaire et intérieure principale est décrite dans la politique de défense du Canada : Protection, Sécurité, Engagement (PSE).

La solution CD-DAR fournira des capacités de sécurité et de défense des TI partout où les extensions et interfaces du R comd, statiques et déployables, et les systèmes de RED déployables identifiés sont accessibles. Cela a une incidence sur les environnements suivants :

a. *Environnement durable :* Cela comprend les emplacements fixes au pays et à l'étranger, comme le CORFC et le COSD lorsqu'il y a une gamme complète d'infrastructures de soutien disponibles ainsi qu'une connectivité complète aux réseaux et systèmes de soutien. L'environnement opérationnel est robuste et fiable;

b. *Environnement épisodique :* Cela concerne tous les lieux de mission où l'infrastructure variera de robuste à limitée, et la disponibilité variera de fiable à non fiable. Ces conditions s'ajoutent aux exigences de fonctionnement dans des situations débranchées, intermittentes et à faible largeur de bande (limitée) et de reprise après une telle situation. Les environnements débranchés, intermittents et limités présupposent le besoin de traitement autonome local, de voies de communication de rechange et de la capacité de se rétablir sans problème des limites de connexion lorsque la connexion est rétablie;

c. *Environnement de collaboration :* Comme la plupart des missions du MDN et des FAC sont menées dans des environnements de systèmes et parties multiples, les capacités de CD-DAR doivent être interopérables avec les réseaux et systèmes gérés par le MDN, les autres ministères et organismes, les alliés et d'autres partenaires internationaux. La solution CD-DAR doit également tenir compte de la nécessité de traiter l'information dans divers domaines de sécurité et mises en garde;

d. *Cyberenvironnement :* Les faiblesses peuvent être exploitées et les répercussions de ces exploitations peuvent être réparties entre les réseaux qui exigent une réactivité maximale. Pour ce faire, on optimise habituellement l'automatisation des capacités

Ébauche

de surveillance, de détection, d'analyse, de prise de décisions et d'intervention, ainsi que l'inclusion de processus et de systèmes souples pour s'adapter à un environnement de menace en évolution rapide.

Le domaine cybernétique nécessite un ensemble solide et cohérent d'outils, de ressources et de capacités pour permettre au MDN et aux FAC de remplir leur mandat et de fonctionner efficacement dans un domaine cybernétique contesté.

3.3 Menaces

Tout comme la guerre asymétrique, les cybermenaces[8] ne sont pas immédiatement visibles par rapport aux conflits militaires traditionnels. D'innombrables acteurs menaçants, cachés dans le cyberespace, peuvent influencer ou cibler le MDN ou les FAC dans leur ensemble, un système précis ou une personne en particulier.

Pour concentrer les efforts de défense dans le cyberdomaine, le Canada doit avoir une bonne connaissance des auteurs des menaces, y compris de leurs intentions, leurs capacités et leurs occasions. Un rapport en libre accès produit par les États-Unis, *The Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee*, identifie certains des principaux auteurs de cybermenaces et les menaces qu'ils posent. Les points suivants tirés du rapport sont mis en évidence pour illustrer l'utilisation du cyberespace par nos adversaires dans l'environnement opérationnel :

a. Certaines nations adoptent une posture cyberspatiale plus ferme en fonction de leur volonté de cibler les systèmes d'infrastructure essentiels et de mener des opérations d'espionnage même lorsqu'elles sont détectées et sous un contrôle public accru;

b. Les cyberopérations sont susceptibles de cibler les intérêts de l'Occident pour soutenir plusieurs objectifs stratégiques : la collecte de renseignements[9] pour soutenir la prise de décision, influencer les opérations pour soutenir les objectifs militaires et politiques et poursuivre la préparation du cyberenvironnement pour les événements imprévus futurs;

c. Plusieurs pays continuent d'avoir du succès dans le cyberespionnage contre les gouvernements et l'industrie;

[8] **Cybermenace (OTAN) :** La possibilité de tentative malveillante visant à endommager ou perturber un système ou un réseau informatique.

[9] **Renseignement :** Produit de la recherche, du traitement, de l'analyse, de l'intégration et de l'interprétation des informations disponibles sur les États étrangers, les forces ou éléments hostiles ou susceptibles de l'être, la géographie et les facteurs sociaux et culturels qui contribuent à la compréhension de l'environnement opérationnel réel ou potentiel.

Remarque : Le terme « renseignement » décrit également les activités qui mènent au produit, ainsi que les organisations qui les exécutent. BTD, fiche 738.

Ébauche

d. Les cyberattaques sont utilisées contre des cibles qui représentent une menace à la stabilité nationale ou à la légitimité du régime;

e. L'espionnage, la propagande et les attaques dans le cyberespace sont utilisés pour soutenir les priorités en matière de sécurité, influencer les événements et contrecarrer les menaces;

f. Certaines nations sont capables de lancer des cyberattaques perturbatrices ou destructrices pour soutenir des objectifs politiques et elles sont disposées à le faire.

Les cybermenaces les plus évoluées proviennent des services de renseignements et des services militaires d'états étrangers. Les gouvernements avancés sur le plan technologique, leurs forces militaires et les entreprises privées sont vulnérables au cyberespionnage parrainé par des États et aux cyberopérations perturbatrices. On peut s'attendre à ce que cette menace augmente au cours des prochaines années.

Les cyberopérations ennemies créent des menaces importantes pour les missions alliées menées dans le cyberespace ou au moyen de celui-ci, où les ennemis peuvent interdire l'accès aux capacités opérationnelles où les manipuler; mener des collectes de renseignements rapides et régulières; et mener des activités de déception. L'enjeu opérationnel est donc de s'assurer de la liberté d'action des FAC dans le cyberespace en défendant les capacités des FAC en appui aux objectifs militaires.

Dans un contexte militaire, alors que l'utilisation du cyberespace est devenue essentielle aux opérations, les adversaires potentiels, y compris les intermédiaires étatiques et les acteurs non étatiques, développent rapidement des moyens cybernétiques d'exploiter les vulnérabilités inhérentes aux systèmes de C4ISR sur lesquels l'armée dépend, ainsi que les technologies opérationnelles comme les systèmes de combat.

Le taux élevé d'innovation technologique, la domination des logiciels commerciaux et la prolifération croissante d'entités dotées de logiciels intégrés et immuables signifient que le potentiel de cyberattaque dépassera les capacités de défense.

a. L'utilisation continue de technologie commerciale signifie que les vulnérabilités des systèmes peuvent être connues, échangées et grandement exploitées. L'interdépendance fondée sur des réseaux reliés rend d'importants systèmes très vulnérables à un effondrement rapide et catastrophique, ce qui nécessite une étape de réparation prolongée. À mesure que le nombre de cybertransactions augmente, la proportion relative d'attaques peut diminuer. Toutefois, le risque d'attaques catastrophiques ne cesse d'augmenter;

Ébauche

b. La prolifération d'appareils avec des systèmes intégrés — l'Internet des objets — ajoute un nouveau danger. Les appareils seront durables, vulnérables aux attaques, et il sera impossible de corriger leur logiciel;

c. L'utilisation par l'État d'armes de cyberattaque ne sera pas limitée principalement en raison de son efficacité et de l'anonymat que procure le cyberespace, ce qui rend certaines attaques pratiquement impossibles à retracer.

3.4 Concept d'opération

Le concept d'opération (CONOPS) définit les rôles et les responsabilités de la cyberforce des FAC, ainsi que les processus et les outils qui formeront la capacité CD-DAR du MDN/des FAC. Il fournit une description de la nouvelle capacité et des conditions dans lesquelles elle fonctionnera, des processus qui seront utilisés pour sécuriser et défendre le cyberenvironnement du MDN/des FAC et de la façon dont les commandants, les cadres, l'état-major et les cyberopérateurs interagiront avec la solution CD-DAR.

Le CONOPS se concentre sur l'emploi des forces (EF)[10] des cybercapacités défensives de la solution CD-DAR pour surveiller et défendre les réseaux du MDN et des FAC, y compris la capacité de détecter, d'analyser et de répondre aux menaces. La capacité CD-DAR fournira également une analyse contextuelle fiable pour soutenir les décisions et les actions du MDN/des FAC dans la conduite de COD au sein des extensions et interfaces désignées du R comd et des systèmes déployables du RED (réseau désigné - protégé B et moins). L'IRSC (réseau classifié - Secret), qui fait partie du R comd au sein du MDN/des FAC, constitue une partie importante de la portée du projet CD-DAR.

Se référer au CONSUP du projet CD-DAR pour plus de détails.

3.5 Concept de soutien

Le concept de soutien (CONSUP) définit un cadre proposé pour gérer le projet CD-DAR en tant que capacité. Il délimite le cadre de gestion pour fournir une approche intégrée de la définition, du développement, de l'institutionnalisation, de la maintenance et de l'évolution de la capacité CD-DAR. Ce cadre de gestion des capacités (CGC) permettra de clarifier la responsabilité, l'obligation de rendre compte et le processus d'acquisition de la capacité et le cycle de vie du soutien, de l'élaboration du concept à l'acquisition et à la mise en œuvre de la capacité, puis à la mise en service, au soutien en service et à l'élimination.

Se référer au CONSUP du projet CD-DAR pour plus de détails.

[10] Au niveau opérationnel, l'emploi des forces fait référence au commandement, contrôle et maintien en puissance des forces affectées, Banque terminologique de la Défense (BTD), Fiche 32173.

ébauche

3.6 Rôles clés

a. Commandants des FAC. Les commandants des FAC, jusqu'au CEMD inclusivement, sont responsables du C2 des forces affectées, y compris la cyberforce;

b. Personnel de soutien aux opérations. Le personnel de soutien opérationnel comprend toutes les personnes du MDN et des FAC qui fournissent un soutien direct et indirect aux activités de planification et d'exécution de la mission du commandant stratégique et opérationnel des FAC. Ils sont souvent situés au quartier général;

c. Personnel fournisseur de services. Le personnel qui met en œuvre et la solution CD-DAR et qui la met à la disposition des utilisateurs. Le CORFC est inclus pour le soutien opérationnel ainsi que pour le traitement des incidents et des événements de sécurité. Le rôle d'opérateur cybernétique est également inclus;

d. Autorité opérationnelle (AO). L'AO est définie comme la personne qui a le pouvoir de définir les exigences et les principes opérationnels, d'établir des normes et d'accepter le risque dans son secteur de responsabilité; l'AO est responsable envers le Chef d'état-major de la Défense (CEMD)[3]. En supposant qu'il n'y aura pas de changements importants à l'organisation et à la gouvernance de la TI dans un avenir prévisible, le Directeur d'état-major de l'État-major interarmées stratégique (DEM EMIS) sera l'AO pour l'infrastructure dans le cadre de la solution CD-DAR;

e. Responsable technique (RT). Le RT est désigné comme la personne qui possède l'autorité d'établir des normes et des exigences techniques, de gérer les configurations, de formuler des conseils techniques et de surveiller le respect des éléments dans son domaine de responsabilité[11]. En supposant qu'il n'y aura pas de changements importants à l'organisation et à la gouvernance de la TI dans un avenir prévisible, le SMA(GI) sera le RT pour l'infrastructure dans le cadre de la solution CD-DAR;

f. Responsable de la sécurité. Le responsable de la sécurité est désigné comme la personne qui a l'autorité de relever les risques, de fournir des conseils et des normes de sécurité en vue de leur approbation par les responsables opérationnels et techniques, et de veiller à la conformité à ces normes dans son domaine de responsabilité. En supposant qu'il n'y aura pas de changements importants à l'organisation et à la gouvernance de la TI dans un avenir prévisible, le SMA(GI)/Directeur – Sécurité (Gestion de l'information) (Dir Sécur GI) sera le responsable de la sécurité pour l'infrastructure dans le cadre de la solution CD-DAR;

g. Autorité d'instruction. L'autorité d'instruction est désignée comme le commandant d'instruction ou d'un commandement qui est responsable d'un groupe professionnel

[11] 2700-1 (SJS J6), 10 November 2017

Ébauche

militaire ou d'une branche et qui commande un centre de soutien de l'apprentissage et un ou plusieurs établissements d'instruction ou centres d'expertise fonctionnels. En supposant qu'il n'y aura pas de changements organisationnels importants dans un avenir prévisible, l'École d'électronique et des communications des Forces canadiennes (EECFC) sera l'autorité d'instruction pour les capacités offertes dans le cadre de ce projet;

h. Mentorat et développement des capacités. Cela consiste à guider les cyberopérateurs à tous les niveaux pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences. Plus concrètement, le rôle du mentor est d'entraîner, de former et de guider les cyberopérateurs pour qu'ils réalisent leur mission grâce à la transformation opérationnelle continue, au développement des compétences, au développement et à la coordination de l'instruction collective, et au développement et au soutien des outils cybernétiques.

3.7 Tâches clés[12]

Tous les cyberopérateurs et les autres utilisateurs (gestionnaires, cadres supérieurs, commandants et leurs états-majors) accomplissent leurs tâches dans un seul environnement intégré. Ces tâches comprennent : le flux de travail, le suivi, l'analyse, l'alerte, la production de rapports, la connaissance de la situation, les interventions et l'instruction (individuelle et collective). Chaque cyberopérateur a accès à un outil de visualisation du tableau de bord commun, adapté à son rôle et à ses responsabilités particulières.

La CS du domaine cybernétique est regroupée au niveau du CORFC (par l'entremise de la solution CD-DAR) et transmise au personnel clé, comme les cadres supérieurs, les commandants, les gestionnaires et d'autres éléments opérationnels du réseau du MDN et des FAC, comme la Marine royale canadienne (MRC), l'Aviation royale canadienne (ARC), l'Armée canadienne (AC), le Commandement des opérations interarmées du Canada (COIC), le Commandement des Forces d'opérations spéciales du Canada (COMFOSCAN) et l'État-major interarmées stratégique (EMIS). La CS du domaine cybernétique peut être transmise par la Capacité de gestion interarmées de l'espace de bataille (CGIEB) et intégrée à la CS des autres domaines opérationnels, c.-à-d. les forces aériennes, maritimes, terrestres, spatiales et d'opérations spéciales.

La solution CD-DAR appuie un certain nombre de tâches et de fonctions liées aux cyberopérations qui ont été définies dans la Note de doctrine interarmées sur les cyberopérations pour appuyer les opérations de réseau, les cyberopérations de soutien, la cybersécurité et les scénarios de cyberdéfense. Les tâches et les fonctions des COD seront analysées plus à fond ultérieurement.

[12] Extrait du concept de cyberopérations défensives, version 1.0, 14 octobre 2018

3.7.1 Se préparer aux cyberopérations défensives (COD)

La mise en place d'une opération de cyberdéfense doit répondre à quatre questions clés :

a. Qu'est-ce que nous essayons de protéger?

b. Quelles sont les menaces possibles contre ce que nous essayons de protéger?

c. Comment essayons-nous de détecter ces menaces?

d. Comment réagissons-nous lorsque nous détectons une manifestation de menace?

Les cyberopérations défensives commencent par ce que l'on prévoit défendre. Il est évident qu'une infrastructure de réseau de niveau secret contient des données secrètes, c'est donc un point de départ. L'impossibilité d'obtenir les données exactes et véridiques dont vous avez besoin, en temps voulu, a le même effet potentiel que l'absence de ces données.

Il existe de nombreux outils qui aideront à créer et à gérer les actifs matériels et logiciels existants d'une organisation, de sorte que le bon ensemble de technologies, de personnes et de processus peut être assemblé à partir des produits commerciaux sur étagère (COTS) et des produits gouvernementaux sur étagère (GOTS). Cependant, très peu de fournisseurs comprennent votre activité et les données que vous utilisez pour mener à bien vos opérations, et il existe donc très peu d'outils que vous pouvez acquérir pour vous aider dans cette activité. Néanmoins, envisagez de créer et de maintenir un inventaire des actifs de données au moment où vous préparez la gestion des informations et des événements de sécurité (GIES) et les outils connexes pour gérer vos actifs logiciels et matériels. L'identification de l'information que vous essayez de protéger et de l'infrastructure que vous utilisez pour y accéder, est la base de toute COD. Elle doit vous indiquer ce que vous essayez de protéger.

Comprendre ce que vous essayez de protéger vous permet d'encercler les wagons, mais comprendre ce qui se trouve à l'extérieur de ce cercle est crucial pour votre défense, il est donc tout aussi important de dresser et de maintenir un inventaire de vos menaces et des tactiques, techniques et procédures (TTP) utilisées par vos adversaires afin de préparer votre défense.

La compréhension et la connaissance proviennent d'une chose essentielle : les relations. Maintenir un inventaire de « tout » est utile, mais il devient vraiment utile pour la CS lorsque vous pouvez créer, maintenir et faire évoluer les liens entre les entités (personnes, lieux, choses et événements) sur de longues périodes de temps pour construire la connaissance et la compréhension, conduisant à la sensibilisation. Sans sensibilisation, vous n'avez pas la capacité de détecter les comportements normaux et anormaux et l'incursion d'un adversaire. Vous devez vous assurer que toute solution est capable d'acquérir des connaissances au moyen de relations, de la création et de l'exploitation de liens.

La détection directe d'éléments malveillants, à l'aide de signatures, de sources, de profils et de comportements connus, au moyen d'un antivirus (AV), d'un antipourriel (AP), d'un système de

prévention des intrusions (SPI) / SDI et d'autres produits de détection des logiciels malveillants, est une capacité intrinsèque de toutes les COD, mais il est nécessaire d'étendre ces capacités de détection pour qu'elles correspondent au niveau de sophistication des adversaires et des attaques actuels. La détection des éléments anormaux et sophistiqués ne peut se faire que grâce à l'étendue et à la profondeur des connaissances accumulées mentionnées ci-dessus. La détection des menaces sera fondée sur le mécanisme direct traditionnel, mais surtout sur votre développement de règles et d'analyses qui contribuent aux comportements heuristiques de vos outils de détection.

3.7.1.1 Établir l'avantage du terrain externe (ATE)

Si vous considérez le domaine cybernétique comme un portrait, l'avantage du terrain externe passe par la compréhension de vos adversaires et de leurs comportements pour lesquels vous devez mettre en place une défense. Bien que les adversaires soient nombreux et qu'il faille essayer d'en avoir une connaissance efficace et à jour, afin de prendre l'avantage, il est important de se rappeler qu'il existe de nombreuses forces opposées à celles-ci sous la forme des nombreuses organisations dont le travail consiste à mettre en place des cyberdéfenses.

Il est évident que le seul moyen de prendre l'avantage est l'interopérabilité et l'échange d'informations, avec des partenaires de sécurité de confiance et l'intégration de sources d'informations de sécurité de confiance, afin d'établir les connaissances défensives nécessaires pour mener une COD.

3.7.1.2 Établir l'avantage du terrain interne (ATI)

Dans le même ordre d'idées, l'établissement d'un avantage sur votre adversaire, pour votre cyberdomaine/portrait interne, signifierait que vous avez une compréhension complète de tous vos actifs internes (matériel, logiciel, réseau, etc.) et de ce qui se passe dans votre infrastructure de TI, de sorte que votre adversaire ne puisse pas s'implanter dans votre infrastructure interne. En tant que but ultime de la COD, il s'agit bien entendu d'un objectif très ambitieux, souvent déterminé par une série de mesures telles que :

a. Moyenne des temps de détection (MTD);
b. Moyenne des temps d'identification (MTI);
c. Moyenne des temps de confinement (MTC);
d. Moyenne des temps de réponse/résolution (MTRR);
e. Nombre de systèmes présentant des vulnérabilités connues;
f. Nombre de certificats Secure Sockets Layer (SSL) configurés de manière incorrecte;
g. Le volume de données transférées sur le réseau;
h. Nombre d'utilisateurs ayant un accès "super utilisateur".

Ébauche

Ce qui précède n'est qu'un petit échantillon des nombreuses mesures utilisées pour déterminer dans quelle mesure une organisation comprend son cyberdomaine interne.

3.7.1.3 Stratégie de surveillance axée sur les adversaires

La défense d'un réseau nécessite une stratégie de surveillance délibérée axée sur les adversaires (SSAA) afin que le défenseur du réseau puisse prévoir les activités des adversaires, s'y préparer et les voir.

Une SSAA complète doit permettre d'établir des liens directs entre les menaces, les efforts d'ingénierie et les actions de l'opérateur de COD, garantissant ainsi l'efficacité et l'efficience des opérations. Une stratégie de surveillance délibérée permet au défenseur de comprendre comment l'adversaire est susceptible d'attaquer (d'après une analyse du rendement des investissements [RI]), comment surveiller les attaques et comment les dissuader. Une SSAA apporte des réponses à ces questions :

a. Qui sont les acteurs de la menace auxquels nous sommes susceptibles de faire face et que souhaitent-ils obtenir comme résultats/effets et pourquoi?

b. Quelles sont les tactiques qui, compte tenu de l'architecture du réseau (comment seront-elles utilisées et où sont-elles situées), sont les plus susceptibles d'être utilisées pour atteindre les résultats de l'adversaire?

c. Quelles sont les capacités techniques disponibles, ou qui peuvent être mises à disposition au sein du réseau en particulier pour soutenir la surveillance?

d. Comment les capacités techniques peuvent-elles être combinées pour répondre aux besoins de la communauté de la défense et de la sécurité - en maximisant l'utilité défensive et en minimisant la liberté d'action et le RI de l'adversaire.

3.7.1.4 Validation et essais

La fonction de validation et d'essai est un effort continu destiné à garantir l'efficacité et l'efficience des plans techniques, des mesures de protection et des mécanismes de coordination pour les COD, et se compose de deux activités :

a. Mettre à l'essai la conception de toutes les capacités opérationnelles;

b. Valider l'efficacité des mises en œuvre dans le temps.

La validation et les tests doivent être exécutés par la communauté du Génie dans le cadre de leurs responsabilités en matière de conception, d'intégration et de maintenance des écosystèmes de COD. Cela favorise des relations de travail plus étroites entre la communauté du Génie et la communauté opérationnelle.

Ébauche

3.7.2 Opérations de préparation aux COD

Les opérations de préparation aux COD sont techniquement une composante de la préparation aux COD, car elles établissent les conditions de réussite de l'exécution de la COD. Elles servent de mécanisme pour garantir l'application et l'intégration efficaces des activités de préparation aux activités d'exécution de la COD. Les opérations de préparation aux COD sont également nécessaires pour garantir que les informations générées par l'exécution de la COD orientent et réorientent la *préparation aux COD* et le soutien au COD. Les activités précises comprennent :

a. Fixer des conditions précises pour assurer le succès d'une mission de COD et pour qu'elle puisse être réactive à toute mission ou exigence opérationnelle ;

b. Mener des activités à forte intensité en ressources afin d'apporter les changements nécessaires pour comprendre les nouvelles menaces et "rendre la situation normale". (Voir encadré);

c. Définir les conditions pour qu'une mission de CDO puisse soutenir une tâche opérationnelle, de sécurité ou du renseignement.

3.7.3 Exécution de la COD

Les sous-sections ci-dessous décrivent brièvement les activités désignées comme faisant partie de l'exécution de la COD.

3.7.3.1 Surveillance

La fonction de surveillance consiste à observer les événements préoccupants et à les signaler soit pour répondre – comprendre, soit pour répondre – neutraliser. Les événements peuvent être générés par des signatures, des analyses de modèles de comportement, des notifications de tiers ou des alertes provenant de déclencheurs définis dans le SSC. Les institutions MITRE, SysAdmin, Audit, Network and Security (SANS) et le National Institute of Standards and Technology (NIST) sont quelques exemples de stratégies de surveillance utilisées par la COD.

3.7.3.2 Activités de réponse

Au moment où un événement se produit, les options dont dispose l'attaquant ont déjà été évaluées dans le cadre des fonctions d'ATI et d'ATE, et le plan de surveillance a été élaboré dans le cadre de la fonction SSAA, ce qui garantit que le système est instrumenté pour surveiller les activités que l'adversaire voudrait entreprendre.

Il existe trois types fondamentaux d'options de réponse : *Répondre – Comprendre, Répondre – Neutraliser*, et *Répondre – Tromper*. Tous les événements finiront par être neutralisés, la question clé est de savoir combien d'activités de compréhension et de déception sont nécessaires avant que cela ne se produise, pendant que cela se produit, ou après. Les connaissances acquises sont enregistrées et utilisées pour de futures COD.

Ébauche

3.7.3.2.1 Triage des cyberévénements

Le processus de triage des cyberévénements vise à déterminer si un événement nécessite une COD. Il s'agit d'examiner si l'événement est susceptible de favoriser les résultats de l'adversaire ou de constituer une partie identifiable des activités de l'adversaire. Les événements qui présentent un lien potentiel avec les résultats de l'adversaire doivent être désignés comme des événements nécessitant une COD. Les connaissances acquises sont enregistrées et utilisées pour de futures COD.

3.7.3.2.2 Répondre – Comprendre

Une fois qu'un événement nécessitant une COD est détecté, une analyse de l'événement est effectuée pour déterminer l'action requise. Les décisions sont prises en fonction d'une analyse technique visant à comprendre les mécanismes de l'attaque, d'une analyse du renseignement et d'une analyse de la situation.

Les deux tâches les plus importantes de la COD sont :

a. Comprendre ce que l'adversaire a fait techniquement sur le système;

b. Ce que l'adversaire essaie d'obtenir.

Dans certains cas, les activités nécessaires pour comprendre un événement nécessitant une COD pourraient inclure des opérations de recherche du renseignement ou la contre-ingérence.

3.7.3.2.3 Répondre – Neutraliser

L'objectif de *Répondre - Neutraliser* est de désactiver ou de rendre inopérants les cyberoutils techniques de l'adversaire et peut être réalisé à n'importe quelle étape du processus d'intervention. Les activités de neutralisation de la menace doivent être mises en œuvre par le soutien en service (SES) et le Génie, sous la direction de la COD et avec l'autorisation du commandant responsable. Toute défense contre une menace immédiate qui est scénarisée et préapprouvée peut être neutralisée par l'opérateur de COD directement.

3.7.3.2.4 Doctrine de réponse

Les activités d'intervention technique de la COD sont similaires à la méthode de l'industrie « détecter, comprendre, répondre et restaurer » avec quelques éléments supplémentaires (voir le concept de la COD pour plus de détails). L'adoption de la doctrine et des pratiques exemplaires de l'industrie permet des opérations efficaces et efficientes en permettant le recours à des conseillers tiers, à un soutien commercial, à une formation commerciale de base et en améliorant la durabilité globale de la capacité.

3.7.3.3 Activités de déception

Une opération de déception dans le cyberenvironnement n'est pas fondamentalement différente d'une opération de déception dans le monde réel. Des efforts sont faits pour désinformer, confondre, distraire et retarder un adversaire. Il est également possible d'obtenir des renseignements sur un adversaire en fonction de la façon dont il interagit avec une

Ébauche

déception délibérée, ce qui peut être extrêmement utile dans le cas où un adversaire compétent est amené à divulguer des outils ou des tactiques qui n'ont pas été observés auparavant. Les actions peuvent également être analysées pour discerner l'intention réelle et la cible de cet adversaire.

Les activités de déception comprennent les activités délibérées proactives et les actions de *Répondre – Tromper* qui se produisent en réponse à un événement particulier.

Les types d'opérations de déception peuvent inclure:

a. La mise en œuvre de pots de miel, y compris les environnements modernes assistés par l'apprentissage machine qui visent à capter et à maintenir l'attention d'un attaquant;

b. La surveillance d'ensembles d'espaces IP délibérément inutilisés afin de détecter les tentatives de reconnaissance du réseau interne et de mouvement latéral;

c. L'introduction de processus, d'agents ou de comptes d'utilisateurs qui agissent comme des fils-pièges;

d. La publication d'information externe comprenant de l'information qui peut être utilisée comme fil-piège ou comme indicateur de reconnaissance.

Les activités de déception entraînent souvent l'exposition d'outils, de tactiques et de savoir-faire sensibles de l'adversaire, qui est obligé d'interagir avec des dispositifs et des logiciels qui tentent précisément de comprendre ses activités.

3.7.3.4 Interdiction défensive externe

L'interdiction défensive externe (IED) est une catégorie d'action qui peut être demandée par le MDN/les FAC à une tierce partie commerciale ou d'un état étranger lorsque cette tierce partie prend une mesure qui a une valeur défensive pour le MDN/les FAC. Les mesures prises par un tiers tirent parti de la position de ce tiers dans l'environnement mondial des télécommunications ou de ses autorités nationales qui ont la capacité juridique de bloquer, de modifier, de ralentir ou de rediriger des éléments de communications malveillantes destinées au MDN/aux FAC.

3.7.4 Fonctions de soutien du la COD

La viabilité et l'efficacité à long terme de la fonction de COD exigent que des fonctions de soutien précises soient conçues et mises en œuvre parallèlement aux fonctions essentielles de la COD. Les fonctions de soutien essentielles de la COD comprennent :

a. Innovation et avantage;

b. Génie de la COD;

c. Opérations de réseau (NetOps) / Maintenance.

Ébauche

Les sous-sections ci-dessous décrivent brièvement les activités désignées comme faisant partie des fonctions de soutien de la COD.

3.7.4.1 Innovation et avantage

La fonction de COD doit être maintenue dans un état où elle possède des avantages sur les adversaires.

La mise en place d'un avantage comporte les étapes suivantes [13] :

a. Déterminer les avantages potentiels;

b. Comprendre la technologie;

c. Valider le contexte et la valeur de l'avantage;

d. Mettre en place l'avantage où et quand il est nécessaire.

Ces avantages ont un effet dissuasif sur les adversaires potentiels et soutiennent une série d'activités ministérielles au-delà de la COD, notamment l'assurance de mission, les opérations de sécurité et la sécurité des TI.

L'innovation et l'avantage sont bien plus qu'un projet de recherche et développement (R et D) traditionnel, principalement en raison de l'éventail d'informations qu'ils prennent en compte, et parce que l'activité se termine par la livraison d'un outil concret. Pour ce faire, la fonction innovation et avantage est responsable des résultats suivants :

a. Définir l'orientation des initiatives de R et D;

b. Définir les orientations et les exigences pour les petits et grands projets d'immobilisations des horizons 0, 1 et 2 qui soutiennent la COD;

c. Diriger l'amélioration des processus et promouvoir un changement de culture au sein de la COD et de ses fonctions de soutien;

d. Définir les exigences pour les cyberexercices des FAC ou tout autre exercice auquel les ressources de COD des FAC participent.

Cela permet de rester proche des technologies de la génération actuelle et de donner un avantage par rapport aux adversaires.

3.7.4.2 Génie des COD

Les capacités de COD nécessitent des efforts dédiés et continus du Génie. Ces efforts commencent traditionnellement une fois que la technologie future ou le nouveau besoin est identifié et progressent à travers des étapes telles que le prototypage, l'élaboration des besoins, les travaux de conception, l'approvisionnement et la mise en service.

[13] Les détails de chaque étape se trouvent dans le concept de cyberopérations défensives, version 1.0, daté du 14 octobre 2018.

Ébauche

L'adoption du nouveau concept de COD exige une augmentation importante du rôle de la communauté du Génie de la sécurité, car le MDN et les FAC cherchent à créer des avantages techniques, à former un terrain externe et interne, à vaincre des adversaires hautement capables, à exécuter les fonctions opérationnelles de COD en tirant parti des systèmes de gestion des connaissances et des actions, et à élaborer des solutions efficaces pour défendre les réseaux déployés et les systèmes de mission pour le combattant. Les systèmes que l'opérateur de COD utilisera pour défendre tous les systèmes du MDN/des FAC doivent être construits, configurés et adaptés pour répondre aux nouvelles exigences.

Lorsqu'ils sont bien exécutés, les travaux du Génie sont l'élément central qui permet l'utilisation efficace et efficiente de la COD dans les systèmes nationaux, déployés et de mission. On ne saurait trop insister sur leur importance.

La fonction du Génie pour ce concept comprend ces rôles en particulier :

a. Le développement de solutions intégrées : Dans ce contexte, une solution intégrée fait référence à l'intégration de la plateforme, à l'intégration architecturale et à l'intégration dans différents environnements techniques;

b. Mesures techniques de COD du Génie et mesures de réponse de COD : Ensemble de capacités, appelées mesures techniques de COD, qui nécessitent une conception, une ingénierie et des tests. Les capacités temporaires de défense, d'atténuation, de correction ou de dissuasion d'une attaque, appelées mesures de réponse de COD, doivent être conçues et testées;

c. Intégration (ou étiquetage) des capacités de COD dans l'architecture de référence de la cybersécurité (ARCS) : Au fur et à mesure que des capacités de COD sont déterminées, elles doivent être soit étiquetées comme étant des capacités de COD, soit saisies et comptabilisées comme un nouveau composant de l'architecture;

d. Achats prépositionnés : La fonction du Génie mettra en œuvre un système d'achats prépositionnés qui permettra aux projets et aux missions d'adopter rapidement les meilleures technologies actuelles. Pour ce faire, la fonction du Génie obtiendra et maintiendra de manière proactive des véhicules et des stocks contractuels pour soutenir des déploiements rapides, comme l'exige la politique PSE. Cette stratégie offre une flexibilité opérationnelle et la possibilité de s'assurer que les systèmes de mission ne sont pas envoyés dans des cyberenvironnements contestés sans les capacités requises. Cette activité est un catalyseur direct de la mission, dont l'absence entraînerait un risque direct et incontestable pour la mission.

e. Fournir un soutien technique pour toutes les phases de la COD : des conseils d'experts sur les capacités et ce qu'elles peuvent fournir sont nécessaires. Ces conseils sont essentiels pour gérer les incidents, comprendre le véritable contexte

Ébauche

technique d'une menace et élaborer des approches nuancées des menaces et des risques.

3.7.4.3 Opérations / maintenance de réseaux

L'exécution de la COD exige que les ressources aient la capacité de se concentrer sur ce qui est le plus important pour la fonction de COD. L'accent mis sur les résultats de l'adversaire permet de faire la distinction entre le fait de contrer un résultat et celui de mener des opérations de réseau. Bien qu'elles soient délimitées, ces deux activités ne doivent pas être considérées comme distinctes ou sans rapport entre elles, car elles sont, en termes très réalistes, hautement interdépendantes et complémentaires.

La liste suivante énumère certaines interdépendances entre les activités d'opérations de réseau et les COD :

a. Les COD et les opérations de réseau nécessitent l'accès à la plupart des mêmes outils;

b. Les données recueillies par les opérations de réseau doivent tenir compte des exigences de la fonction de COD, et vice versa;

c. Les processus utilisés par les opérations de réseau doivent tenir compte des exigences de la fonction de COD et vice versa;

d. Prendre des mesures pour identifier, comprendre ou répondre à un incident ou une menace est un sous-ensemble des mesures prises pour gérer un réseau. Les mécanismes opérationnels, les processus, les mécanismes d'audit et les capacités de suivi des opérations de réseau sont des catalyseurs directs de la COD.

Bien qu'interdépendantes, l'exécution de ces deux séries d'activités doit rester distincte dans la mesure du possible.

3.7.5 Systèmes de gestion des connaissances et des actions

Le développement d'une capacité de COD compétente et maintenable exige que l'ensemble de la fonction soit axé sur les données, les informations et les connaissances. Bien qu'elle ne soit pas arrivée à maturité, la volonté de créer un système répondant à ces exigences est toujours là. Par conséquent, la définition complète de ce qui est nécessaire pour les systèmes de gestion des connaissances et des actions pour les COD demandera des efforts, mais certaines caractéristiques de haut niveau incluent notamment les suivantes :

a. Une suite d'analyse du renseignement et un dépôt de connaissances sur le renseignement;

b. Une suite de surveillance intégrée (GIES, Détection et intervention aux points d'extrémité (DIPE), etc.);

Ébauche

c. Des outils de gestion du risque opérationnel automatisés et axés sur les événements;

d. Une automatisation de la gestion des risques de sécurité, de la conformité et de la gestion des vulnérabilités;

e. Un inventaire des cybercapacités qui comprend des caractéristiques de planification pour la planification et l'exécution des COD;

f. Une capacité de gestion des incidents d'entreprise qui fournit une base de connaissances incorporée pour aider à la résolution ou à la neutralisation des événements;

g. Un lien avec les outils de gestion des opérations de réseau ou leur mise en œuvre.

3.8 Caractéristiques de l'utilisateur

Tous les cyberopérateurs et autres utilisateurs (gestionnaires, cadres, commandants et leur personnel) exécutent leurs tâches dans un environnement intégré unique. Ces tâches comprennent : le flux de travail, le suivi, l'analyse, l'alerte, la production de rapports, la connaissance de la situation, les MI et l'instruction (individuelle et collective). Chaque cyberopérateur dispose d'un outil commun de visualisation du tableau de bord, personnalisable en fonction de son rôle et de ses responsabilités.

La CS du domaine cybernétique est regroupée au niveau du CORFC (par l'entremise de la solution CD-DAR) et transmise au personnel clé, comme les cadres supérieurs, les commandants, les gestionnaires et d'autres éléments opérationnels du réseau du MDN et des FAC, comme la MRC, l'ARC, l'AC, le COIC, le COMFOSCAN et l'EMIS. Au besoin, la CS du cyberdomaine est transmise à la CGIEB du MDN/des FAC pour être intégrée à la CS des autres aspects opérationnels des missions et des opérations des FAC.

La solution CD-DAR soutient un certain nombre de tâches et de fonctions liées aux cyberopérations qui ont été définies dans la note de doctrine interarmées sur les cyberopérations pour appuyer les opérations de réseau, les cyberopérations de soutien, la cybersécurité et les scénarios de cyberdéfense. Les tâches et fonctions des COD seront analysées plus en détail ultérieurement.

3.8.1 Cyberopérateurs

Les cyberopérateurs sont l'épine dorsale de la cyberforce. Il s'agit du personnel, à tous les niveaux hiérarchiques, dont le rôle principal est de : « détecter, reconnaître et identifier les cyberentités hostiles ou autrement non autorisées et contribuer à la destruction, à la neutralisation, à la suppression ou à l'élimination de l'ennemi dans le cyberespace et par d'autres moyens ».

Ébauche

Les cyberopérateurs dirigent les COD, assurent la liaison et travaillent en collaboration avec d'autres ministères et organismes, ainsi qu'avec les alliés du Canada, afin d'améliorer la capacité du MDN et des FAC de fournir un cyberenvironnement sécurisé. Ils surveillent les réseaux de communication des FAC afin de déceler toute tentative d'accès non autorisé et d'intervenir face à celles-ci. Ils fourniront aussi un cyberappui afin de combler les besoins opérationnels des FAC Compétences des cyberopérateurs.

Il ne faut pas confondre le métier de cyberopérateur avec celui de technicien des systèmes d'information et de télécommunications aérospatiales (SITA), de spécialiste des systèmes de communication et d'information de l'Armée de terre (SSCIAT), d'opérateurs d'équipement d'information de combat (Marine) (OP EICM), et les métiers des communicateurs navals (COMM N). Ces groupes professionnels militaires s'occupent principalement de la configuration, l'installation, l'exploitation et la maintenance des réseaux de communication et de l'ITI, tandis que les cyberopérateurs se concentrent sur la surveillance et la protection de l'ITI contre les menaces hostiles et le refus de l'utilisation du cyberespace par les forces hostiles. Les 26 emplois pour les cyberopérateurs (CYBEROP, 00378) peuvent être exécutés par le personnel de la force régulière ou de la réserve, sauf pour le poste le plus élevé dans le groupe professionnel, c'est-à-dire celui de conseiller cybernétique.

Les cyberopérateurs sont formés et éduqués à l'art de la cyberguerre en portant une attention particulière aux aspects suivants :

a. la nature du cyberespace et du domaine cybernétique;
b. les menaces, les acteurs de la menace et leur impact sur le cyberespace;
c. les principes et techniques de détection, de reconnaissance, d'identification et d'attribution de toutes les natures des entités cybernétiques;
d. les principes et techniques des COD, y compris les mesures de défense internes (MDI) et les mesures d'intervention (MI);
e. les tactiques, techniques et procédures (TTP) pour :
    i. la coordination du soutien cybernétique;
    ii. le commandement et contrôle;
    iii. la cyberreconnaissance;
    iv. la cybersurveillance;
    v. la gestion des cyberincidents;
    vi. la criminalistique cybernétique;
    vii. l'identification des cybermenaces;

Ébauche

viii. les fonctions du Centre des cyberopérations.

4 DIRECTIVES RELATIVES AU PLAN ET À LA CONCEPTION

La solution CD-DAR permettra au MDN et aux FAC de mener des opérations de cybersécurité et donnera au CORFC/COSD la capacité de fournir des CS cybernétiques, de défendre les environnements de réseau du MDN et des FAC et de mener des COD. À cette fin, la capacité doit pouvoir effectuer plusieurs fonctions essentielles.

4.1 Travaux et services inclus

Bien que plusieurs outils pour la cybersécurité soient nécessaires pour satisfaire aux exigences de la solution CD-DAR, en théorie, les éléments ou composants clés fonctionnels recherchés peuvent être regroupés comme suit :

a. La capacité de maintenir la CS, au moyen d'une ICSO, des alertes, des menaces et des mesures correctives dans l'ensemble du réseau de commandement du MDN et des FAC, et d'alimenter la connaissance de la situation aux fins de prise de décisions et l'exécution des interventions par des interfaces normalisées et des flux de travail automatisés à l'appui du soutien à la décision de l'élément de commandement, et la mise en œuvre des interventions selon les directives.

   Comme décrit à la section 2.4, l'ICSO est malléable et adapté aux besoins de chaque commandant, qu'ils soient au niveau stratégique, opérationnel ou tactique. Elle offre une marge de manœuvre dans les vues opérationnelles pour consolider les informations destinées aux commandants. Elle fonctionne également sur des réseaux indisponibles, peu fiables, fournissant une CS d'environnement cybernétique local, ou dont la capacité est limitée (épisodique);

b. Capacité de créer et de tenir à jour un dépôt des cyberdonnées (CDR) faisant autorité qui comprend des données de cyberrenseignement multisources à intégrer (hébergées et exploitées avec des applications et un dépôt fiable) dans le réseau de commandement assigné en tant que système cohésif;

c. La capacité d'effectuer une découverte automatisée ou sur demande de cyberentités et d'événements afin d'identifier et de suivre rapidement tous les actifs (autorisés et non autorisés) connectés au réseau de commandement et d'évaluer leurs attributs en matière de vulnérabilité, de configuration, de risque et de conformité aux correctifs;

d. La capacité d'effectuer une surveillance automatisée de la cybersécurité afin d'identifier rapidement la présence d'entités ou de comportements cybernétiques

Ébauche

non conformes, d'événements, d'alertes, de vulnérabilités ou d'autres changements de statut des entités dans le cyberespace du MDN/des FAC;

e. La capacité d'effectuer les activités essentielles liées à la sécurité comme la gestion des biens, l'évaluation des vulnérabilités, le contrôle de documents, la gestion de la configuration et les fonctions du changement de configuration telles que l'évaluation de la sécurité et le processus d'autorisation;

f. La capacité de recueillir, de conserver et d'analyser continuellement des renseignements sur les cybermenaces dans l'environnement du réseau de commandement et de détecter et de caractériser les activités suspectes fournit un contexte pour les évaluations des risques et des vulnérabilités en temps quasi réel;

g. La capacité d'effectuer la gestion automatisée des tâches (GT) pour identifier, contenir et éradiquer une menace de façon adaptative et dynamique;

h. La capacité d'utiliser un système intégré d'entraînement opérationnel pour s'assurer que les cyberopérateurs, les gestionnaires, les cadres et les autres opérateurs sont à jour et maîtrisent leurs tâches, rôles et responsabilités dans le système intégré, y compris :

    i. la capacité de créer une simulation de menace, de pénétration et d'attaque opérationnelle pour exercer l'équipe de cyberopérateurs et évaluer leur état de préparation opérationnelle ainsi que leur efficacité;

    ii. un composant d'entraînement opérationnel individuel axé sur les opérateurs individuels (tâches, rôles, progrès dans leur rôle);

    iii. une instruction axée sur les compétences et la validation des cyberopérateurs, opérateurs et civils dans leur rôle attribué autant au niveau individuel que collectif;

    iv. un composant d'instruction collective pour une capacité d'opération de sécurité pour la cyberdéfense. Il s'agit d'une réplique d'un ensemble de systèmes d'exploitation avec des ensembles de données hors ligne pour permettre une gamme complète de fonctions et de scénarios réalistes à des fins d'instruction.

4.1.1 Sources de données du cyberdomaine

À l'heure actuelle, le renseignement sur les menaces est partagé avec une quinzaine d'organisations et d'unités organisationnelles internes (p. ex. COMRENSFC, COIC, CEMA) et externes (p. ex. CST, CCC, Gp5, partenaires de l'OTAN), vraisemblablement dans une gamme de formats et de niveaux d'automatisation. Il s'agit d'une forme d'information essentielle à la cybersécurité et à la défense internes et partagées qui mérite une plus grande attention.

Ébauche

4.1.2 Capacités déployées

L'un des principaux moteurs du projet CD-DAR est de défendre la liberté d'action[14] des commandants opérationnels. Le projet CD-DAR fournira aux commandants de théâtre la capacité d'accéder au cyberdomaine pour les opérations par l'intermédiaire du cyberespace; il assurera la fiabilité de l'information transmise/échangée dans le cyberespace du MDN et des FAC; il aura une capacité d'accès en situation de largeur de bande intermittente et faible, et pourra tirer parti des capacités de détection et d'intervention déployables dès qu'elles seront disponibles. Il est particulièrement crucial pour le déploiement et la capacité locale de tirer parti des mesures de sécurité et de défense automatisées dès qu'elles deviennent disponibles.

4.1.2.1 Navire de combat canadien

Le navire de combat canadien est la plateforme de la MRC qui doit remplacer les frégates de la classe Halifax. Étant donné que le navire de combat canadien peut être chargé d'agir en tant que quartier général d'une force opérationnelle interarmées en mer, il devra être en mesure de mener des COD de ses environnements de réseau respectifs. Par conséquent, le projet CD-DAR a pour mandat de doter le navire de combat canadien de capacités similaires à celles de tout autre quartier général (QG) terrestre de la FOI.

4.2 Travaux et services exclus

Le projet CD-DAR n'évaluera et/ou ne recommandera pas de produits ponctuels, y compris des produits de sécurité, sauf dans la mesure où ils contribuent à améliorer la posture de sécurité globale des domaines mandatés qu'il cible. Par exemple, les caractéristiques d'un produit qui ne contribuent pas à la cybersécurité présentent peu d'intérêt, sauf si elles contribuent à l'intégration et/ou à l'interopérabilité et à l'amélioration de la posture de cybersécurité. Les caractéristiques qui, bien entendu, dégradent la posture de cybersécurité des domaines ciblés, sont d'un grand intérêt lors de l'évaluation et des tests, mais là encore, le contexte sera toujours celui de la posture de sécurité globale. Par exemple, la capacité d'un progiciel antivirus à s'intégrer dans un GIES et/ou un tableau de bord cyberopérationnel (TBCO)/une ICSO est plus intéressante que la convivialité de son interface utilisateur graphique (IUG) pour l'utilisateur final (on s'attend à ce qu'un autre groupe évalue et sélectionne des produits individuels en fonction de caractéristiques et de capacités autres que celles liées à la vision des capacités du CD-DAR).

4.3 Utilisation de la technologie

Il est prévu que la solution CD-DAR soit un amalgame de technologies qui, une fois intégrées dans une solution finale, répondront aux aspirations du projet en matière de souplesse,

[14] La **liberté d'action** est la capacité d'employer des forces avec peu ou pas de contraintes. Il s'agit donc de pouvoir opérer dans le cyberenvironnement en ayant la certitude que cet environnement sera disponible et qu'on pourra s'y fier en cas de besoin.

Ébauche

d'adaptabilité, de longévité et d'efficacité dans la réalisation de COD. Certaines des technologies clés comprennent :

a. Outils logiciels de gestion de l'information et des événements de sécurité (GIES) – La pierre angulaire de la COD est la connaissance de votre cyberportrait. De quoi est-il fait? Comment est-il utilisé? Qu'est-ce qui constitue un comportement "normal"? Quand quelque chose change? Est-ce que nous nous attendions à ce changement? Quand nous attendons-nous à ce que les choses se produisent? Quels sont les risques, les menaces et les adversaires que nous pouvons rencontrer? Comment devons-nous nous attendre à ce qu'ils se comportent?

   En tant qu'êtres humains, nous nous posons et répondons constamment à ces questions chaque jour, pour être conscients des choses qui nous entourent. C'est ce que les outils GIES font pour notre ITI; et il y a une foule d'outils de ce type disponibles. Nous en aurons besoin. Nous devrons les intégrer, les comprendre et les contrôler/diriger, pour pouvoir mener des COD efficaces. Nous devons être en mesure de peindre notre portrait [cybernétique] jusqu'au moindre coup de pinceau, afin de voir ce qui ne va pas dans le tableau dès que cela se produit.

b. Plateformes de mégadonnées/lac de données – Il ne fait aucun doute que les outils GIES (ci-dessus) génèrent un flot de données qui submergent rapidement les approches traditionnelles de stockage des données et les rendent inutiles. En outre, l'analyse, l'augmentation et la convolution que nous ferons pour transformer ces données en informations utiles doubleront, tripleront, voire décupleront cette quantité, sans parler de la quantité de ces données que nous devons conserver et pendant combien de temps. Les technologies de mégadonnées et de lac de données devront être incorporées simplement pour survivre à une mise en œuvre initiale.

   Les lacs de données, ou plus exactement les ***réservoirs de données*** (puisque tout ce qui les concerne doit être contrôlé pour éviter qu'ils ne soient submergés, et soit qu'ils nous inondent, soit qu'ils se transforment en "marécages" de données), doivent être conçus/architecturés et pris en charge afin de garantir que chaque élément de données est accessible, utilisable et régi pour apporter de la valeur à la solution et à l'organisation dans son ensemble.

c. Intelligence artificielle / apprentissage machine (IA/AM) – L'intelligence artificielle (IA) et l'apprentissage machine (AM), deux concepts distincts bien que souvent pris ensemble, offrent un certain nombre d'avantages pour les COD. L'IA consiste à observer et à comprendre l'environnement d'une manière humaniste, et à être capable de réagir dans un contexte similaire. L'AM consiste à utiliser cette compréhension pour construire et conserver des connaissances, qui peuvent ensuite être utilisées pour prendre des mesures. Dans le contexte de la cybersécurité, elles

Ébauche

peuvent être utilisées pour détecter et automatiser, semi-automatiser ou déclencher une réponse à une [cyber] menace ou à un [cyber] incident, avec une intervention [flux de travail] automatisée, semi-automatisée ou manuelle similaire qui atténuera ou vaincra l'action malveillante. L'utilisation de cette technologie constitue une part importante de la capacité d'innovation et prospective du projet CD-DAR.

d. Analyse des schémas comportementaux – L'analyse des schémas comportementaux est généralement un résultat ou une fonction de l'IA/AM. C'est en déterminant et en mémorisant ce qui est un comportement "normal" (ou en se faisant dire ce qui est normal) que l'on détecte le comportement anormal des adversaires. Elle facilite les activités de surveillance en automatisant une partie de l'observation des événements dans le cyberdomaine afin de trouver d'éventuelles menaces et/ou activités qui devraient être examinées et confirmées comme "normales" ou "anormales" et, dans ce dernier cas, elle fournit le mécanisme permettant de déclencher une alerte. Elle peut être très efficace si on lui apprend de manière appropriée ce qu'il faut rechercher.

e. Plateformes infonuagiques – Les plateformes infonuagiques ont démontré leur efficacité, pour certaines charges de travail, en fournissant des ressources d'infrastructure plus simples, plus réactives et plus évolutives comme composantes de l'ITI. Le projet CD-DAR cherchera à utiliser cette technologie de deux manières.

   Premièrement, comme le ministère cherche à utiliser la technologie d'infonuagique comme élément de son ITI, la solution doit vérifier les implications de l'utilisation de cette technologie du point de vue de la cybersécurité, et s'assurer que la solution reste vigilante quant à l'utilisation de la technologie d'infonuagique, ses risques, ses vulnérabilités et son intégrité dans le contexte de la cybersécurité.

   Deuxièmement, la solution CD-DAR pourrait tirer parti des technologies de l'infonuagique pour fournir sa solution afin de bénéficier de son approche de l'affectation des ressources, de ses aspects d'autoréparation et de sa capacité à évoluer en fonction des besoins, sans efforts importants requis de la part de techniciens et administrateurs des services de TI.

4.4 Concept

Le projet de CD-DAR servira à acquérir une solution de cyberdéfense (qui se traduit en capacités) dans le but d'améliorer l'aide à la décision en général et la sécurité du cyberespace du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'y réagir. La solution intégrée fournira une analyse contextuelle fiable à l'appui des décisions et des mesures du MDN et des FAC à l'intérieur d'extensions et d'interfaces désignées du réseau de

Ébauche

commandement (R comd) ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables à l'appui de la conduite de COD.

La solution comprendra des capacités de COD qui comprennent les suivantes, sans s'y limiter :

a. **Détection de matériel non autorisé** : Prévenir et corriger l'utilisation non autorisée de matériel sur l'ITI du MDN/des FAC principalement en mettant en œuvre le contrôle de sécurité critique (CSC) nº 1 du Centre for Internet Security (CIS). Le projet CD-DAR fournira un moyen automatisé d'identifier tous les dispositifs de TI connectés au réseau, leur emplacement (logique et physique) et leur configuration;

b. **Détection des logiciels non autorisés** : Prévenir et corriger l'utilisation non autorisée de logiciels sur l'ITI du MDN/des FAC principalement en mettant en œuvre le CSC nº 2 du CIS. Le projet CD-DAR fournira un moyen automatisé d'identifier tous les logiciels installés sur le réseau, leur emplacement (logique et physique) et leur configuration.

   En ce qui concerne les entités (c.-à-d. le matériel et les logiciels) installées sur le réseau, la capacité fera en particulier ce qui suit:

   i. Normaliser les noms des entités;

   ii. Identifier automatiquement toutes les entités et leurs configurations (autorisées et non autorisées);

   iii. Fournir topologiquement une carte de réseau visuelle de toutes les entités;

   iv. Suivre automatiquement toutes les entités connectées au réseau (autorisées et non autorisées);

   v. Maintenir une base de données sécurisée des entités autorisées;

   vi. Valider automatiquement l'identité de l'entité autorisée;

   vii. Répondre automatiquement à la découverte d'entités non autorisées;

c. **Privilèges administratifs non autorisés** : Prévenir et corriger les privilèges administratifs matériels et logiciels non autorisés, généralement excessifs, sur l'ITI du MDN/des FAC principalement en mettant en œuvre le CSC nº 5 du CIS. Le CD-DAR fournira une capacité permettant d'assurer l'utilisation appropriée des comptes administratifs.

   Cette capacité fera en particulier ce qui suit :

   i. Normaliser les noms des entités;

Ébauche

ii. Identifier automatiquement toutes les entités et leurs configurations (autorisées et non autorisées);

iii. Suivre les comptes administratifs;

iv. Maintenir une base de données sécurisée des entités autorisées;

v. Évaluer les comptes administratifs pour assurer la conformité et la cyberdéfense;

vi. Répondre automatiquement à la découverte d'entités non autorisées;

d. **Mauvaises configurations** : Prévenir et corriger les configurations non autorisées sur l'ITI du MDN/des FAC principalement en mettant en œuvre le CSC nº 3 du CIS. Le projet CD-DAR fournira un moyen automatisé d'analyser la conformité aux configurations autorisées.

Plus précisément, la conformité de la configuration permettra ce qui suit :

i. Normaliser les noms des entités;

ii. Identifier automatiquement toutes les entités et leurs configurations (autorisées et non autorisées);

iii. Suivre automatiquement toutes les entités connectées au réseau (autorisées et non autorisées);

iv. Déclencher et consigner automatiquement les informations relatives à la conformité de la configuration et alerter et faire rapport automatique sur celles-ci;

v. Évaluer automatiquement la conformité aux configurations de base en tenant compte de la probabilité de compromission et de l'identification des entités critiques à l'appui de la priorisation;

e. **Vulnérabilités connues** : Prévenir et corriger les vulnérabilités connues sur l'ITI du MDN/des FAC principalement en mettant en œuvre le CSC nº 4 du CIS. Le projet CD-DAR fournira un moyen automatisé d'analyser les vulnérabilités des configurations existantes.

Plus précisément, la conformité des vulnérabilités permettra ce qui suit :

i. Normaliser les noms des entités;

ii. Identifier automatiquement toutes les entités et leurs configurations (autorisées et non autorisées);

Ébauche

iii. Suivre automatiquement toutes les entités connectées au réseau (autorisées et non autorisées);

iv. Déclencher, enregistrer, alerter et signaler automatiquement les vulnérabilités connues;

v. Évaluer automatiquement les répercussions des vulnérabilités connues en tenant compte du type d'entité du cyberespace du MDN du point de vue du système ou du service, de l'ensemble de la chaîne de destruction, de la probabilité de compromission et de l'identification des entités critiques afin de soutenir la priorisation;

vi. Déterminer, acquérir, installer et vérifier automatiquement les correctifs requis pour tous les produits et systèmes, y compris les systèmes d'exploitation, les applications, les commutateurs, les routeurs et les dispositifs;

f. **Sécurité des fichiers :** Prévenir et corriger les étiquettes de fichiers incorrectes pour certains types de fichiers de données, assurer l'application de la chaîne de possession dans les fichiers de données et appliquer des politiques d'information précises sur l'ITI du MDN/des FAC. Le projet CD-DAR produira automatiquement et appliquera l'étiquetage des données à l'appui des politiques de contrôle des documents liées aux transferts de fichiers interdomaines.

Plus précisément, la fonctionnalité de transfert de fichiers interdomaines permettra ce qui suit :

i. Surveiller et détecter les événements associés au trafic réseau;

ii. Surveiller et détecter les événements associés aux utilisateurs;

iii. Automatiser l'étiquetage des données des fichiers;

iv. Assurer l'application de l'étiquetage des données des fichiers;

g. **Activités anormales** : Surveiller et corriger les activités adverses visant à infiltrer l'ITI du MDN/des FAC, à en subvertir l'utilisation appropriée et à en exfiltrer les données. Le projet CD-DAR fournira une capacité de DIPE.

Plus précisément, la défense des points d'extrémité permettra ce qui suit :

i. Rassembler et regrouper :

1) de nouveaux ensembles de données et métadonnées selon les besoins;

2) des données détaillées concernant l'état actuel de chaque appareil d'extrémité (comme les processus en cours d'exécution, les réglages de

Ébauche

registres, les fichiers actuellement ouverts, les connexions actives au réseau, le compte d'utilisateur en cours d'utilisation et les détails matériels comme l'utilisation de la mémoire et de l'unité centrale de traitement [CPU]);

3) des données criminalistiques (historiques) des appareils d'extrémités (comme les processus exécutés, les fichiers ouverts et créés, les applications/commandes/scripts utilisés, les comptes d'utilisateur utilisés et les applications installées);

4) cueillette à distance des images de la mémoire ou des fichiers pour une enquête judiciaire;

5) des images du disque dur (serveur, poste de travail ou portable) pour une enquête judiciaire;

6) des données par paquets complets;

7) des données brutes de trafic réseau pour la collecte hors bande;

8) des données à l'appui de l'analyse judiciaire;

9) des données d'inventaire des entités;

10) des données de gestion de la configuration;

11) des données sur les utilisateurs accrédités;

12) des données sur l'identité des administrateurs accrédités;

13) des données sur les vulnérabilités;

14) des données de renseignement sur les menaces;

15) le renseignement de sources ouvertes (OSINT) pour l'analyse multisources et multiconditions (OS16);

ii. Surveiller, déclencher, enregistrer, alerter et signaler automatiquement les événements :

1) Absorber et corréler les données du SDI et de GIES;

2) Événements de cyberentités;

3) Événements de trafic réseau à travers les domaines / conditions;

4) Événements d'utilisateur;

iii. Soutenir les enquêtes et les analyses :

Ébauche

1) Effectuer des analyses rétrospectives en corrélant les événements historiques, les tendances et les comportements avec les événements en temps réel; reconstituer les activités d'après le contexte/les métadonnées; et soutenir la chasse aux menaces persistantes avancées (MPA), aux menaces internes et aux indicateurs au moyen d'une analyse personnalisée des données historiques à court terme;

2) Répondre aux exigences du GC en matière de chaîne de possession numérique;

3) Absorber et corréler les données d'évaluation de la sécurité et d'autorisation;

iv. Une intervention :

1) Pour les situations préautorisées, exécution automatique avec possibilité d'outrepasser manuellement, enregistrement et rapport des interventions techniques;

2) Identifier, définir, automatiser, consigner les flux de travail en réponse aux incidents, et faire rapport sur ceux-ci.

4.5 Évaluation de la sécurité et autorisation (ESA)

Une ESA complète sera menée conformément au Guide d'évaluation de la sécurité et autorisation (GESA), ce qui donnera lieu à la promulgation d'une directive appropriée relativement à la mise en place du matériel et des logiciels, au recours au personnel et à la mise en œuvre des procédures afin de satisfaire aux exigences en matière de sécurité propres aux capacités.

Ébauche

5 EXIGENCES EN MATIÈRE D'EFFICACITÉ DU SYSTÈME

Cette section définit les exigences en matière d'efficacité du système pour le projet CD-DAR. Ces exigences décrivent et détaillent les capacités requises par les FAC et doivent être utilisées en parallèle avec le CONOPS du projet CD-DAR.

Les exigences en matière d'efficacité du système ont été saisies au chapitre 9 – Tableau des exigences du présent document et complétées par les exigences de rendement présentées à la section 6.

La seule mesure du succès des produits livrables du projet sera fondée sur la satisfaction des exigences de la COI et de la COF, décrites respectivement dans les sections 2.2 et 2.3, en conjonction avec le tableau des exigences présenté à la section 9.

5.1 Exigences générales

Les exigences communes pour le projet CD-DAR ont été définies à la section 9.1 du tableau des exigences.

Deux niveaux de mesure définissent les différentes exigences en matière de rendement : essentiel ou souhaitable.

5.1.1 Exigences essentielles

Une exigence essentielle est un critère permettant de garantir la conformité de la solution CD-DAR avec les exigences minimales relatives à la performance et aux opérations. La performance ainsi décrite est jugée à ce point importante que si une solution proposée répond à tous les critères souhaitables et à tous les autres critères essentiels sauf un, elle sera rejetée. Dans le présent document, le verbe devoir au présent (« doit ») désigne une exigence essentielle.

5.1.2 Exigences souhaitables

Les exigences souhaitables servent à évaluer de façon plus approfondie des éléments de la solution qui satisfont à toutes les exigences essentielles. Une exigence souhaitable décrit une exigence liée au rendement selon laquelle on considère qu'un rendement plus élevé que le niveau essentiel stipulé revêt une valeur opérationnelle importante. Dans le présent document, les verbes devoir au conditionnel (« devrait ») et pouvoir au conditionnel (« pourrait ») désignent une exigence souhaitable.

5.1.3 Avertissement concernant les niveaux de mesure

La stipulation d'un critère essentiel suppose que celui-ci est réalisable à un coût raisonnable. Toutefois, dans l'éventualité où une exigence essentielle serait jugée par la suite impossible à respecter pour des raisons techniques ou financières, elle sera réévaluée. Les critères de performance établis dans l'EBO ne peuvent être modifiés qu'avec l'approbation du DP, après consultation du GP.

Ébauche

5.2 Opérabilité

La solution CD-DAR fournira des capacités de sécurité et de défense des TI partout où les extensions et interfaces du R comd, tant statiques que déployées, et les systèmes RED déployables désignés sont accessibles. Il s'agit des environnements durables, des environnements épisodiques, des environnements collaboratifs et des cyberenvironnements qui ont été décrits à la section 3.2.

Les exigences d'opérabilité ont été définies dans le tableau des exigences de la section 9. Ces exigences précisent les besoins du projet pour les phases de découverte, d'analyse, de réponse et d'évolution de la cyberdéfense (voir le cadre d'analyse du projet CD-DAR à la figure 2).

5.3 Surviabilité

En tant que système primaire et critique pour le COD, la solution CD-DAR sera utilisée par les opérateurs cybernétiques, les gestionnaires, les cadres supérieurs et les autres opérateurs 24 heures sur 24, 7 jours sur 7. Les exigences relatives à la fiabilité, à la disponibilité et à la maintenabilité du système doivent répondre à ce besoin opérationnel et doivent être soutenues et entretenues conformément au CONSUP du projet.

L'architecture du système doit être conçue de manière à ce que chaque équipement puisse être réparé, entretenu et remplacé avec un impact minimal sur le fonctionnement de la capacité.

La capacité doit être efficace dans tous les environnements opérationnels, comme il est indiqué à la section 3.2 du présent EBO, puisque la solution CD-DAR sera intégrée au réseau hôte en tant que capacité interne. Le système doit, dans la mesure du possible, être conçu pour résister aux menaces identifiées à la section 3.3 du présent EBO, grâce à l'utilisation de technologies adaptatives et d'analyses intégrées à la solution CD-DAR.

Les exigences de surviabilité ont été définies dans le tableau des exigences de la section 9. Ces exigences précisent les besoins du projet pour les phases de découverte, d'analyse, de réponse et d'évolution de la cyberdéfense.

5.4 Maintainabilité

En tant que système primaire et critique pour le COD, la solution CD-DAR sera utilisée par les opérateurs cybernétiques, les gestionnaires, les cadres supérieurs et les autres opérateurs 24 heures sur 24, 7 jours sur 7. Les exigences relatives à la fiabilité, à la disponibilité et à la maintenabilité du système doivent répondre à ce besoin opérationnel et doivent être soutenues et entretenues conformément au CONSUP du projet.

Le système doit être réparé et fonctionner comme il est déterminé par la catégorisation de sécurité (anciennement l'énoncé de sensibilité) et le processus d'évaluation de la sécurité et d'autorisation (ESA).

Ébauche

Le système doit utiliser des fonctions de surveillance et de contrôle de la santé dans l'infrastructure existante des FAC pour surveiller et maintenir l'exploitation nominale de la solution CD-DAR.

L'architecture du système doit être conçue de manière à ce que chaque équipement puisse être réparé, entretenu et remplacé avec un impact minimal sur le fonctionnement de la capacité.

Les pannes prévues, nécessaires à l'entretien et à la mise à niveau planifiés du système, doivent être relativement rares, de courte durée et sans incidence sur l'ITI du MDN et des FAC. Afin de maintenir le rythme opérationnel, le système doit pouvoir être rétabli à sa configuration opérationnelle minimale (à définir plus tard) rapidement. Par conséquent, tous les efforts raisonnables doivent être faits pour rétablir la configuration opérationnelle minimale ou meilleure en raison d'une panne imprévue et menant à une exploitation nominale complète.

Cette capacité devrait être déployée sur des plates-formes matérielles de qualité commerciale standard. Ainsi, la configuration matérielle du système doit répondre aux exigences de maintenabilité pour ce matériel. De plus, tout logiciel de développement doit être élaboré à l'aide des pratiques exemplaires de l'industrie afin d'assurer un niveau élevé de fiabilité et de facilité d'entretien.

On s'attend à ce que la communauté d'utilisateurs et la fonctionnalité du système évoluent au fil du temps. Pour répondre au besoin d'évolution, le système doit appliquer les pratiques exemplaires et les lignes directrices de l'industrie afin de s'assurer que le logiciel et le système de la capacité sont évolutifs, extensible et modifiable, tout en restant interopérables avec les autres ministères et les partenaires alliés.

Les exigences de maintenabilité ont été définies dans le tableau des exigences de la section 9. Ces exigences précisent les besoins du projet pour les phases de découverte, d'analyse, de réponse et d'évolution de la cyberdéfense.

5.5 Disponibilité

En tant que système primaire et critique pour le COD, la solution CD-DAR sera utilisée par les opérateurs cybernétiques, les gestionnaires, les cadres supérieurs et les autres opérateurs 24 heures sur 24, 7 jours sur 7. Les exigences relatives à la fiabilité, à la disponibilité et à la maintenabilité du système doivent répondre à ce besoin opérationnel et doivent être soutenues et entretenues conformément au CONSUP du projet.

Afin de maintenir le rythme opérationnel, le système doit pouvoir être rétabli à sa configuration opérationnelle minimale rapidement. Par conséquent, tous les efforts raisonnables doivent être faits pour rétablir rapidement la configuration opérationnelle minimale ou meilleure en raison d'une panne imprévue et menant à une exploitation nominale complète. Les pannes prévues, nécessaires pour l'entretien et les mises à niveau prévues, doivent également être de courte durée et relativement rares.

Ébauche

La solution CD-DAR doit pouvoir effectuer une surveillance et une analyse localisées et appuyer la prise de décisions responsables au sein de réseaux régionaux déconnectés, intermittents et limités géographiquement, même lorsqu'il est déconnecté d'un point de gestion central. La solution CD-DAR déployée doit rendre le même niveau de disponibilité que la capacité durable lorsqu'elle fonctionne dans des environnements déconnectés, intermittents et limités géographiquement.

Les exigences de disponibilité ont été définies dans le tableau des exigences de la section 9. Ces exigences précisent les besoins du projet pour les phases de découverte, d'analyse, de réponse et d'évolution de la cyberdéfense.

5.6 Fiabilité

Pour répondre à la disponibilité opérationnelle requise, la solution CD-DAR doit être hautement fiable, tel que défini par la disponibilité des capacités de CD-DAR, avec un taux de défaillance relativement faible.
Les exigences de fiabilité ont été définies dans le tableau des exigences de la section 9. Ces exigences précisent les besoins du projet pour les phases de découverte, d'analyse, de réponse et d'évolution de la cyberdéfense.

5.7 Durabilité environnementale

La solution CD-DAR doit satisfaire aux normes de gérance environnementale du MDN. Le MDN et les FAC ont adopté le code de gérance environnementale suivant. Le MDN et les FAC doivent :

a. intégrer les facteurs environnementaux aux autres considérations pertinentes (opérations, finances, sécurité, santé, développement économique, etc.) qui entrent en ligne de compte dans la prise de décision;

b. respecter, sinon dépasser la lettre et l'esprit de la législation fédérale;

c. au sein du MDN et des FC, accroître le niveau de sensibilisation à l'environnement par des séances de formation, et favoriser et reconnaître les initiatives du personnel qui mènent à des effets positifs sur l'environnement;

d. reconnaître que le cycle de vie de la gestion des matières dangereuses (sélection initiale, acquisition, utilisation, manutention, entreposage, transport et élimination) est un facteur essentiel de toute planification, particulièrement pour ce qui est de déterminer si l'acquisition des matières est vraiment nécessaire étant donné leurs caractéristiques (voir la DOAD 4003-1, *Gestion des matières dangereuses*);

e. assurer l'intégration des considérations environnementales dans les politiques et les pratiques en matière d'approvisionnement;

Ébauche

f. prendre des mesures pour prévenir la pollution associée aux activités et opérations quotidiennes par des moyens économiques de réduction de la consommation des matières premières, des substances toxiques, de l'énergie, de l'eau et d'autres ressources, et de diminution du volume des déchets et du bruit;

g. acquérir, gérer et aliéner les terres sans nuire à l'environnement, notamment en protégeant les aires écologiquement importantes.

Les exigences de durabilité environnementale ont été définies dans le tableau des exigences de la section 9. Ces exigences précisent les besoins du projet pour les phases de découverte, d'analyse, de réponse et d'évolution de la cyberdéfense.

5.8 Analyse comparative entre les sexes plus (ACS+)

À rédiger une fois que l'ACS+ aura été réalisée pour le projet.

5.9 Santé et sécurité

La solution ne doit pas causer d'autres préoccupations sur le plan de la santé et de la sécurité que celles qu'impose l'environnement d'exploitation, pour les opérateurs. Elle doit être conforme avec tous les codes de santé et sécurité du MDN et des FAC.

Les exigences de santé et sécurité ont été définies dans le tableau des exigences de la section 9. Ces exigences précisent les besoins du projet pour les phases de découverte, d'analyse, de réponse et d'évolution de la cyberdéfense.

5.10 Exigences en matière de livraison

La quantité de dispositifs nécessaires pour répondre aux exigences du projet CD-DAR est une composante de la conception d'architecture et des livrables de l'intégrateur de système principal (ISP) et ne peut être précisée à l'heure actuelle.

Les ISP sont encouragés à faire appel à des entreprises autochtones dans le cadre de l'engagement du GC à favoriser le développement économique des communautés autochtones du Canada.

5.11 Exigences en matière d'efficacité des sous-systèmes

S. O. Tout composant de sous-système pour le projet CD-DAR doit répondre aux exigences principales du projet pour les sections ci-dessus.

Ébauche

6 MESURES DE RENDEMENT

Les mesures de rendement sont présentées ci-dessous sous la forme de paramètres de rendement du système selon les conventions suivantes :

a. ***Indicateur de rendement*** : titre indiquant le type de mesure du rendement;

b. ***Description du rendement*** : une description de l'indicateur de rendement;

c. ***Quantité (Qté)*** : valeur de l'indicateur à atteindre;

d. ***Unité de mesure*** : unité dans laquelle la quantité est mesurée.

6.1 Mesures au niveau du système

ID de l'objectif de rendement	Indicateur de rendement	Description	Qté
OREN.1	Lien entre entités	Détecter qu'une cyberentité devient active (connectée) dans le cyberespace du MDN et des FAC. (p. ex., un ordinateur portable a été connecté au réseau, un utilisateur a ouvert une session, une clé USB a été branchée à un ordinateur, etc.).	À déterminer
OREN.2	Prévention automatique des attaques	Éviter automatiquement une attaque contre le réseau ou le processeur central par l'utilisation d'un outil de protection comme le système de prévention des intrusions sur l'hôte.	À déterminer
OREN.3	Entrée de vérification et affichage de la console GIES	Créer une entrée de vérification et l'envoyer à la console de gestion de l'information et des événements de sécurité (GIES).	À déterminer
OREN.4	Analyse automatique des anomalies des fichiers	Extraire automatiquement des fichiers d'une source, comme des pièces jointes d'un courriel ou un téléchargement du réseau, les exécuter dans une chambre de détonation et les analyser pour déceler des signes d'activités malveillantes.	À déterminer
OREN.5	Alerte automatique du SDI et affichage de la console	Déclencher une alerte dans le système de détection d'intrusion (SDI), puis envoyer l'alerte et les paquets associés à la console GIES.	À déterminer

ébauche

ID de l'objectif de rendement	Indicateur de rendement	Description	Qté
OREN.6	Détection des attributs des entités	Déceler si la cyberentité détectée dans le cyberespace du MDN et des FAC est humaine ou non, et découvrir ses caractéristiques clés.	À déterminer
OREN.7	Identification et emplacement de l'entité	Cerner suffisamment de caractéristiques clés de la cyberentité détectée dans le cyberespace du MDN et des FAC pour déterminer son identité et sa position (physique et logique) précises.	À déterminer
OREN.8	Caractérisation de l'intention	Établir la caractéristique opérationnelle précise de la cyberentité détectée dans le cyberespace du MDN et des FAC pour la classer comme amie, ennemie ou Inconnue afin d'appuyer une décision d'engagement.	À déterminer
OREN.9	Recherches et collecte de données mensuelles dans le système	Rechercher dans les registres mensuels pour tout système dans le cyberespace du MDN et des FAC et recueillir les résultats.	À déterminer
OREN.10	Corrélation entre entités malveillantes et alertes	Créer des tableaux croisés dynamiques pour aider les cyberopérateurs à identifier les entités avec un comportement malveillant similaire ou relié et avertir l'opérateur afin qu'il puisse amorcer des mesures d'intervention.	À déterminer
OREN.11	Récupération des captures de paquets d'une entité selon les critères	Extraire les captures de paquets (PCAP) indexées d'une semaine de la mémoire en ligne avec des critères liés à l'entité comme des adresses IP, noms d'hôte, ports, comptes d'utilisateurs ou contenu.	À déterminer
OREN.12	Reconnaissance de l'événement inquiétant et mesure	Reconnaître un événement inquiétant et le marquer comme anodin ou remplir un incident et l'envoyer au tiers 2.	À déterminer
OREN.13	Isolation de l'hôte infecté	Isoler un hôte infecté.	À déterminer

Ébauche

ID de l'objectif de rendement	Indicateur de rendement	Description	Qté
OREN.14	Identification et contact du propriétaire de l'incident	Déterminer, puis contacter l'administrateur de système, l'officier de la sûreté ou l'officier des opérations au site contenant le système lié à l'incident potentiel.	À déterminer
OREN.15	Déploiement du cycle de vie des SDI, à la flotte de capteurs	Développer, télécharger, mettre à l'essai et déployer les signatures SDI à une flotte de capteurs.	À déterminer
OREN.16	Élaboration d'un plan d'intervention de multiples systèmes ou comptes	Identifier, analyser et développer un plan d'intervention contre une intrusion dans de multiples systèmes ou comptes.	À déterminer
OREN.17	Analyse de la charge utile des maliciels des niveaux 2 et 3	Fournir l'analyse de la charge utile pour une nouvelle souche de virus au tiers 2 et tiers 3.	À déterminer
OREN.18	Définition et rétablissement des flux de données en panne	Identifier et rétablir les capteurs ou les flux de données en panne.	À déterminer
OREN.19	Information des intervenants sur les incidents majeurs	Réunir les intervenants et les informer des détails de l'incident majeur en cours.	À déterminer
OREN.20	Signature de la flotte des SDI ou purge du contenu GIES	Purger mensuellement/trimestriellement toutes les signatures déployées à la flotte SDI ou tout le contenu déployé à la console GIES.	À déterminer
OREN.21	Mise à l'essai et recommandation des correctifs majeurs	Mettre à l'essai et recommander des correctifs majeurs à l'entreprise.	À déterminer
OREN.22	Analyse et documentation du contenu sur les incidents graves	Tout en adhérant aux normes de la chaîne de possession légale :	À déterminer

Ébauche

ID de l'objectif de rendement	Indicateur de rendement	Description	Qté
		• Analyser et documenter le contenu du système impliqué dans l'incident majeur • Déployer une équipe d'intervention en cas d'incident • Récupérer les données • Trier les données	
OREN.23	Analyse criminalistique à distance	Extraire à distance les artéfacts criminalistiques à des fins d'analyse et de preuve. • Fichiers • Processus • Mémoire • Registre • Image du disque dur virtuel • Image du disque dur au niveau des bits	À déterminer
OREN.24	Évaluation de l'intention d'un adversaire	Évaluer les actions et les intentions potentielles d'un adversaire qui opère par des réseaux circonscrits.	À déterminer
OREN.25	Analyse, rapport et présentation	Rapporter les résultats d'analyse et présenter des preuves juridiquement recevables.	À déterminer
OREN.26	Opérationnalisation du cycle de vie des outils d'analyse personnalisés	Développer, déployer et rendre opérationnel des outils adaptés complexes de détection et d'analyse comme ceux utilisés dans les scripts pour Perl et GIES.	À déterminer
OREN.27	Base de référence des COD du cycle de vie des IPO	Réviser, examiner et créer une base de référence pour une instruction permanente d'opérations (IPO) pour une opération de cybersécurité défensive interne.	À déterminer
OREN.28	Mise en pratique des nouvelles procédures	Exercer les nouvelles procédures durant les quarts de travail des cyberopérateurs.	À déterminer
OREN.29	Avis de menace et de vulnérabilité émergentes	Informer les cyberopérateurs des nouvelles menaces et vulnérabilités.	À déterminer

Ébauche

ID de l'objectif de rendement	Indicateur de rendement	Description	Qté
OREN.30	Opérationnalisation des nouvelles techniques de défense	Créer de nouvelles techniques de défense fonctionnelles avec les nouvelles TTP.	À déterminer
OREN.31	Opérationnalisation des nouvelles techniques de défense fondées sur des outils	Créer de nouvelles techniques de défense fonctionnelles avec de nouveaux outils pour traiter les menaces nouvellement identifiées et priorisées.	À déterminer
OREN.32	Évolution de la posture de sécurité	Améliorer la posture de sécurité globale (politiques, processus, outils) du cyberespace vulnérable du MDN et des FAC pour traiter les menaces nouvellement identifiées et priorisées.	À déterminer
OREN.33	Perte de données	Aucune perte de paquets aux points de présence surveillés	À déterminer
OREN.34	Perte de données	Aucune perte de journal des événements	À déterminer
OREN.35	Perte de données	Aucune perte de renseignement	À déterminer
OREN.36	Intégrité des données	Intégrité des données vérifiables	À déterminer
OREN.37	Surveillance des données	Empêcher les adversaires de détecter (et d'éviter) la présence des capacités de surveillance.	À déterminer
OREN.38	Livraison d'événements de données	Assurer la livraison entière des événements de sécurité des appareils finaux au centre d'opérations de cybersécurité défensive tout en les protégeant d'accès ou de modification non autorisés.	À déterminer
OREN.39	Capacité de survie	Appuyer la surviabilité de la cybersécurité et les capacités des COD, même lorsque certains secteurs du cyberespace sont compromis ou contestés.	Vrai

Ébauche

ID de l'objectif de rendement	Indicateur de rendement	Description	Qté
OREN.40	Protection de la divulgation des documents	Protéger des divulgations non autorisées des documents et des registres de nature délicate maintenus par les capacités des opérations de la cybersécurité défensive.	Vrai

6.2 Mesures au niveau des sous-systèmes

Voir le tableau des exigences à la section 9.

Ébauche

7 BESOINS EN PERSONNEL ET EN INSTRUCTION

Pour être efficace, le système doit être exploité et soutenu par des ressources qualifiées affectées aux rôles clés, tels que définis à la section 3.6 ci-dessus.

La solution doit intégrer les pratiques exemplaires et mettre en œuvre l'apprentissage fondé sur les connaissances des opérations et mesures précédentes.

7.1 Besoins en personnel

La dotation de la solution CD-DAR comprendra le personnel militaire, les fonctionnaires et le personnel contractuel.

7.1.1 Personnel opérationnel

Le système sera utilisé par le personnel du MDN et des FAC qui se voit attribuer des rôles et des pouvoirs d'utilisateur accrédités au sein de la solution CD-DAR. D'autres utilisateurs temporaires et permanents seront ajoutés au besoin pour répondre aux exigences en matière de saisie de données pour les opérations et pour répondre aux besoins en matière de transfert de matériel et de capacité de pointe pour la préparation et la clôture des missions. Le personnel opérationnel affecté à ces postes sera doté par Cyber Uplift.

7.1.2 Personnel de maintenance

On prévoit que le système sera tenu à jour par le personnel du MDN et des FAC qui se voit attribuer la fonction de soutien respective à l'appui de la solution CD-DAR. Dans le cadre de la phase de définition, une analyse du SES sera menée, ainsi qu'une mobilisation continue de l'industrie, afin de déterminer une stratégie de maintenance qui offre le meilleur rendement, la souplesse et l'optimisation des ressources. Aujourd'hui, le CORFC est le gestionnaire du cycle de vie du matériel (GCVM) de facto pour la plupart des équipements et des logiciels cybernétiques existants.

7.2 Instruction

Afin de bien exploiter et soutenir la solution CD-DAR, un régime d'instruction efficace doit être fourni. L'instruction du cadre initial sera offerte dans le cadre de la portée du projet. Toutefois, l'instruction périodique sera donnée dans le cadre du SES de la capacité et sera la responsabilité de l'AO. L'AO peut déléguer au RT le pouvoir d'assurer la maintenance et la formation des administrateurs.

Le programme d'instruction sur la solution CD-DAR doit fournir une instruction supplémentaire sur le contenu du projet, fondée sur une approche d'instruction des formateurs, intégrée au programme d'instruction des COD du MDN et des FAC.

La solution doit être accompagnée de toute l'instruction nécessaire aux utilisateurs appropriés qui représentent l'autorité opérationnelle, aux cyberopérateurs et au personnel de soutien, conformément aux politiques et normes d'instruction des FAC et aux conclusions de l'évaluation des besoins d'instruction. Ceci englobe les installations, le matériel d'instruction et

Ébauche

les formateurs qualifiés nécessaires pour atteindre la capacité opérationnelle initiale et un système d'instruction continue pour assurer une capacité opérationnelle totale.

7.2.1 Évaluation des besoins d'instruction

Une évaluation des besoins en perfectionnement professionnel (EBPP) complète sera effectuée, définissant les orientations concernant la spécialité professionnelle, les qualifications préférées du groupe professionnel militaire (GPM), la durée de l'instruction, les grades préférés et les profils de carrière.

7.2.2 Environnement d'instruction

La vision de la cyberdéfense sur le plan décisionnel, d'analyse et de la réponse est un environnement intégré unique qui permet la collaboration et la conduite de la cybersécurité et des COD dans de multiples domaines de classification variable. Cela comprend, mais sans toutefois s'y limiter, les personnes, les politiques, les processus et les outils nécessaires à la visualisation, à la gestion des tâches, à l'instruction individuelle et collective et à un référentiel de données accessible et exploitable menant à un domaine cybernétique défendable du MDN et des FAC.

La solution doit fournir un système d'entraînement opérationnel intégré pour s'assurer que les cyberopérateurs, les gestionnaires, les cadres et les autres opérateurs sont à jour et maîtrisent leurs tâches, rôles et responsabilités dans la solution CD-DAR intégrée, y compris :

a. la capacité de créer une simulation de menace, de pénétration et d'attaque opérationnelle pour exercer l'équipe de cyberopérateurs et évaluer leur état de préparation opérationnelle ainsi que leur efficacité;

b. un composant d'entraînement opérationnel axé sur les opérateurs individuels (tâches, rôles, progrès dans leur rôle);

c. une instruction axée sur les compétences et la validation des cyberopérateurs, opérateurs et civils dans leur rôle attribué autant au niveau individuel que collectif;

d. un composant d'instruction collective pour une capacité d'opération de sécurité pour la cyberdéfense. Il s'agit d'une réplique d'un ensemble de systèmes d'exploitation avec des ensembles de données hors ligne pour permettre une gamme complète de fonctions et de scénarios réalistes à des fins d'instruction.

La solution doit dispenser une capacité de simulation d'instruction pour appuyer l'instruction opérationnelle collective dans un contexte opérationnel personnalisable. Les scénarios pour les simulations de formation doivent être créés, maintenus, modifiés et exécutés par les cyberopérateurs à partir des systèmes et des postes de travail actuels dans un environnement de formation ou d'exercice. La solution doit intégrer les pratiques exemplaires et mettre en œuvre l'apprentissage fondé sur les connaissances des opérations et mesures précédentes.

Ébauche

7.2.3 Produits livrables pour l'instruction

Ceux-ci comprendront, mais pourraient ne pas être limités aux :

a. Plans d'instruction et matériel d'instruction avec les outils en ligne dans le cyberespace du MDN et des FAC :

   i. Instruction des membres du cadre initial d'instructeurs, axée à la fois sur l'instruction individuelle et collective des cyberopérateurs;

   ii. Instruction continue, axée à la fois sur l'instruction individuelle et collective des cyberopérateurs;

b. Une capacité de mentorat d'opération et de développement des capacités (MODC) est pévue afin de guider les cyberopérateurs pour améliorer leurs compétences et améliorer les cyberopérations des FAC afin d'assurer le maintien des compétences. Voir le CONOPS de la solution CD-DAR pour plus de détails.

Ébauche

8 JALONS

Jalon de gestion	Date de base	Date prévue	Date réelle	Autorité approbatrice	Variance (mois) [base - réelle]
FS(ID) - Approuvée (niveau le plus élevé)			Janv 2016	CCD	
Analyse des options – EBO – Approuvé			Avril 2019	CDF	
Analyse des options – Charte du projet – Approbation			Oct 2020	CEM Cyber	
AP / PD (Déf) – Approuvé (niveau le plus élevé)			Juin 2020	Conseil du Trésor	
Modification à la DI et publication de l'IQ provisoire	S. O.		Juil 2020	SPAC	
Publication de l'IQ	Oct 2020	Avril 2021		SPAC	+6 mois
Publication de la demande de propositions (DP) provisoire	Mars 2021	Mars 2022		SPAC	+13 mois
Mise en œuvre – Invitation à soumissionner – Approuvé	Fév 2022	Nov 2022		CGDG	+9 mois
Publication de la DP	Mai 2022	Déc 2022		SPAC	+7 mois
Mise en œuvre - Documents contractuels - finalisés	Déc 2022	Août 2023		CGDG	+8 mois
Réunion de planification initiale	Nov 2022	Oct 2023		SMA(Fin)	+11 mois
CGP	Féb 2023	Nov 2023		CGP	+9 mois
AP / PD (MO) – Approuvé (niveau le plus élevé)	Juin 2023	Mai 2024		Conseil du Trésor	+11 mois
Mise en œuvre – Contrat - Attribué	Sept 2023	Juil 2024		CGDG	+10 mois
Mise en œuvre – COI	Sept 2026	Août 2027		CEM Cyber	+12 mois
Mise en œuvre – COF	Sept 2027	Août 2028		CEM Cyber	+12 mois
Mise en œuvre – Clôture du projet	Déc 2027	Nov 2028		SMA(GI)	+12 mois
Dernière réunion du CSR (examen de l'état d'avancement)			Fév 2020		
Prochaine réunion du CSR (examen de l'état d'avancement)	Fév 2021	Fév 2021			

Ébauche

9 GLOSSAIRE

Terme	Description
Intelligence artificielle	L'intelligence artificielle (IA) est la simulation de processus d'intelligence humaine par des machines, en particulier des systèmes informatiques. Ces processus comprennent l'apprentissage (l'acquisition d'information et les règles d'utilisation de l'information), le raisonnement (l'utilisation de règles pour arriver à des conclusions approximatives ou définitives) et l'autocorrection.
Entité responsable des actifs	Matériel réel et souhaité, identité du logiciel, configuration, vulnérabilités connues et privilèges administratifs.
Autorisation	Le droit ou la permission qui est accordé à une entité du système pour accéder à une ressource du système.
Réseau de commandement	Réseau de communications qui relie un échelon de commandement à une partie ou à la totalité de ses échelons subalternes aux fins de commandement et de contrôle. L'infrastructure du réseau secret consolidé (IRSC) fait partie du réseau de commandement du MDN et des FAC. Le réseau de commandement comprend les extensions et les interfaces du R comd et les systèmes du RED déployables. Tout au long de ce document, l'expression « réseau de commandement » sera utilisée pour inclure les termes ci-dessus.
Attaque des réseaux informatiques	Une opération militaire qui vise à interdire l'accès aux systèmes des technologies de l'information ou à l'information qui y est hébergée ou à perturber, à détériorer ou à détruire cette information ou ces systèmes. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]
Défense des réseaux informatiques	Mesures visant à protéger, à surveiller, à analyser, à détecter et à aborder les activités non autorisées menées dans les systèmes d'information et des réseaux informatiques. Il s'agit également d'une mesure prise en vue d'assurer une protection aux réseaux de technologie de l'information contre les activités non autorisées, de surveiller les réseaux, d'analyser les activités, de repérer les activités non autorisées, de surveiller ces activités et de les contrer. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]

Exploitation des réseaux informatiques	Activité de collecte de renseignements ayant pour but d'avoir accès à des données et de les recueillir à partir d'un STI d'un adversaire, d'un adversaire éventuel ou d'une autre partie approuvée par le gouvernement du Canada, ou de contrôler ce STI. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]
Opérations de réseaux informatiques	Opérations comprenant les attaques de réseaux informatiques, la défense de réseaux informatiques et l'exploitation de réseaux informatiques. [Source : Politique provisoire du MDN et des FC sur les opérations du réseau informatique des FC, 21 novembre 2013]
Cyberactif	Dispositifs électroniques programmables et réseaux de communication, y compris le matériel, les logiciels et les données. [Source : North American Electric Reliability Corporation, Glossary of Terms Used in Reliability Standards 14 (25 mai 2012)]
Domaine cybernétique	Ensemble des domaines, des entités et des activités liés au cyberespace ou ayant une incidence sur celui-ci. Note de définition : Le domaine cybernétique comprend l'infrastructure dépendante et les personnes ou utilisateurs du cyberespace. [Source : Note de doctrine conjointe – Cyberopérations v6]
Cyberentité	Une cyberentité est définie comme « toute chose distincte ou tout acteur distinct qui existe dans l'infrastructure cybernétique [cyberespace] ».
Cyberenvironnement (ou Cyberterrain)	Réseau interdépendant de structures de TI, incluant Internet, les réseaux de télécommunications, les systèmes informatiques et les contrôleurs intégrés ainsi que les logiciels et les renseignements qu'ils contiennent. [Source : Introduction aux cyberopérations des FAC, février 2014]
Chaîne de cyberdestruction	Collecte des processus liés à l'utilisation de cyberattaques sur les systèmes.
Cyberopérations	Les cyberopérations sont définies comme la conduite d'opérations offensives, défensives et de soutien dont le principal but est l'atteinte des objectifs dans le domaine cybernétique ou au moyen du domaine cybernétique.

	[Source : Note de doctrine conjointe – Cyberopérations v6]
Cybersécurité	Ensemble des technologies, des processus, des pratiques et des mesures d'atténuation et d'intervention conçues pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés afin d'assurer la confidentialité, l'intégrité et la disponibilité. [Source : TERMIUM Plus®, Banque de données terminologiques et linguistiques du gouvernement du Canada, 9 octobre 2014.]
Cybermenace	Une cybermenace est un événement ou un acte délibéré ou accidentel susceptible d'entraîner la compromission d'un système de TI du gouvernement du Canada. [Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC), 4 août 2015]
Cyberespace	Le réseau interdépendant de structures de technologie de l'information, incluant Internet, les réseaux de télécommunications, les systèmes informatiques ainsi que les processeurs et les contrôleurs intégrés, notamment le logiciel et les renseignements qu'ils contiennent. [Source : Note de doctrine conjointe – Cyberopérations v6]
Cyberopérations défensives	Cyberopérations défensives. Une opération défensive menée dans le cyberespace ou au moyen du cyberespace pour détecter, vaincre ou atténuer les actions offensives et exploitantes pour maintenir la liberté d'action. [Source : Cyberopérations, Note de doctrine interarmées v6; dossier DTB693742]
Détruire	Détruire est un verbe utilisé dans le cadre des tâches de mission qui consiste à endommager un objet ou une force ennemie de façon qu'il soit inutilisable à moins d'être remis en état ou reconstitué. Dans un contexte cybernétique, il peut s'agir d'actions offensives contre la confidentialité, l'intégrité ou la disponibilité des données ou de l'information qui sont essentielles aux opérations ennemies et qui rendent les opérations ennemies inutiles jusqu'à ce qu'elles soient reconstituées. (Par exemple, supprimer tous les fichiers d'un

	serveur, réécriture des données d'entrée-sortie de base, d'un système ou d'un micrologiciel, ou causer des dommages physiques aux systèmes de contrôle industriel, etc.).
Détection	Découverte par un moyen quelconque de la présence d'une personne, d'un objet ou d'un phénomène susceptible d'avoir un intérêt militaire. Dans un contexte cybernétique, la détection est axée sur les entités cybernétiques et la découverte, la saisie, l'enregistrement, le suivi et la maintenance de leurs attributs clés.
Chaîne de possession numérique	Préservation de l'intégrité de la preuve numérique ainsi que d'une procédure d'exécution de la documentation chronologique vers la preuve.
Analyse criminalistique	L'analyse criminalistique est un terme d'analyse approfondie, d'enquête dont le but est d'identifier et de documenter objectivement les coupables, les raisons, le cours et les conséquences d'un incident de sécurité ou d'une violation des lois de l'État ou règles de l'organisation.
Ordinateur hôte	Dans un réseau informatique, un ordinateur qui fournit aux utilisateurs finaux des services comme le calcul et l'accès à la base de données et qui peut exécuter des fonctions de contrôle de réseau. [Source : Banque de terminologie de la Défense, fiche n^{o} 13461]
Identification	L'identification est un processus consistant à atteindre une caractérisation précise d'une entité détectée par une action ou un moyen quelconque de manière à pouvoir prendre des décisions en temps réel, y compris l'engagement ESA des armes, avec un niveau de confiance élevé. Dans un contexte cybernétique, cela signifie qu'il faut effectuer l'analyse d'une entité cybernétique de façon suffisamment détaillée et avec une chaîne juridique de preuves pour permettre aux commandants de cyberforces de prendre des décisions opérationnelles et des plans pour prendre des mesures appropriées au besoin. Dans certains cas, cette tâche peut comprendre une analyse criminalistique détaillée des artéfacts matériels et logiciels guidée par une compréhension approfondie des renseignements sur les menaces.

Gestion de l'information	Discipline qui consiste à orienter et à appuyer la gestion efficace et efficiente de l'information au sein d'une organisation, et ce, du stade de la planification et de l'élaboration des systèmes jusqu'à celui de leur élimination ou de leur conservation à long terme. [Source : Secrétariat du Conseil du Trésor du Canada, Cadre stratégique pour l'information et la technologie, 1er juillet 2007]
Système d'information	Un ensemble d'équipements, de méthodes et de procédures et, au besoin, de personnel organisé de manière à remplir des fonctions de traitement de l'information. Remarque : Un système d'information peut également assurer le transfert d'informations en plus des fonctions de traitement, par exemple au sein d'un réseau local reliant plusieurs ordinateurs faisant partie du système d'information. [Source : Banque de terminologie de la Défense, fiche no 20171]
Technologie de l'information	Matériel ou système utilisé pour l'acquisition, le stockage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, la commutation, les échanges, la transmission ou la réception automatiques de données ou de renseignements. Elle englobe la conception, le développement, l'installation et la mise en œuvre de systèmes et d'applications informatiques visant à satisfaire à des exigences opérationnelles. [Source : Secrétariat du Conseil du Trésor du Canada, Cadre stratégique pour l'information et la technologie, 1er juillet 2007]
Infrastructure de technologie de l'information	L'ensemble des ordinateurs, des communications, des logiciels d'exploitation, des programmes utilitaires et des outils de gestion qui soutiennent l'automatisation de la gestion de l'information à l'échelle d'une organisation. L'ITI ne comprend pas les applications et leurs bases de données connexes. [Source : Banque de terminologie de la Défense, fiche no 1837]
Bibliothèque de l'infrastructure des technologies de l'information	Ensemble de pratiques détaillées en matière de gestion des services de TI [GSTI] visant à aligner les services de TI sur les besoins opérationnels.

Service de technologie de l'information	Points distincts d'interaction entre la technologie de l'information et les personnes, tant à l'intérieur qu'à l'extérieur d'une organisation. [Source : Nouvelle définition pour le projet de CD-DAR]
Lieu de services de technologie de l'information	Poste de travail, bureau, immeuble ou espace similaire dans une zone de prestation de services où les personnes établissent leurs points distincts d'interaction avec la technologie de l'information. [Source : Nouvelle définition pour le projet de CD-DAR]
Renseignement	Produit de la recherche, du traitement, de l'analyse, de l'intégration et de l'interprétation des informations disponibles sur les États étrangers, les forces ou éléments hostiles ou susceptibles de l'être, la géographie et les facteurs sociaux et culturels qui contribuent à la compréhension de l'environnement opérationnel réel ou potentiel. Remarque : Le terme « renseignement » décrit également les activités qui mènent au produit, ainsi que les organisations qui les exécutent. [Source : Banque de terminologie de la Défense, fiche n^{o} 738]
Mesures de défense internes	Les mesures de défense internes sont des mesures prises et des activités menées dans son propre cyberespace pour assurer la liberté d'action.
Apprentissage machine	Processus par lequel une unité fonctionnelle améliore son rendement en acquérant de nouvelles connaissances ou compétences, ou en réorganisant les connaissances ou les compétences existantes. [Source : Banque de terminologie de la Défense, fiche n^{o} 21880]
Neutraliser	Neutraliser est un verbe utilisé dans le cadre des tâches de mission qui consiste à rendre temporairement un élément ennemi incapable d'entraver une opération en particulier. La tâche doit indiquer clairement ce qu'il faut neutraliser. Il est ambigu d'énoncer simplement « neutraliser les préparatifs de l'ennemi » ou « neutraliser les forces de sécurité de l'ennemi ». Dans un contexte cybernétique, il peut s'agir d'actions

	offensives contre la confidentialité, l'intégrité ou la disponibilité des données ou de l'information qui empêchent les unités des forces ennemies d'utiliser leurs cybercapacités offensives ou défensives (par exemple, interrompre les flux de capteurs d'un domaine cible à l'unité de cyberdéfense responsable).
Cyberopération offensive	Cyberopération offensive. Opération offensive ayant pour but de projeter une puissance dans le cyberespace ou au moyen de celui-ci pour produire des effets à l'appui d'objectifs militaires. [Source : Cyberopérations, Note de doctrine interarmées v6; dossier DTB 693752]
Autorités opérationnelles	Commandants et leurs états-majors (comme le MDN, le CEMD, le cmdt du COIC, le DOS de l'EMIS ainsi que les autres commandants stratégiques et opérationnels et leurs états-majors) qui comptent activement sur les services de TI pour réussir leurs missions, opérations et tâches, qu'il s'agisse de services ou de fonctions administratives d'ordre national, international, expéditionnaire ou ministériel. Il s'agit des consommateurs finaux des produits de connaissance de la situation de la solution de la solution CD-DAR. [Source : Nouvelle définition]
Autorité opérationnelle	Personne qui a l'autorité de définir des besoins et des principes directeurs, de fixer des normes et d'accepter des risques dans son domaine de responsabilité. [Source : Banque de terminologie de la Défense, fiche n^{o} 43435]
Résultat	Un résultat est « tout ce qui arrive à la suite et comme effet de quelque chose ». [Source : Guide et outils de gestion par analyse de résultat]
Surveiller passivement	L'écoute passive (surveillance) est la surveillance ou l'enregistrement de données qui vise uniquement à observer un flux de communication et à prendre connaissance des données qu'il contient, mais pas à modifier ou à affecter ce flux de toute autre manière. [Source : Glossaire du NIST : CNSSI 4009-2015 IETF RFC 4949 V2 – Adapté]

Reconnaissance	La reconnaissance signifie la détermination, par quelque moyen que ce soit, du caractère amical ou ennemi ou de l'individualité d'un autre, ou d'objets tels que des aéronefs, des navires, des chars d'assaut ou de phénomènes tels que les modèles de communications électroniques. Dans un contexte cybernétique, cela signifie analyser les attributs clés des entités cybernétiques et de leurs activités (sur la conviction que les données sur de nombreux attributs peuvent être fausses, périmées, incomplètes ou trompeuses, etc.) dans le contexte holistique du domaine des opérations mondiales et interarmées ou de l'information, pour déterminer si les activités observées sont le résultat de menaces naturelles ou délibérées et estimer les répercussions de ces menaces.
Mesures d'intervention	En cyberopérations défensives, mesures prises et activités menées dans le cyberespace ou au moyen de celui-ci, à l'extérieur de son propre cyberespace, pour contrer des menaces actuelles ou imminentes en vue de conserver la liberté d'action. [Source: Compte rendu des décisions – Réunion du Comité mixte de terminologie tenue au Centre de guerre des Forces canadiennes du 26 au 29 avril 2016]
Catégorisation de la sécurité	Processus qui consiste à déterminer la catégorie de sécurité des activités opérationnelles, des systèmes d'information et des biens de TI. [Source : Terminum]
Renseignement d'origine électromagnétique (SIGINT)	Le renseignement obtenu de communications électromagnétiques, de systèmes de communication ainsi que de transmissions électromagnétiques non liées aux communications, par des personnes autres que les destinataires prévus. [Source : Compte rendu des décisions – Réunion du Comité mixte de terminologie tenue au Centre de guerre des Forces canadiennes du 26 au 29 avril 2016]
Connaissance de la situation	La connaissance des éléments de l'environnement opérationnel nécessaire pour prendre des décisions informées.

	[Source : Banque de terminologie de la Défense, fiche nº 41441]
Cyberopérations de soutien	Opération de réseau assignée par un commandant, ou sous son contrôle direct, en soutien de cyberopérations offensives ou défensives. [Source : Compte rendu des décisions – Réunion du Comité mixte de terminologie tenue au Centre de guerre des Forces canadiennes du 26 au 29 avril 2016]
Supprimer	La suppression consiste à dégrader temporairement une capacité de l'ennemi pour permettre une action des forces amies. L'effet est temporaire et il ne dure qu'aussi longtemps que la force amie fait feu. Dans un contexte cybernétique, il peut s'agir d'une série de cyberactions offensives qui dégradent ou neutralisent la capacité d'une force belligérante d'utiliser le cyberespace. (Exemple : Les attaques entraînant un déni de service).
Tâche	Un ensemble d'actions réalisées pour atteindre un objectif précis dont l'accomplissement est l'une des fonctions d'un employé occupant un poste particulier.
Relation de confiance	Politiques qui régissent la manière dont les entités de différents domaines respectent les autorisations des autres. [Source : NIST SP800-95]
Dispositif virtuel	Un dispositif qui imite un dispositif matériel/appareil mais qui n'existe que sous forme de logiciel.

10 ACRONYMES ET ABRÉVIATIONS

Acronyme / Abréviation	Description
SSCIAT	Spécialiste des systèmes de communication et d'information de l'Armée de terre
SMA(Fin)	Sous-ministre adjoint (Finances)
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
IA	Intelligence artificielle
SSC	Système de suivi consultatif
ZResp	Zone de responsabilité
IPA	Interface de programmation d'applications
MPA	Menaces persistantes avancées
AP	Antipourriel
ATIS	Technicien de systèmes d'information et de télécommunications aérospatiales
AUS	Australie
AV	Logiciel antivirus
AR	Analyse de rentabilisation
CEM Cyber	Chef d'état-major du cyberespace
C2	Commandement et contrôle
C4ISR	Commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance
AC	Armée canadienne
FAC	Forces armées canadiennes
COMFOSCAN	Commandement – Forces d'opérations spéciales du Canada

CCE	Communications Configuration Enumeration
CCSS	Système Communications Configuration Score System
CD-DAR	Cyberdéfense – Décision, analyse et réponse
DCD	Dépôt de cyberdonnées
CEMD	Chef d'état-major de la Défense
CDF	Chef – Développement des forces
GOIFC	Groupe des opérations d'information des Forces canadiennes
CORFC	Centre d'opérations des réseaux des Forces canadiennes
EECFC	École de l'électronique et des communications des Forces canadiennes
CIICS	Cyber Information and Incident Coordination System
CIS	Centre for Internet Security
EECI	Environnement d'essai cyberintégré
COIC	Commandement des opérations interarmées du Canada
CGC	Cadre de gestion des capacités
PA	Plan d'action
TBCO	Tableau de bord cyberopérationnel
R comd	Réseau de commandement
CONOPS	Concept des opérations
CONSUP	Concept de soutien
ICSO	Image commune de la situation opérationnelle
CARO	Centre d'analyse et de recherche opérationnelle

COTS	Commercial sur étagère
CPE	Common Platform Enumeration
CPU	Unité centrale de traitement
SSC	Sensibilisation à la cybersécurité
CSC	Contrôles de sécurité critique
CST	Centre de la sécurité des télécommunications
IRSC	Infrastructure du réseau secret consolidé
FSI	Fournisseur de services infonuagiques
ARCS	Architecture de référence de la cybersécurité
CVE	Common Vulnerabilities and Exposures
DAR	Décision, analyse et réponse
DOAD	Directives et ordonnances administratives de la Défense
CCD	Comité des capacités de la Défense
COD	Cyberopération défensive
AD-COD	Aide à la décision pour les cyberopérations défensives
COSD	Centre des opérations des services de la Défense
IDE	Interdiction défensive externe
DASE	Directeur – Achat de systèmes électroniques
DG Cyber	Directeur général – Cyberespace
CGDG	Comité de gouvernance des directeurs généraux
DGOGI	Directeur général – Opérations (Gestion de l'information)
DIIGI	Directeur – Ingénierie et intégration (Gestion de l'information)

Dir Sécur GI	Directeur – Sécurité (Gestion de l'information)
MDN	Ministère de la Défense nationale
DoD	Department of Defence (États-Unis)
DEM EMIS	Directeur d'état-major – État-major interarmées stratégique
EFRD	Évaluation des facteurs de risque dynamiques
RDDC	Recherche et développement pour la défense Canada
GRD	Gestion du risque dynamique
RED	Réseau étendu de la Défense
DIPE	Détection et intervention aux points d'extrémité
ATE	Avantage du terrain externe
EF	Emploi de la force
COF	Capacité opérationnelle finale
Gp5	Groupe des cinq
ACS+	Analyse comparative entre les sexes plus
GC	Gouvernement du Canada
PGEC GC	Plan de gestion des événements de cybersécurité du gouvernement du Canada
GOTS	Gouvernemental sur étagère
IUG	Interface utilisateur graphique
DE	Disponibilité élevée
EOHN	Exigences obligatoires de haut niveau
QG	Quartier général

Mat	Matériel
MDI	Mesures défensives internes
SDI	Système de détection d'intrusion
PEI	Passerelle d'échange d'information
COI	Capacité opérationnelle initiale
IC	Indicateurs de compromission
IP	Protocole Internet
PMPI-AI	Proposition de modification du plan d'investissement – Analyse de l'incidence
RPI	Réunion de planification initiale
SPI	Système de prévention des intrusions
SES	Soutien en service
TI	Technologie de l'information
ATI	Avantage du terrain interne
ITI	Infrastructure de technologie de l'information
ITI à l'appui du C2	Infrastructure de technologie de l'information à l'appui du commandement et contrôle
IQ	Invitation à se qualifier
STI	Système de technologie de l'information
GSTI	Gestion des services de technologie de l'information
CGEBI	Capacité de gestion de l'espace de bataille interarmées
FOI	Force opérationnelle interarmées
KML	Langage de balisage de Google (Keyhole Markup Language)

GCVM	Gestionnaire du cycle de vie du matériel
MISP	Malware Information Sharing Platform
AM	Apprentissage machine
Min DN	Ministre de la Défense nationale
GPM	Groupe professionnel militaire
MTBF	Moyenne des temps de bon fonctionnement
MTC	Moyenne des temps de confinement
MTD	Moyenne des temps de détection
MTI	Moyenne des temps d'identification
MTRR	Moyenne des temps de réponse/résolution
NAT	Traduction d’adresses de réseau
OTAN	Organisation du Traité de l’Atlantique Nord
COMM NAV	Spécialiste en communications navales
OP EICM	Opérateur d'équipement d'informations de combat (Marine)
C2 réseau CICS	Commandement et contrôle de réseau – Capacité intégrée de connaissance de la situation
NetOps	Opérations de réseaux
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
NVG	NATO Vector Graphics
NZ	Nouvelle-Zélande
AO	Autorité opérationnelle

Phase d'AO	Phase d'analyse des options
AM	Autre ministère
MODC	Mentorat opérationnel et développement des capacités
OSINT	Renseignement de sources ouvertes
AP(Déf)	Approbation du projet (définition)
PACS	Systèmes de contrôle des accès physiques
DAP	Directive d'approbation de projet
PAT	Conversion d'adresses de ports (Port Address Translation)
EP(ID)	Énoncé de projet (identification)
PCAP	Capture de paquets
DP	Directeur de projet
EBPP	Évaluation des besoins en perfectionnement professionnel
GP	Gestionnaire de projet
CGP	Conseil de gestion du programme
OREN	Objectif de rendement
SPAC	Services publics et Approvisionnement Canada
ISP	Intégrateur de système principal
Qté	Quantité
R et D	Recherche et développement
MI	Mesures d'intervention
CAFR	Contrôle d'accès en fonction des rôles
ARC	Aviation royale canadienne

MRC	Marine royale canadienne
DI	Demande d'information
DP	Demande de propositions
RI	Rendement des investissements
CS	Connaissance de la situation
ESA	Évaluation de la sécurité et autorisation
GEAS	Guide d'évaluation et d'autorisation de la sécurité
SANS	SysAdmin, Audit, Network and Security Institute
SCAP	Security Content Automation Protocol
GIES	Gestion de l'information et des événements de sécurité
SIGINT	Renseignement d'origine électromagnétique
EMIS	État-major interarmées stratégique
IPO	Instructions permanentes d'opération
EBO	Énoncé des besoins opérationnels
CSR	Comité supérieur de révision
FS(ID)	Feuille de synthèse (Identification)
SPC	Services partagés Canada
PSE	Protection, Sécurité, Engagement
SSL	Protocole SSL
Logiciels	Logiciels
SWID	Identification du logiciel
RT	Responsable technique

DAT	Document d’architecture technique
CT	Conseil du Trésor
À dét.	À déterminer
TTP	Tactiques, techniques et procédures
PUD	Portrait unifié des données
UEBA	Analytique des comportements des utilisateurs et des entités
R.-U.	Royaume-Uni
É.-U.	États-Unis
XCCDF	Extensible Configuration Checklist Description Format
PIZ	Point d'interface de zone

Ébauche

Ébauche

11 ATTRIBUTS CLÉS DES CYBERENTITÉS

11.1 Attributs clés des cyberentités

Nº	Description
1	Nom de l'utilisateur principal et les réseaux ou domaines auxquels il est branché.
2	Nom d'utilisateurs alternatifs (un ou plus) et les réseaux ou domaines auxquels ils sont branchés.
3	Remplir les sections pour le nom, le rang et les renseignements relatifs à l'identification selon le dossier personnel ou d'une manière qui peut être corrélée plus tard.
4	Service, CIDP ou numéro d'attestation de sécurité industrielle
5	Division, formation, unité, sous-unité, etc.
6	Lieu principal ou lieu de travail
7	Autres lieux de travail temporaires
8	Domaine principal ou point de rapport
9	Autres domaines temporaires ou points de rapport
10	Adresses courriel pour chaque domaine ou réseau
11	Autorisations ou droits propriétaires pour les utilisateurs, les fichiers, les dossiers, les réseaux, les appareils
12	Active Directory (AD), protocole allégé d'accès annuaire (LDAP), X.500 Statut d'enregistrement
13	Rapports de vulnérabilités actuelles comme les fichiers, dossiers de documents et courriels associés à la personne, menaces connues, historique des rapports associés aux événements ou incidents, historique des points de terminaisons utilisés.
14	Date de la dernière vérification ou inspection ou du dernier examen
15	Accès ou emplacement des rapports de données de l'utilisateur

Ébauche

11.2 Attributs clés des cyberentités non humaines

Nº	Description
1	Type d'hôte - physique ou virtuel
2	Nom de l'hôte (conformément à la convention de dénomination utilisée)
3	Numéro de fabricant / numéro de série / numéro d'inventaire du matériel (avec la marque d'inventaire en corrélation avec le titulaire du compte)
4	Processeur (fabricant, numéro de série, modèle, etc.)
5	Mémoire (fabricant, numéro de série, modèle, etc.)
6	Inventaire et identification de toutes les unités remplaçables en ligne (URL) à bord de l'appareil (CDROM / DVDRW / ports USB, matériel / clavier / souris / moniteurs / adaptateurs de réseau, processeurs, cartes mères, alimentations, conteneurs / cadres, etc.)
7	Type ou objectif principal de l'appareil (poste de travail, routeur de bureau virtuel, commutateur, pare-feu, passerelle, filtre Web, système de détection d'intrusion, système de prévention des intrusions, contrôleur de domaine, points d'accès sans fil, serveurs d'applications, serveur Mai, bases de données, applications intranet, etc.)
8	Modèle de périphérique, sous-modèle, version
9	Adresse MAC (ou adresses si plus d'une interface) pour tous les types d'interfaces externes
10	Adresse IP et sous-réseau (fixe ou attribuée par le DHCP)
11	Nom de l'hôte de l'URL
12	Méthode d'attribution de l'adresse IP : DHCP, réservée par le DHCP ou attribuée par l'hôte fixe
13	Heure de l'hôte
14	Serveur temporel du réseau hôte (si configuré à distance)
15	Hôte de passerelle
16	DNS principal, alternatif, deuxième alternatif hôte
17	Serveur DHCP hôte
18	Serveur WINS hôte
19	Serveur mandataire Web hôte (le cas échéant)
20	Tables de routage hôtes

Ébauche

Nº	Description
21	Tableaux de transfert des ports hôtes
22	Tables de traduction d'adresses réseau hôtes (TAR)
23	Domaine hôte
24	Contrôleur de domaine principal attribué
25	Contrôleur de domaine secondaire attribué
26	Active Directory (AD), protocole allégé d'accès annuaire (LDAP), X.500 Statut d'enregistrement
27	IPv4 -ou-IPv6
28	Droits d'autorisation d'hôte (propriétaire, administrateurs, utilisateurs, invités, etc.) et comment ils sont assignés ou contrôlés (répertoire local ou actif)
29	Données SNMP utilisées et numéro de version
30	État du protocole ICMP
31	Logiciel antivirus basé sur hôte et version
32	Logiciel de prévention des intrusions basé sur hôte et version
33	Logiciel de détection des intrusions basé sur hôte et version
34	État du service de pare-feu basé sur l'hôte
35	Autorité de certification de l'hôte
36	Ports hôtes (ouvert, fermé, écoute, mode furtif)
37	Système d'exploitation et version
38	Version d'image de base (le cas échéant)
39	Inventaire des logiciels installés - haut niveau
40	Inventaire des logiciels installés - niveau détaillé - toutes les DLL et les exécutables de soutien, les fichiers de configuration et les modules logiciels ou les composants connexes.
41	Code de hachage de la configuration de base (pour faciliter la détection de modifications à la configuration de base)
42	Services en cours d'exécution sur le périphérique et les ports utilisés
43	Certificats de services hôte
44	Nom d'utilisateurs enregistrés et actuellement authentifiés

Ébauche

Nº	Description
45	Lieu - Nom de lieu physique (comme dans la BFC Petawawa, bâtiment P114, salle 101, bureau 5) et son équivalent géodésique (latitude, longitude, altitude), ou tout simplement, s'il s'agit d'un appareil mobile, sa latitude, sa longitude et son altitude.
46	Propriétaire - titulaire du compte matériel
47	Source d'alimentation (principale, batterie interne, batterie externe)
48	Source du système d'alimentation de secours
49	Propriétés physiques - température, humidité
50	Rapports de vulnérabilité existants, menaces connues, historique des rapports associés aux événements ou aux incidents
51	Réseau nommé, enclave, sous-réseau, etc. auxquels l'appareil est directement branché
52	Date de la dernière vérification ou inspection ou du dernier examen
53	Accès ou emplacement des registres internes de l'appareil (le cas échéant) (GIES, SNMP, SCOM, etc)

Ébauche

Sous-ministre adjoint (Gestion de l'information)

Concept d'opération (CONOPS)

Cyberdéfense – Décision, analyse et réponse (CD-DAR)

Ébauche

N^{O} PSD :	C.000707
TITRE :	Cyberdéfense – Décision, analyse et réponse (CD-DAR)
ÉTAPE DU PROJET :	Définition
PARRAIN DU PROJET :	Sous-ministre adjoint (Gestion de l'information) (SMA[GI])
DATE D'ENTRÉE EN VIGUEUR :	Le 02 février 2021
VERSION :	1.0

Page laissée vierge intentionnellement.

Ébauche

PAGE DE SIGNATURE

Titre du projet : Cyberdéfense – Décision, analyse et réponse (CD-DAR)

Appuyé par :

DRPCC	Signature	Titre	Nº de téléphone	Date
		Gestionnaire de projet (GP), CD-DAR		

DDFOC	Signature	Titre	Nº de téléphone	Date
N.M. Mallory		Directeur de projet (DP), CD-DAR		

DGDFCI	Signature	Titre	Nº de téléphone	Date
		DGDFCI		

Approuvé par :

CEM Cyber	Signature	Titre	Nº de téléphone	Date
		CEM Cyber	À déterminer	

Ébauche

Page laissée vierge intentionnellement.

Ébauche

REGISTRE DES MODIFICATIONS

Les ébauches de documents distribués doivent être conformes à la convention de version définie dans le « Plan de gestion des registres et des documents du projet » jusqu'à ce que le document soit officiellement approuvé par le biais du processus de gestion des registres et des documents de la Cyberdéfense – Décision, analyse et réponse (CD-DAR).

La première version officielle du présent document sera la version 1.0.

Chaque nouvelle version (V1.0, V2.0, etc.) du présent document sera désignée dans le tableau ci-dessous par le numéro de version assigné au document révisé. Le tableau comprendra également le numéro de demande de modification (DM) attribué à chaque modification approuvée intégrée au document révisé.

Tous les éléments du présent document publié, notamment les pages préliminaires, le corps du texte (le texte, les tableaux ainsi que les figures et les illustrations) et les parties complémentaires, doivent être soumis aux processus de gestion intégrée des modifications et de gestion des registres et des documents officiels.

Nota : Si un document contient un extrait d'un autre document, cet extrait ne sera révisé qu'au moment de la révision du document d'origine.

Version	Date	Modifié par	DM	Commentaires
V1.0	xx-02-2021	Maj N. Mallory		Version originale

Ébauche

Page laissée vierge intentionnellement.

Ébauche

SOMMAIRE

Les cybermenaces les plus évoluées proviennent des services du renseignement et des services militaires d'États étrangers. Les gouvernements, les forces militaires et les entreprises privées à la fine pointe de la technologie sont vulnérables au cyberespionnage parrainé par des États ainsi qu'à des cyberopérations perturbatrices. On peut s'attendre à ce que cette menace augmente au cours des prochaines années. Les cybermenaces sont de plus en plus complexes à combattre, car il est de plus en plus difficile de déterminer avec certitude la source des cyberattaques ainsi que les défis liés au champ de compétence causés par l'éloignement possible des cyberattaques.

À l'heure actuelle, les organisations déploient de nombreuses stratégies et technologies qui mettent l'accent sur une défense du réseau périmétrique ou des appareils des utilisateurs (ordinateurs portatifs, imprimantes, tablettes, etc.) fondée sur les méthodes d'attaque répertoriées (virus, maliciels, etc.). Ces solutions s'avèrent trop souvent inefficaces puisqu'elles sont susceptibles de produire une grande quantité d'alertes pour la plupart fausses. Celles-ci sont impossibles à traiter automatiquement par un système, il faut donc analyser ces alertes à la main, ce qui nécessite beaucoup de temps et un important bassin d'experts. Parce que ces alertes sont très nombreuses, le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) ne disposent pas du temps nécessaire et des ressources pour intervenir chaque fois qu'une alerte est déclenchée et doivent se résigner à ne pas toutes les traiter. Malgré les efforts déployés par le gouvernement, les attaquants font continuellement évoluer leurs méthodes pour contourner les cyberdéfenses et exploiter les changements technologiques, ce qui constitue une menace constante à la sécurité nationale et au bien-être du Canada et des Canadiens.

Le projet de CD-DAR, qui porte le numéro C.000707, servira à acquérir une solution de cyberdéfense (qui se traduit en capacités) dans le but d'améliorer l'aide à la décision en général et à la sécurité du cyberespace du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'y réagir. La solution intégrée fournira une analyse contextuelle fiable pour appuyer les décisions et les actions du MDN et des FAC à l'intérieur d'extensions et d'interfaces désignées du réseau de commandement[1] (R comd) ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables à l'appui de la conduite d'opérations cybernétiques défensives (OCD).

En fin de compte, la cyberforce du MDN et des FAC sera équipée, entraînée et préparée à mener efficacement des OCD en s'appuyant sur une solide capacité fondamentale de cybersécurité et de cyberdéfense ainsi que sur un cadre de capacité de surveillance en service (SES) permettant de maintenir et d'optimiser les processus opérationnels des OCD, les outils matériels et logiciels de CD-DAR et l'instruction récurrente du personnel afin de garantir que la capacité de CD-DAR reste disponible, fiable et pertinente sur le plan opérationnel et qu'elle permette le développement de la croissance future tout au long de sa vie en service.

[1] Le réseau de commandement est un réseau de communication qui relie un échelon de commandement avec certains ou tous ses échelons subordonnés à des fins de commandement et de contrôle.

Page laissée vierge intentionnellement.

Ébauche

TABLE DES MATIÈRES

Ébauche

Ébauche

TABLE DE FIGURES

Ébauche

LISTE DE TABLES

Ébauche

1 INTRODUCTION

1.1 Objectif

Le présent concept d'opération (CONOPS) définit les rôles et les responsabilités de la cyberforce ainsi que les processus et les outils qui formeront la capacité de Cyberdéfense – Décision, analyse et réponse (CD-DAR) du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC). Il fournit une description de la nouvelle capacité et des conditions dans lesquelles elle fonctionnera, des processus qui seront utilisés pour sécuriser et défendre le cyberenvironnement du MDN et des FAC, comme on le précise dans la portée du projet ci-dessous et de la manière dont les commandants, les cadres, le personnel et les cyberopérateurs interagiront dans le cadre de la CD-DAR.

1.2 Besoin en matière de capacités

Le MDN et les FAC ont besoin d'une capacité de cyberdéfense applicable aux domaines stratégiques, opérationnels et propres à la mission. La capacité doit fournir une découverte du réseau, des outils de cyberdéfense logicielle intégrés, un dépôt de base de données de confiance et une image commune de la situation opérationnelle (ICSO); la capacité doit tenir compte des facteurs humains et permettre la criminalistique cybernétique à distance. Le MDN et les FAC ont besoin d'une surveillance intégrée de leur architecture de réseau et des informations pertinentes qu'elle contient ainsi que d'une connaissance complète de la situation, de la détection, de l'analyse et de la formulation d'une réponse aux cybermenaces en temps opportun dans les domaines stratégiques, opérationnels et tactiques.

1.3 Portée

Le présent CONOPS est axé sur l'emploi d'une force (EF)[2] de capacités de cyberdéfense de la CD-DAR pour surveiller et défendre les réseaux du MDN et des FAC, y compris la capacité de détecter les menaces, de les analyser et d'y réagir. La capacité de CD-DAR fournira également une analyse contextuelle fiable pour appuyer les décisions et les actions du MDN et des FAC dans la conduite des opérations cybernétiques défensives (OCD) à l'intérieur d'extensions et d'interfaces désignées du réseau de commandement[3] (R comd) ainsi que des systèmes du Réseau étendu de la Défense (RED) déployables (réseau désigné – Protégé B et moins). L'Infrastructure du réseau secret consolidé (IRSC) (réseau classifié – Secret) fait partie du réseau de commandement au sein du MDN et des FAC et une partie importante de la portée de la CD-DAR sera appliquée à l'IRSC. La structure du réseau de commandement est en constante évolution, car de plus en plus de services, de systèmes et d'infrastructures de réseau sont regroupés au sein de l'IRSC afin de répondre plus efficacement aux exigences et aux opérations des FAC. Les capacités de CD-DAR sur les systèmes du RED déployés comprendront toute l'infrastructure, du

[2] Au niveau opérationnel, l'emploi d'une force renvoie au commandement, au contrôle et au maintien en puissance des forces allouées, Banque de terminologie de la défense (BTD), Fiche nº 32173.

[3] Le réseau de commandement est un réseau de communication qui relie un échelon de commandement avec certains ou tous ses échelons subordonnés à des fins de commandement et de contrôle.

point final jusqu'à l'interface d'entrée de l'infrastructure du RED contrôlée par Services partagés Canada (SPC) à la passerelle d'accès au réseau (après déchiffrement) située au Canada.

Tous les réseaux et toutes les infrastructures en dehors du réseau de commandement du MDN et des FAC sont hors de portée de la CD-DAR; toutefois, il est entendu que ces systèmes peuvent apporter une contribution aux réseaux inclusifs. Ces entrées seront surveillées par la CD-DAR au point d'entrée pour détecter toute anomalie susceptible de déclencher un incident.

À terme, la capacité de CD-DAR permettra à la cyberforce des FAC de défendre la liberté d'action et les intérêts des FAC dans le cyberespace ainsi que de produire des effets militaires dans l'ensemble d'un cyberenvironnement contesté à l'appui des missions et des opérations des FAC.

1.4 Missions

Protection, Sécurité, Engagement : La politique de défense du Canada (PSE) accorde une grande attention aux opérations et à la défense dans le cyberespace en adoptant une position plus affirmée dans le cyberdomaine et en renforçant les cybercapacités du MDN et des FAC. La CD-DAR s'harmonise à PSE et au programme de cyberassurance de la mission (CAM) du MDN et des FAC en fournissant des cybercapacités pour appuyer les opérations militaires, en protégeant les réseaux et les équipements militaires essentiels contre les cyberincidents et en permettant aux cybercapacités de mieux appuyer les « missions principales des FAC :

a. Détecter et dissuader les menaces ou les attaques visant le Canada et s'en défendre;
b. Détecter et dissuader les menaces et les attaques visant l'Amérique du Nord et s'en défendre en partenariat avec les États-Unis, notamment par l'entremise du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD);
c. Diriger des efforts de l'Organisation du Traité de l'Atlantique Nord (OTAN) ou de coalitions visant à dissuader et à vaincre des adversaires, y compris des terroristes, à l'appui de la stabilité mondiale ou contribuer des forces à ces efforts;
d. Diriger des opérations de paix internationales et des missions de stabilisation avec les Nations Unies, l'OTAN, et d'autres partenaires multilatéraux ou y participer;
e. Participer au renforcement des capacités à l'appui de la sécurité d'autres pays et de leur capacité d'apporter une contribution à la sécurité à l'étranger;
f. Prêter assistance aux autorités civiles et aux organismes d'application de la loi, notamment ceux chargés de la lutte contre le terrorisme à l'appui de la sécurité nationale et de la sécurité des Canadiens à l'étranger;
g. Prêter assistance aux autorités civiles et aux partenaires non gouvernementaux à la suite de catastrophes ou d'urgences majeures survenant au pays ou à l'étranger;
h. Mener des opérations de recherche et de sauvetage[4] ».

[4] *Protection, Sécurité, Engagement : La politique de défense du Canada* (PSE), ministre de la Défense nationale, 2017.

1.5 Hypothèses

Les hypothèses relatives à la capacité de CD-DAR sont les suivantes :

a. Le financement de toute mise à jour nécessaire de l'infrastructure opérationnelle sera attribué;

b. La bande passante actuelle au sein de l'infrastructure de la technologie de l'information (ITI) permettra de tenir compte des exigences en matière de mises à jour des données sur la connaissance de la situation (CS) que requiert la solution de CD-DAR, particulièrement dans les emplacements déployés;

c. Les politiques, les organisations et les pratiques du gouvernement ainsi que du MDN et des FAC continueront d'améliorer leur réponse aux cybermenaces;

d. Les ministères de soutien, y compris le Centre de la sécurité des télécommunications Canada (CSTC), SPC et le Service canadien du renseignement de sécurité (SCRS) continueront à contribuer à la cybersécurité nationale;

e. Les processus actuels du Directeur général – Opérations (Gestion de l'information) [DGOGI] seront adaptés aux technologies utilisées sur le terrain et répondront aux facteurs externes de changement social et aux changements de nature du cyberconflit.

1.6 Contraintes

Les contraintes liées à la capacité de CD-DAR sont notamment les suivantes :

a. Habilitation de sécurité – La nature du domaine de la cybersécurité exige que le personnel et l'industrie possèdent des habilitations de sécurité allant jusqu'au niveau TRÈS SECRET du renseignement d'origine électromagnétique (SIGINT) et satisfassent à des restrictions de citoyenneté de l'Australie/de la Nouvelle-Zélande/du Royaume-Uni/des États-Unis (AUS/NZ/RU/É.-U.) visant uniquement les citoyens CANADIENS;

b. Exigence de conception – Les systèmes de processus, les logiciels et le matériel doivent pouvoir être utilisés par le personnel opérationnel actuel du MDN et des FAC, y compris le personnel qui produit et utilise actuellement l'information sur la connaissance de la situation. Pour réussir, la capacité de CD-DAR n'exige généralement pas une instruction excessive qui modifie fondamentalement les compétences et les métiers ou professions offerts pour remplir ces rôles.

1.7 Intervenants internes

Les intervenants internes sont des organisations au sein du MDN et des FAC qui sont directement ou indirectement touchées par la capacité de CD-DAR. Les intervenants internes de la CD-DAR sont répertoriés dans le tableau 1 ci-dessous.

Ébauche

Tableau 1 – Intervenants internes de la CD-DAR

Organisation	Responsabilités
État-major interarmées stratégique (EMIS)	L'EMIS fournit une analyse militaire et une aide à la prise de décision au chef d'état-major de la défense (CEMD), le principal conseiller militaire du gouvernement du Canada (GC). La capacité de gestion interarmées de l'espace de bataille (CGIEB) étaye les informations opérationnelles et les processus décisionnels des FAC afin de déterminer la bonne combinaison de personnes, de processus et de technologie pour la fourniture d'une image commune de la situation opérationnelle des FAC (ICSO FAC) à l'usage des commandants en vue d'obtenir la connaissance de la situation (CS). La CD-DAR alimentera la CGIEB au moyen d'une CS cybernétique pertinente pour les opérations en cours.
Commandement des opérations interarmées du Canada (COIC)	Le COIC est responsable de l'intégration des capacités des FAC, y compris le commandement, le contrôle, les communications, l'informatique, le renseignement, la surveillance et la reconnaissance (C4ISR), ainsi que les capacités spatiales et cybernétiques dans des forces opérationnelles propres à la mission. Il exécute et maintient les opérations au Canada, en Amérique du Nord et à l'étranger en réponse aux directives formulées par le GC.
Directeur général – Opérations (Gestion de l'information) [DGOGI]	Le DGOGI fournit la base opérationnelle du Groupe de gestion de l'information (Gp GI). La division couvre tous les niveaux de commandement – tactique, opérationnel et stratégique – afin de coordonner, de soutenir et de fournir le commandement et contrôle (C2) ainsi que les capacités de renseignement dont les FAC et le Ministère ont besoin pour faire leur travail.
7e Groupe des communications (7 Gp Comm)	Le 7 Gp Comm relève directement du DGOGI. Le 7 Gp Comm fournit, coordonne et gère les technologies de l'information et les services de réseau du MDN et des FAC qui permettent le C2 et le partage de l'information à l'appui des objectifs opérationnels du MDN et du commandement des FAC. La mission du 7 Gp Comm consiste à maintenir en puissance les systèmes de communication et d'information (SCI) pour permettre aux FAC d'exercer le C2 et de mettre sur pied des capacités en matière de ligne à l'appui des opérations des FAC.
Centre des opérations des services de la Défense (COSD)	Le COSD relève du 7 Gp Comm. Le COSD assure le soutien en service des réseaux de technologie de l'information (TI) aux opérations et aux activités du MDN et des FAC, y compris le

Ébauche

Organisation	Responsabilités
	soutien des TI d'entreprise et le soutien des réseaux d'information aux environnements et aux commandants.
Groupe des opérations d'information des Forces canadiennes du QG (GOIFC QG)	Le GOIFC relève du DGOGI. Le GOIFC met sur pied et emploie des capacités en matière de renseignement d'origine électromagnétique (SIGINT), de guerre électronique et de cyberopérations pour appuyer les opérations des FAC et du MDN. Le GOIFC assure le développement des capacités de cyberdéfense, de renseignement et d'information à l'appui des forces du Canada, des États-Unis, de la Grande-Bretagne, de la Nouvelle-Zélande et de l'Australie et aux forces de coalition; il soutient également les réseaux classifiés de communications, ainsi que l'Équipe d'inspection technique de sécurité (EITS).
Centre d'opérations des réseaux des Forces canadiennes (CORFC)	Le CORFC relève du GOIFC. Le CORFC offre en tout temps la surveillance de la situation et la gestion des incidents à l'appui de l'exploitation des réseaux des FAC et du MDN et de la protection contre la cyberexploitation.
Élément de coordination de composante cybernétique du commandant de la composante cybernétique des forces interarmées (ECCC CCCFI)	L'ECCC CCCFI relève du CCCFI par l'entremise du GOIFC. L'ECCC CCCFI met à disposition des experts du cyberenvironnement et maintient la cyberconnaissance de la situation mondiale puisque celle-ci a une incidence sur le COIC et ses missions. L'élément est situé au même endroit que le COIC.
Directeur général – Service des applications d'entreprise (DGSAE)	Le DGSAE fournit des applications de TI et des services de gestion de l'information (GI) pour appuyer les opérations des FAC et les objectifs généraux du MDN.
Directeur général – Réalisation de projets (Gestion de l'information) [DGRPGI]	Le DGRPGI collabore avec les clients, les intervenants et les collègues du groupe GI pour planifier, concevoir, mettre au point et déployer stratégiquement des solutions technologiques, des capacités et des changements à la capacité de gestion de l'information/technologie de l'information (GI/TI) du MDN et des FAC.
Directeur général – Technologie et planification stratégique (Gestion de l'information) [DGTPSGI]	Le DGTPSGI établit l'orientation stratégique et tactique de la transformation du programme de GI/TI pour le MDN et les FAC. Le DGTPSGI soutient les opérations des FAC, les priorités ministérielles et les objectifs du gouvernement en assurant un accès transparent et en temps opportun à une information fiable, au renseignement et à la technologie dans un environnement sûr.

Ébauche

Organisation	Responsabilités
Directeur – Développement des capacités (Gestion de l'information) [DDCGI]	Le DDCGI relève du DGTPSGI. Le DDCGI est responsable de la gestion, de la surveillance et de la coordination des activités au sein du MDN et des FAC pour appuyer le programme de transformation de TI du GC. Il est également responsable de la gestion du portefeuille ministériel des licences d'entreprise. Le DDCGI est actuellement le DP de la gestion des services de technologie de l'information (GSTI). En outre, le DDCGI est le centre d'expertise par l'intermédiaire du Bureau national de gestion des services (BNGS).
Directeur – Ingénierie et intégration (Gestion de l'information) [DIIGI]	Le DIIGI relève du DGTPSGI. Le DIIGI dirige le MDN et les FAC dans l'ingénierie, les essais et l'intégration des capacités de l'infrastructure de GI/TI. Le DIIGI soutient l'officier principal de l'information de la Défense en tant qu'ingénieur en chef et architecte en chef, et participe également à la fonction C4ISR et à la cybersécurité. Le DIIGI détermine les possibilités, dans le cadre de l'architecture technologique actuelle, d'améliorer l'efficacité, de réduire la complexité et les coûts, et d'accroître l'interopérabilité avec les organisations partenaires, en particulier l'OTAN et les pays membres du Combined Communications-Electronics Board (CCEB).
Directeur – Sécurité (Gestion de l'information) [Dir Sécur GI]	Le Dir Sécur GI relève du DGTPSGI. Le Dir Sécur GI supervise la sécurité des TI et de l'information au sein du MDN et des FAC. Il soutient et conseille l'officier principal de l'information de la Défense, le chef de la sécurité et les diverses autorités opérationnelles sur l'efficacité des mesures d'atténuation des risques de sécurité des TI par le biais des programmes d'évaluation et d'autorisation de la sécurité, de surveillance et de conformité et de sécurité de l'information industrielle. Il remplit aussi les fonctions de signataire autorisé du Ministère pour tous les systèmes de TI, d'autorité ministérielle en matière de sécurité des communications (SECOM) et d'autorité ministérielle en matière de sécurité des émissions (EMSEC).

1.8 Intervenants externes

Les intervenants externes sont des organisations extérieures au MDN et aux FAC qui assurent l'interface ou l'échange de cyberinformations/de cyberrenseignements avec le MDN et les FAC et/ou la capacité de CD-DAR. Les intervenants externes de la CD-DAR sont énumérés dans le tableau 2 ci-dessous.

Ébauche

Tableau 2 – Intervenants externes de la CD-DAR

Organisation	Responsabilités
Sécurité publique Canada (SP)	SP est le fer de lance de la priorité numéro un du GC qui consiste à assurer la sécurité des Canadiens au pays et à l'étranger par la coordination des activités des ministères et organismes fédéraux chargés de protéger les Canadiens et leurs communautés, leurs entreprises et leurs intérêts. SP fonctionne comme une plaque tournante centralisée pour coordonner les efforts de lutte contre le terrorisme, les infrastructures essentielles et la sécurité cybernétique et des transports. Les FAC continuent de travailler en étroite collaboration avec SP pour soutenir la stratégie nationale de cybersécurité.
Centre de la sécurité des télécommunications Canada (CSTC)	Le CSTC est l'organisation nationale SIGINT pour le renseignement étranger et l'autorité technique (AT) pour la cybersécurité et l'assurance de l'information. Le Centre canadien pour la cybersécurité (CCC) du CSTC contribue à la protection des systèmes et des informations sur lesquels les Canadiens comptent chaque jour et est la principale autorité technique du GC en matière de cybersécurité. L'autorité opérationnelle reste du ressort de chaque ministère.
Services partagés Canada (SPC)	SPC fournit des services de TI modernes, sûrs et fiables aux organisations du GC. Une partie de son mandat consiste à concevoir et à exploiter une infrastructure de TI efficace, efficiente et sécurisée qui protège les données et les biens technologiques du GC. SPC élabore des politiques, des normes, des plans et des conceptions en matière de sécurité et fournit des services liés à la sécurité pour la prestation des services gouvernementaux. SPC est responsable de l'application de contrôles tels que le pare-feu, l'antivirus et l'antimaliciel, l'accès à distance sécurisé et la gestion de la vulnérabilité aux systèmes et aux services du GC.
Service canadien du renseignement de sécurité (SCRS)	Le SCRS recueille et analyse des informations liées à la menace concernant la sécurité du Canada dans des domaines tels que le terrorisme, l'espionnage, la prolifération des armes de destruction massive, l'ingérence étrangère et la cyberfalsification touchant les infrastructures essentielles.
Gendarmerie royale du Canada (GRC)	La GRC a un vaste mandat lorsqu'il s'agit d'enquêter sur des criminels et de les appréhender dans le monde en ligne, ou de mettre autrement fin à des activités de cybercriminalité. La stratégie de la GRC en matière de cybercriminalité a donc une large portée et reflète le rôle de la cybercriminalité dans

Ébauche

Organisation	Responsabilités
	plusieurs domaines d'application de la loi. Sa vision consiste à réduire la menace, les répercussions et la victimisation associées à la cybercriminalité au Canada au moyen de mesures d'application de la loi.
Groupe des cinq	Le partenariat du Groupe des cinq est une alliance de renseignement comprenant l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis et fait partie du traité multilatéral UKUSA. Le MDN et les FAC continueront à travailler en étroite collaboration avec les partenaires du Groupe des cinq sur la cybersécurité. Leur expertise et leur soutien sont indispensables au succès de nos opérations de cyberdéfense.
Organisation du Traité de l'Atlantique Nord (OTAN)	L'OTAN est une coalition militaire intergouvernementale qui s'appuie sur une cyberdéfense forte et résiliente pour remplir les tâches essentielles de l'Alliance en matière de défense collective, de gestion des crises et de sécurité coopérative. L'objectif principal de l'OTAN en matière de cyberdéfense est de protéger ses propres réseaux (y compris les opérations et les missions) et de renforcer la résilience dans toute l'Alliance. L'OTAN a créé un nouveau Centre d'opérations dans le cyberespace dans le cadre de sa structure de commandement renforcée. L'OTAN peut s'appuyer sur les cybercapacités nationales pour ses missions et ses opérations.

Ébauche

2 DESCRIPTION DU SYSTÈME ACTUEL

2.1 Emploi d'une cyberforce

Comme on l'a mentionné dans la section 1.3, le présent CONOPS porte sur l'emploi d'une force (EF) de cyberforce des FAC à l'appui des opérations et des missions des FAC. Les opérations interarmées sont menées au moyen du processus d'EF qui comprend toutes les activités nécessaires pour planifier les opérations interarmées, les exécuter et les examiner (leçons retenues [LR]). Inversement, le concept de soutien (CONSOUT) traite de la mise sur pied d'une force (MPF) et du développement des forces (DF) de la cyberforce et des cybercapacités opérationnelles[5].

Les opérations des FAC se déclinent en trois grandes catégories, à savoir les opérations de routine, de contingence ou d'intervention rapide. Les opérations de routine sont normalement de nature récurrente, peuvent généralement être planifiées et sont programmées sur une base annuelle. La plupart des opérations cybernétiques défensives sont des opérations de routine.

Les opérations de contingence sont planifiées en vue d'évènements connus ou ceux auxquels on peut raisonnablement s'attendre, ce qui permet un processus formel de planification opérationnelle. Le COIC a élaboré le plan de contingence (CONPLAN) des Instructions techniques du Génie construction (ITGC) pour les opérations dont l'objectif principal concerne les cyberopérations. Un ordre d'opération permanent (OOP) a également été élaboré pour faciliter l'instanciation du CONPLAN ITGC, appelé l'Op LADON.

Enfin, les opérations d'intervention rapide sont les activités d'EF qui nécessitent une action immédiate des FAC pour sauver des vies, réduire la souffrance humaine ou atténuer les dommages matériels. Afin de produire des effets rapides, on réduira la planification à l'essentiel, et on acceptera de plus grands risques dans la planification, la préparation et la coordination de l'opération. On traitera des opérations d'intervention rapide plus en détail dans la section 2.4[6].

2.2 Organisations de cyberdéfense

Comme l'illustre la figure 1, la cyberforce des FAC est employée sous l'autorité du CEMD et dirigée par le commandant de la cyberforce (CFC). Les opérations de routine sont dirigées par le commandant de la division du cyberespace des FAC, tandis que le CCCFI rend compte au commandant du COIC pour le C2 des opérations de contingence et d'intervention rapide.

Les rôles et les responsabilités en matière de cybersécurité et de défense de chaque unité de cyberdéfense du MDN et des FAC participant à la conduite d'OCD, ainsi que les processus actuels de cyberdéfense sont décrits dans les sous-parties suivantes.

2.2.1 Centre d'opérations des réseaux des Forces canadiennes (CORFC)

Le mandat du CORFC est tiré de PSE, de la stratégie nationale de cybersécurité, et plus particulièrement, dans les plans d'opération de la cyberdivision des Forces canadiennes et les directives du commandant du GOIFC.

---

[5] Publication interarmées des Forces canadiennes (PIFC) 3.0, *Les opérations*, chapitre 2, p. 2-1.

[6] PIFC 3.0, *Les opérations*, chapitre 6, p. 6-3.

Ébauche

Le CORFC est l'unité nationale opérationnelle de cyberdéfense qui se voit continuellement attribuer des tâches essentielles à la mission pour représenter le MDN et les FAC ainsi que les autorités opérationnelles de réseau applicables. Le CORFC a évolué d'une organisation exécutant des tâches d'opérations de réseau et d'assurance de mission à une organisation axée sur les opérations cybernétiques défensives – mesures défensives internes (OCD-MDI) [7].

Plus précisément, le CORFC est mandaté pour[8] :

a. Planifier et exécuter les OCD-MDI en appui au MDN et aux FAC;
b. Préparer les éléments de la force pour les OCD-MDI et les activités menées par l'EITS conformément à la posture de la force et disponibilité opérationnelle (PF&DO) du GOIFC;
c. Fournir des renseignements tactiques de cyberdéfense à l'appui des OCD tactiques des FAC, conformément aux priorités en matière de renseignement;
d. Maintenir une capacité de réponse de cyberdéfense en tout temps.

2.2.1.1 Structure organisationnelle

Le CORFC est une organisation de niveau 4 au sein du SMA(GI), et l'une des quatre unités relevant du GOIFC.

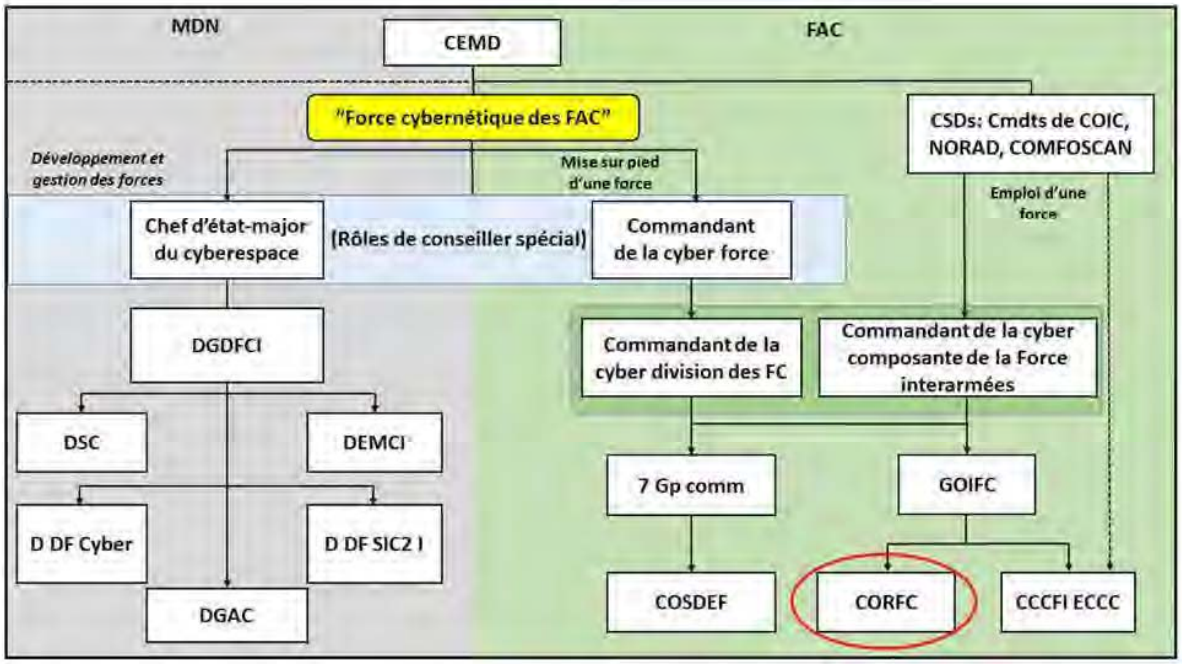


Figure 1 – CORFC – Organisation de niveau 4 au sein du GOIFC

[7] OCD-MDI : En opérations cybernétiques défensives, mesures prises et activités menées dans son propre cyberespace pour assurer la liberté d'action. BTD, Fiche nº 694340.

[8] CONOPS CORFC, 12 avril 2019.

2.2.1.2 Rôles et responsabilités

La mission du CORFC, de concert avec les partenaires et les alliés de l'ensemble du MDN et des FAC ainsi que du gouvernement, est d'obtenir et de maintenir la supériorité cybernétique dans les zones de responsabilité (ZResp) cybernétiques du MDN et des FAC afin d'assurer la liberté d'action de la force amie et de permettre aux commandants opérationnels de prendre des décisions éclairées en matière de défense et de sécurité en ce qui concerne le cyberenvironnement.

Au nom du CFC FAC, le CORFC dirige les opérations de routine et la défense des réseaux du MDN et des FAC. Le CORFC est une organisation dynamique qui a subi des changements importants. Les fonctions du CORFC sont dirigées par la section des opérations, la section des opérations de cyberdéfense (Ops CD) fournissant des conseils et une coordination tout au long du cycle de vie d'un cyberévènement.

2.2.2 Centre des opérations des services de la Défense (COSD)

Le Centre des opérations des services de la Défense (COSD) coordonne la prestation des services de TI dans l'ensemble du Ministère, fournit une orientation fonctionnelle aux centres de gestion des services et coordonne le soutien à l'entreprise de niveau 3, de concert avec le Bureau de services national (BSN). Au niveau national, le COSD effectue les demandes de service et la gestion des incidents, et est responsable de la coordination des opérations de service, y compris l'interface principale avec SPC et d'autres fournisseurs de services externes, dont Telus et Bell. En outre, il surveillera et facilitera la CS partagée du rendement des réseaux du MDN et des FAC.

2.2.2.1 Structure organisationnelle

Comme l'illustre la figure 2, le COSD est une organisation de niveau 4 au sein du SMA(GI) sous le 7 Gp Comm. Même si le COSD n'interagit pas directement avec les utilisateurs, il agit en tant qu'entité de niveau opérationnel pour faire acheminer à un niveau supérieur les incidents des CGS par l'intermédiaire du BSN ou de l'équipe de coordination des opérations de réseau.

Le COSD a deux unités chargées de fournir un soutien en service à la TI d'entreprise du MDN et des FAC :

a. Le BSN, au sein duquel les agents répondent à toutes les demandes adressées au COSD et prennent les mesures nécessaires en cas d'évènement;

b. Le Bureau des opérations de réseau, qui s'occupe de la gestion des demandes de service, de la gestion des incidents et de la gestion des problèmes.

Le COSD-BSN peut fonctionner à titre de fournisseur de services de premier niveau, mais il le fait habituellement durant les heures creuses ainsi qu'au cours du déploiement d'une opération. Le COSD soumettra les demandes de services au système de GSTIE au nom du client et transmettra la demande à l'unité de service désignée (USD) concernée du CGS pour que les mesures nécessaires soient prises lorsque le CGS retourne au travail.

Le COSD-opérations de réseau coordonne l'exécution des demandes nécessitant plusieurs fournisseurs de services, ce qui peut comprendre SPC. Le COSD résout les problèmes liés au transfert et met fin aux conflits d'exploitation des réseaux afin de garantir une disponibilité constante du réseau.

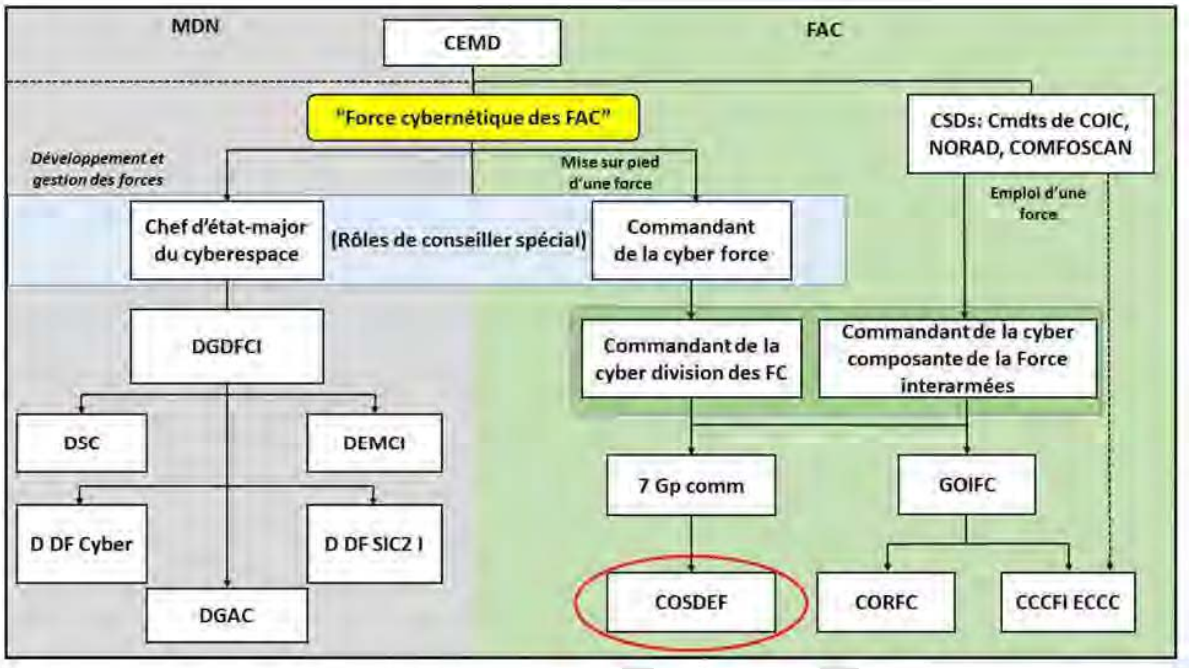


Figure 2 – COSD – Organisation de niveau 4 au sein du 7 Gp Comm

2.2.2.2 Rôles et responsabilités du COSD

Le COSD assure la coordination nationale des opérations de GSTI dans l'ensemble du MDN et des FAC. Il maintient et gère la technologie de l'information du MDN, s'occupe de gérer les SCI des FAC et coordonne la prestation de services de SCI en réponse aux besoins et aux objectifs opérationnels. Les responsabilités clés du COSD sont les suivantes :

a. Coordination des opérations des services de TI du MDN et des FAC;
b. Résolution de problèmes liés au service;
c. Surveillance et production de rapports quant au réseau d'entreprise;
d. Bureau de services national;
e. Interruption de service des Forces canadiennes;
f. Priorité à la gestion du changement.

2.2.3 Élément de coordination de composante cybernétique du commandant de la composante cybernétique des forces interarmées (ECCC CCCFI)

Compte tenu de l'environnement opérationnel de plus en plus cybernétique, une nouvelle section composée d'experts a été créée sous le CCCFI. L'Élément de coordination de composante cybernétique (ECCC) du CCCFI fournit une expertise et des conseils sur toute la gamme des cyberopérations au commandant du COIC et au personnel dans tous les domaines fonctionnels à l'appui des missions des FAC, tant au pays qu'à l'étranger. L'unité est placée sous le commandement opérationnel (OPCOM) du GOIFC, mais sous le contrôle opérationnel (OPCON) et l'autorité de planification du COIC, qui relève du chef d'état-major (opérations) du COIC.

2.2.3.1 Force opérationnelle de l'Élément de coordination de composante cybernétique (FO ECCC)

La Force opérationnelle de l'Élément de coordination de composante cybernétique (FO ECCC) est un prolongement du CCCFI dans le théâtre d'opérations nationales ou expéditionnaires. Le chef d'équipe de la FO ECCC rend compte au commandant de la Force opérationnelle (CFO) et relève du CCCFI par l'intermédiaire de l'ECCC CCCFI. Le chef d'équipe de la FO ECCC est normalement l'autorité déléguée pour formuler des conseils en matière de cyberopérations au CFO et agit en tant qu'élément de planification avancée des cyberactivités et des cyberopérations. Le CCCFI fournit au chef d'équipe de la FO ECCC des directives précises, des attentes claires et une limite de responsabilité.

2.2.3.2 Structure organisationnelle

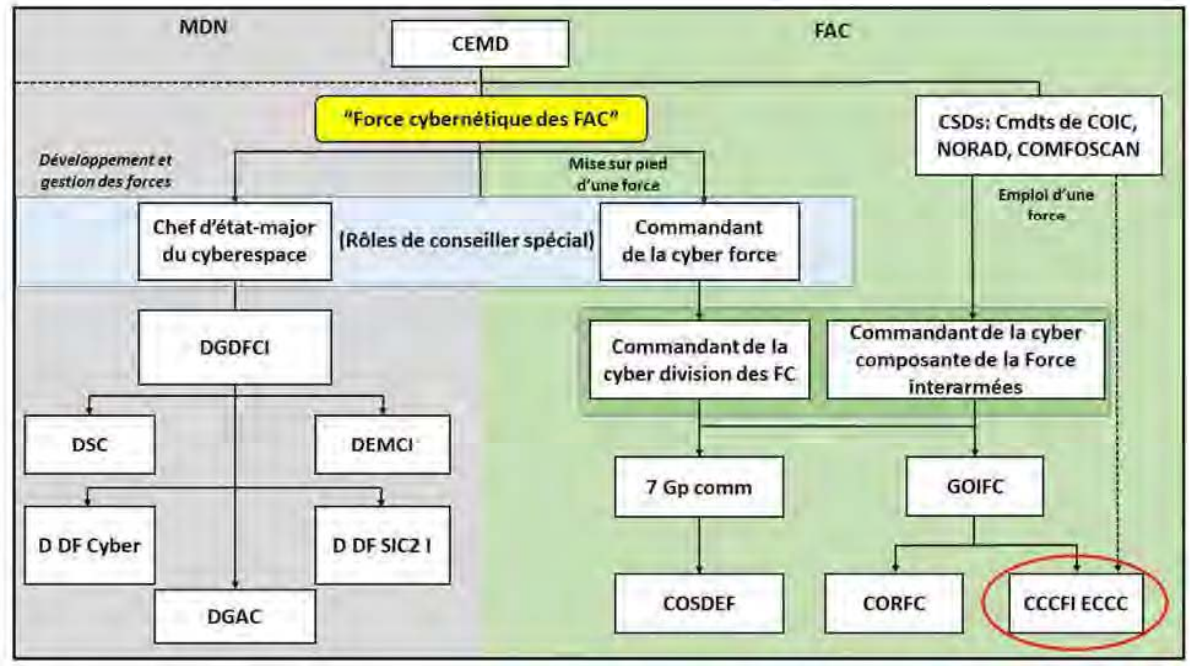


Figure 3 – ECCC CCCFI – Organisation de niveau 4 sous le GOIFC

2.2.3.3 Rôles et responsabilités de l'ECCC CCCFI

Le mandat de l'ECCC CCCFI est de conseiller le commandant du COIC et le personnel de planification sur les questions relatives au cyberdomaine et de préparer les cyberannexes à tous les ordres d'opération du COIC. Ses principaux rôles sont les suivants :

a. Fournir des conseils sur l'utilisation des cybercapacités pour les missions et les activités d'instruction;

b. Élaborer et tenir à jour une CS cybernétique complète pour le commandant du COIC;

c. Coordonner les activités avec d'autres ministères et les forces militaires alliées afin de déterminer la portée des menaces pour le Canada provenant du cyberespace et d'y réagir;

d. Fournir un point de présence unique du GOIFC à l'appui du commandant du COIC;

e. Saisir les leçons retenues en matière de cybernétique et déterminer les besoins afin de mettre en place des capacités modernes.

Outre son rôle de conseil et de planification en matière de cyberdéfense pour les opérations nationales et en déploiement, l'ECCC CCCFI ne participe pas directement à la cyberdéfense.

2.2.4 **Relation entre le CORFC, le COSD et l'ECCC CCCFI**

2.2.4.1 **Relation du CORFC avec l'ECCC CCCFI et le COSD**

Le CORFC, l'ECCC CCCFI et le COSD n'ont pas de responsabilités interdépendantes, mais collaborent dans la mesure du possible dans leur domaine respectif.

2.2.4.2 **Relation du COSD avec le CORFC**

Il n'y a pas de relation de commandement entre le COSD et le CORFC. Le COSD fournit un soutien au CORFC, mais ne joue pas un rôle actif dans la cyberdéfense. Le CORFC compte sur le soutien du COSD pour le signalement des incidents et la gestion des services, tels que la mise à jour des logiciels, la mise à niveau du matériel, etc. Depuis la séparation du COSD du CORFC, il n'y a pas eu de véritable relation entre les deux unités. Leurs rôles sont assez distincts, et leurs activités sont coordonnées (hiérarchisées, harmonisées, etc.) au niveau opérationnel par l'équipe J3 du DGOGI.

Ce qui suit est une façon simple de différencier le mandat du CORFC de celui du COSD :

Le CORFC s'occupe de « *ce qui se passe **sur** le réseau* »; tandis que

Le COSD s'occupe de « *ce qui se passe **au moyen du** réseau* ».

2.2.4.3 **Relation du COSD avec l'ECCC CCCFI**

Comme pour le CORFC, le COSD n'a pas de relation de commandement avec l'ECCC CCCFI, mais il existe une importante collaboration entre eux pour fournir un soutien aux experts à des fins de planification de la cyberdéfense.

2.2.4.4 **Relation de l'ECCC CCCFI avec le CORFC**

Même s'il existe une forte collaboration technique avec le CORFC, l'ECCC CCCFI n'a pas de relation de commandement avec le CORFC. Le CORFC soutient l'ECCC CCCFI à l'aide de conseils d'experts en matière de planification de la cyberdéfense pour les opérations nationales et en déploiement.

2.3 Concept opérationnel actuel du CORFC[9]

La tâche essentielle du CORFC est la conduite d'OCD-MDI en appui au MDN et aux FAC. Bien que la nature de ces activités varie, il est important de noter que le CORFC exerce ses fonctions dans le cadre de la cyberdéfense et de la cybersécurité. Même si les deux sont étroitement liées, il existe des différences qui doivent être comprises par tous les membres du CORFC et ceux qui interagissent avec l'unité. La mise en œuvre, l'application et la gestion de la politique et des

[9] Concept opérationnel, CONOPS CORFC, page 3.

normes de cybersécurité sont des facteurs essentiels pour la conduite efficace des OCD. L'OCD se concentre sur la continuité des opérations militaires (assurance de la mission) où la cybersécurité est axée sur le maintien de la confidentialité, de l'intégrité et de la disponibilité des réseaux du MDN et des FAC grâce aux pratiques exemplaires de l'industrie.

Toutes les activités et fonctions du CORFC peuvent être divisées en quatre phases :

a. Orientation et direction stratégiques/opérationnelles;
b. Établissement des priorités et planification;
c. Exécution;
d. Reconstitution.

La figure 4 illustre le concept opérationnel du CORFC.

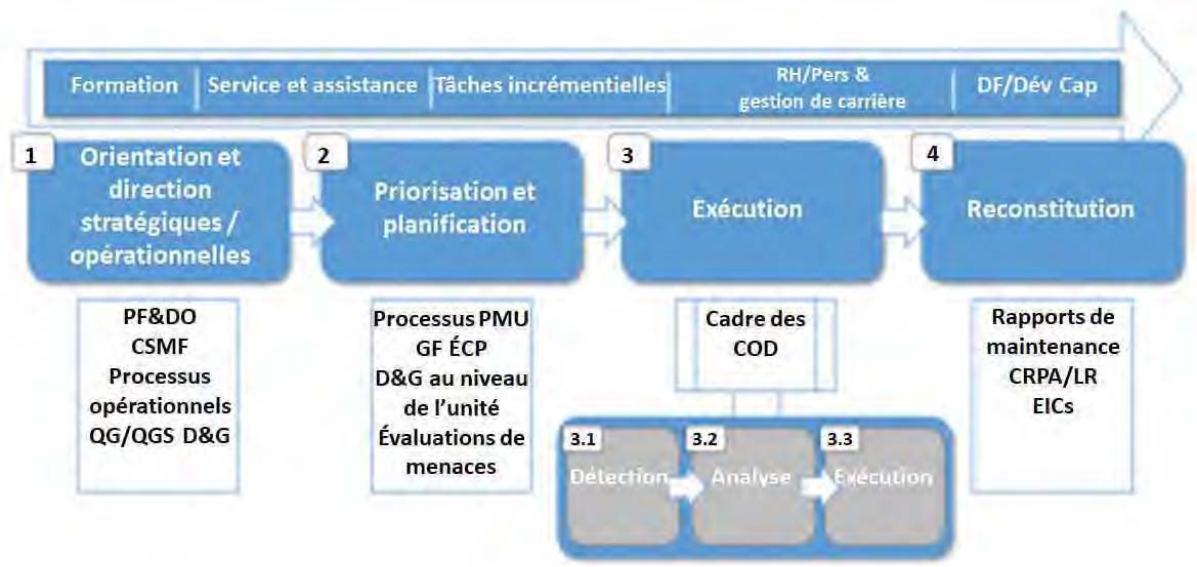


Figure 4 – Concept opérationnel du CORFC

La phase d'exécution est le centre de gravité du CORFC dans la conduite des cyberopérations et est réalisée par l'application d'un cadre des OCD. Le cadre des OCD (illustré à la figure 5) définit le concept d'emploi des éléments de force du CORFC.

Les principaux apports à cette étape sont le renseignement au niveau tactique et les objectifs et effets souhaités pour permettre l'exécution de l'OCD par les éléments de force du CORFC.

2.3.1 Cadre des opérations cybernétiques défensives

Toutes les activités liées aux OCD s'inscrivent dans l'une des trois phases principales du cadre des OCD : détection, analyse et action. (Voir la figure 5.)

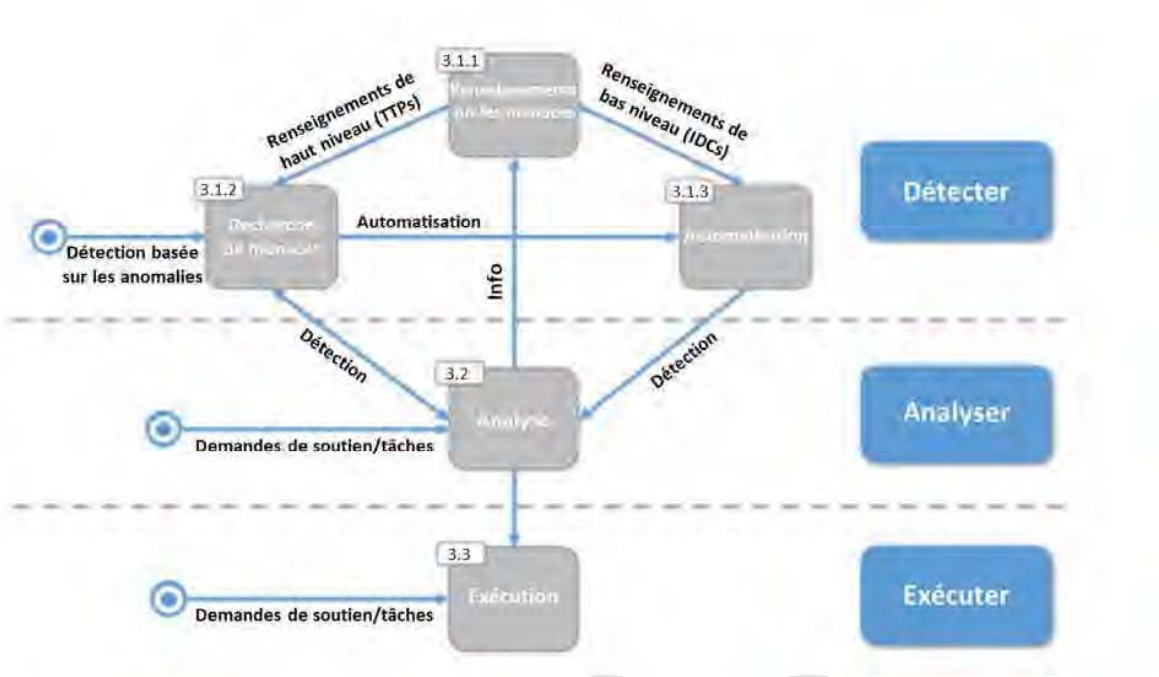


Figure 5 – Cadre des OCD

2.3.1.1 **Détection**

La phase de détection comprend les activités nécessaires à la collecte et à la diffusion de produits de renseignement exploitables pour soutenir la découverte d'un évènement de cybersécurité menant à la détection d'incidents de cybersécurité.

2.3.1.2 **Analyse**

Une fois que les menaces ont été détectées, une analyse plus approfondie est nécessaire pour fournir un contexte à la nature de la menace et doter les éléments de force du CORFC des connaissances suffisantes pour pouvoir passer à la phase de l'action. Les principales activités menées au cours de cette phase sont l'analyse détaillée des menaces détectées sur le réseau et l'hôte afin de déterminer l'ampleur et la profondeur de la compromission, y compris l'analyse détaillée des maliciels et l'enquête de la criminalistique cybernétique des points d'extrémité touchés.

2.3.1.3 **Action**

Une fois que les éléments de force ont une connaissance suffisante de la nature des menaces détectées, ils sont alors en mesure d'agir. La nature de cette intervention est principalement déterminée par la séquence des ordres d'opération et les objectifs et effets inhérents qui doivent être atteints. Les activités typiques d'OCD-MDI qui concernent cette phase sont les suivantes :

a. Intervention en cas d'incident;

b. Opérations de déception;

c. Opérations de correction;

Ébauc

d. Rapport.

2.4 Interactions organisationnelles et échange de renseignements/d'informations

L'échange et le partage de renseignements/d'informations entre les différentes équipes du CORFC et les intervenants sont essentiels à la réussite des opérations cybernétiques défensives.

2.4.1 Équipe des opérations de cyberdéfense (Ops CD)

L'équipe des opérations de cyberdéfense (Ops CD) coordonne les OCD du MDN et des FAC et les interventions en cas d'incident avec les organisations internes et externes du Ministère. Les Ops CD fournissent une CS au moyen de rapports et coordonnent les efforts des différentes équipes du CORFC en cas de cyberévènement ou de cyberincident.

2.4.1.1 Activités clés de l'équipe des Ops CD

Les activités clés réalisées par les Ops CD sont les suivantes :

a. Coordination avec des organisations externes (au CORFC) sur les cyberévènements;
b. Coordination au sein du CORFC sur les cyberévènements du MDN et des FAC;
c. Briefing hebdomadaire au CEM et au COIC.

2.4.1.2 Interaction et échange de renseignements/d'informations avec les intervenants

Les interactions des Ops CD et l'échange de renseignements/d'informations avec les intervenants comprennent ce qui suit :

a. Fournir une CS et demander une autorisation supérieure au GOIFC;
b. Échanger des rapports avec le Groupe des cinq quotidiennement/hebdomadairement;
c. Collaborer avec le SCRS au besoin, selon l'attribution des tâches;
d. Recevoir des rapports de renseignement préliminaires du CCC;
e. Recevoir des alertes, des avis de mesures prises (p. ex. application de correctifs) de SPC – EIIC GC (Équipe d'intervention en cas d'incident cybernétique du gouvernement du Canada);
f. Recevoir des alertes de la Sécurité publique – Centre canadien de réponse aux incidents cybernétiques (CCRIC) sur des activités intéressant le MDN et les FAC (par exemple, une adresse IP [protocole Internet] inhabituelle du MDN accédant à des réseaux externes);
g. Échanger également des informations sur les incidents avec la capacité d'intervention en cas d'incidents informatiques de l'OTAN (NCIRC).

Voir la figure 9 de l'annexe A pour une représentation graphique des interactions de l'équipe des Ops CD et de l'échange de renseignements/d'informations avec les intervenants.

2.4.1.3 Flux de travail de l'équipe des Ops CD

Les trois flux de travail utilisés par les Ops CD sont également présentés dans l'annexe A et sont les suivants :

Ébauche

Figure 15 – Flux de travail des Ops CD pour la coordination des cyberévènements;

Figure 16 – Gestion des cyberévènements, y compris avec le Groupe des cinq sur Pegasus, par l'intermédiaire de l'équipe d'intervention en cas d'incident informatique de la Défense;

Figure 17 – Flux de travail de la cybergestion et de la cyberinformation.

2.4.2 **Cellule de renseignement sur les cybermenaces (CRCM)**

La cellule de renseignement sur les cybermenaces (CRCM) fonctionne actuellement de 8 h à 17 h (avec une capacité d'appoint) pour fournir des renseignements proactifs et réactifs afin d'améliorer les opérations de cyberdéfense. L'accent est mis sur les systèmes des FAC qui sont vulnérables, précieux pour un adversaire et essentiels pour les opérations en déploiement et la conduite quotidienne des opérations. Les principaux objectifs de la CRCM sont les suivants :

a. Comprendre les ITI essentielles du MDN et des FAC et leurs vulnérabilités;

b. Comprendre les tactiques, techniques et procédures (TTP) adverses et les intentions en ce qui concerne ces vulnérabilités;

c. Atténuer le risque résiduel pour les systèmes du MDN et des FAC de manière proactive, au moyen de conseils aux administrateurs et aux ingénieurs de systèmes;

d. Réduire le temps d'intervention en cas de compromission, par la création d'une stratégie d'intervention basée sur la compréhension des réseaux du MDN et des FAC et des actions de leurs adversaires.

2.4.2.1 **Activités clés du CRCM**

Les activités clés réalisées par le CRCM sont les suivantes :

a. Appui à la décision du renseignement pour les cyberopérations – Le CRCM met en œuvre des processus de renseignement conventionnels (par exemple, l'analyse tactique de l'environnement opérationnel [ATEO]) pour faire face au cyberdomaine et fournir des renseignements et des priorités à l'appui du processus décisionnel du commandant;

b. Sensibilisation aux menaces émergentes – Le CRCM doit se tenir au courant du renseignement cybernétique à source ouverte et se sensibiliser aux menaces, cibler les modèles et avoir accès aux données historiques pour dégager des tendances;

c. Évaluations de la menace tactique (avec l'ECCC CCCFI) – Le CRCM prépare des évaluations de la menace tactique selon les besoins, généralement uniquement lorsque l'équipement se trouve dans un théâtre d'opérations. Ces évaluations sont effectuées conjointement au moyen du travail réalisé par l'ECCC CCCFI (anciennement connu sous le nom d'équipe interarmées des cyberopérations [EICO]) du COIC.

2.4.2.2 **Interaction et échange de renseignements/d'informations avec les intervenants**

Les interactions du CRCM et l'échange de renseignements/d'informations avec les intervenants comprennent ce qui suit :

Ébauche

a. Fournir des renseignements susceptibles d'influencer les futures opérations à l'officier des opérations (O Ops) du CORFC;

b. Fournir des rapports de renseignement et des priorités en matière de renseignement aux Ops CD et recevoir également des tâches des Ops CD;

c. Peaufiner les évaluations de la menace et des risques (EMR) et les fournir à l'ECCC CCCFI; cependant, il recevra l'évaluation de la mission de l'ECCC CCCFI pour analyse;

d. Échanger des renseignements avec la cyberéquipe du Commandement du renseignement des Forces canadiennes (COMRENSFC) et lui faire rapport;

e. Fournir des renseignements à SPC et recevoir des informations sur les menaces de SPC pour la CS;

f. Fournir des briefings hebdomadaires sur les incidents/menaces sur les réseaux du GC et recevoir des informations sur les menaces pour la CS de la part de la Sécurité publique et du CCRIC;

g. Solliciter l'expertise du CCC et recevoir en même temps des alertes et des avis de vérification.

h. Même s'il ne s'agit pas d'une démarche officielle, échanger des informations avec le régiment des transmissions interarmées pour préparer l'équipement et le déploiement.

Une représentation graphique des interactions du CRCM et des échanges de renseignements/d'informations avec les intervenants est fournie à la figure 10 de l'annexe A.

2.4.3 **Équipe de traitement des incidents**

L'équipe de traitement des incidents du CORFC, conformément à la NGI 6003-1-1, joue le rôle de chef de file national pour le traitement des incidents dans le cadre établi pour une approche d'entreprise coordonnée. L'équipe de traitement des incidents est le point de contact central pour le signalement et le traitement de tous les incidents de sécurité des systèmes d'information. Pour obtenir de plus amples informations sur les activités de l'équipe de traitement des incidents du CORFC, veuillez vous reporter à la référence N.

2.4.3.1 **Activités clés de l'équipe de traitement des incidents**

Les activités clés réalisées par l'équipe de traitement des incidents sont les suivantes :

a. Le signalement et le traitement de tous les incidents de sécurité des systèmes d'information – Les incidents traités par l'équipe de traitement des incidents ne sont pas tous des cyberincidents. L'équipe s'appuie sur les officiers de la sécurité des systèmes d'information (OSSI) pour accomplir les tâches sur place afin de détecter les incidents et d'alerter l'équipe de traitement des incidents. Les OSSI ne sont généralement pas des postes à temps plein et, le plus souvent, leurs tâches ne sont pas prioritaires.

b. L'instruction des OSSI, qui est essentielle pour assurer la conformité et détecter les incidents.

Ébauche

2.4.3.2 **Interaction et échange de renseignements/d'informations avec les intervenants**

Les interactions de l'équipe de traitement des incidents et l'échange de renseignements/d'informations avec les intervenants comprennent ce qui suit :

a. Fournir des rapports d'incidents aux Ops CD et recevoir des tâches des Ops CD;

b. Recevoir les rapports de renseignement de SPC;

c. Recevoir les rapports d'incident des OSSI des unités/bases/escadres;

d. Fournir des renseignements aux OSSI nationaux et aux OSSI des éléments des FAC à des fins d'atténuation et d'instruction;

e. Informer le centre spécial national du Chef du renseignement de la Défense (CRD) de tout incident de sécurité des TI déclenché par l'équipe de traitement des incidents et touchant des renseignements compartimentés de nature délicate;

f. Signaler immédiatement au Directeur général – Sécurité de la Défense (DGSD) toute infraction à la sécurité, toute violation de la sécurité ou toute tentative de pénétration des mesures de sécurité d'informations hautement délicates ou d'équipements classifiés;

g. Fournir les incidents au CCC;

h. Fournir des incidents à risque moyen ou élevé au Dir Sécur GI; recevoir également des missions du Dir Sécur GI.

Une représentation graphique des interactions de l'équipe de traitement des incidents et de l'échange de renseignements/d'information avec les intervenants est fournie à la figure 11 de l'annexe A.

2.4.3.3 **Flux de travail de l'équipe de traitement des incidents**

Le flux de travail principal de l'équipe de traitement des incidents est présenté à l'annexe A et est le suivant :

Figure 18 – Flux de travail de l'équipe de traitement des incidents – Processus de gestion des incidents liés à la sécurité des systèmes d'information du MDN.

2.4.4 **Équipe de surveillance**

L'équipe de surveillance procède à une analyse du trafic des réseaux du MDN et des FAC afin de détecter les appareils potentiellement compromis en vue d'une enquête plus approfondie. Les schémas de manœuvre comprennent la détection des menaces connues basée sur les signatures (signatures commerciales et personnalisées) et la détection basée sur les anomalies des menaces précédemment inconnues. L'équipe de surveillance participe au maintien de la fiabilité des réseaux, ce qui permet aux FAC de maintenir leur supériorité cybernétique au sein de la ZResp cybernétique des FAC.

2.4.4.1 **Activités clés de l'équipe de surveillance**

Les activités clés réalisées par l'équipe de surveillance sont les suivantes :

Ébauche

a. Surveillance de la sécurité des menaces préalablement détectées, par exemple les menaces fournies par les services d'abonnement ou par d'autres sources connues;

b. Recherche sur la détection et la détermination des anomalies du réseau – L'anomalie du trafic du réseau déclenchera une analyse qui peut nécessiter la participation d'autres équipes du CORFC, par exemple pour accéder aux dossiers historiques afin d'expliquer les schémas de trafic pour déterminer si l'anomalie peut être expliquée;

c. Participation aux visites d'aide technique (VAT) – Avec les membres de la reconnaissance (RECO) et l'équipe de la criminalistique cybernétique, l'équipe de surveillance apporte un soutien aux VAT.

2.4.4.2 **Interaction et échange de renseignements/d'informations avec les intervenants**

Les interactions de l'équipe de surveillance et l'échange de renseignements/d'informations avec les intervenants comprennent ce qui suit :

a. Fournir aux Ops CD des retours et des rapports de surveillance autogénérés pour le triage et la distribution aux unités selon les besoins; recevoir également des tâches des Ops CD;

b. Consulter et utiliser des outils du CCC afin de recueillir de meilleures données de renseignement;

c. Recevoir des conseils de la Police militaire (PM) sur les questions juridiques;

d. Échanger continuellement des informations avec l'Unité nationale de contre-espionnage (UNCE), le Service national des enquêtes des Forces canadiennes (SNEFC) et SPC – EIIC GC;

e. Recevoir le soutien des outils du DIIGI 3-5 pour s'assurer que tous les systèmes sont à jour;

f. Collaborer avec les équipes de la CRCM, de la RECO et de la criminalistique cybernétique et échanger continuellement des informations avec ces équipes;

g. Recevoir les capacités internes et la collecte de données de l'équipe de soutien des systèmes de détection des intrusions.

Une représentation des interactions de l'équipe de surveillance et des échanges de renseignements/d'informations avec les intervenants est fournie à la figure 12 de l'annexe A.

2.4.4.3 **Flux de travail de l'équipe de surveillance**

Les deux flux de travail utilisés par l'équipe de surveillance sont présentés à l'annexe A et sont les suivants :

Figure 19 – Flux de travail lié à l'évaluation des menaces connues;

Figure 20 – Flux de travail lié à l'évaluation des menaces inconnues.

2.4.5 **Équipe de reconnaissance**

Les troupes de RECO fournissent des évaluations réalistes et en direct de la vulnérabilité et de l'exploitation avancée des systèmes d'information et des procédures pour évaluer la posture de sécurité du client et effectuent des démonstrations contrôlées de ce qu'un attaquant pourrait

Ébauche

accomplir dans l'infrastructure des TI d'un client. Les évaluations de la posture de sécurité sont adaptées aux besoins et aux systèmes d'information des clients et sont effectuées sous une supervision stricte. La troupe de RECO fournit un rapport final et, au besoin, un briefing de recommandations particulières sur la manière d'améliorer la posture de sécurité du client sur la base des résultats de l'évaluation.

2.4.5.1 **Activités clés de l'équipe de RECO**

Les activités clés réalisées par l'équipe de RECO sont les suivantes :

a. Découverte des actifs (pour fournir une CS et des informations sur un réseau donné, y compris le système d'exploitation, les ports et les services fonctionnant sur chaque hôte, etc.);

b. Balayage ciblé (pour confirmer la conformité aux fins de l'ESA, et la CS en cours à l'appui des missions);

c. Évaluation de la vulnérabilité (pour valider la mise en œuvre des recommandations d'essais de validation de l'ingénierie de sécurité [VIS] du DIIGI et la CS continue des réseaux du MDN et des FAC et pour vérifier que les recommandations de sécurité ont été mises en œuvre);

d. Essai de pénétration – Pour déterminer la faisabilité d'un ensemble particulier de vecteurs d'attaque; cibler les niveaux de risque liés à l'exécution de plusieurs vulnérabilités à faible risque traitées dans une séquence particulière; cerner les vulnérabilités qui peuvent être difficiles ou impossibles à détecter au moyen d'un logiciel automatisé d'analyse des vulnérabilités des réseaux ou des applications; évaluer l'ampleur des répercussions sur les activités et des répercussions opérationnelles potentielles des attaques réussies; évaluer la capacité des défenseurs de réseau à détecter les attaques et à y faire face avec succès; et fournir des preuves à l'appui d'une vigilance accrue dans la posture de sécurité des systèmes de TI du MDN et des FAC;

e. Forces d'opposition (FOROP) dans le cadre d'exercices;

f. *(Pas une capacité actuelle)* Constitution d'équipes rouges.

2.4.5.2 **Interaction et échange de renseignements/d'informations avec les intervenants**

Les interactions de l'équipe de RECO et l'échange des renseignements/d'informations avec les intervenants comprennent ce qui suit :

a. Recevoir des tâches des Ops CD et fournir en même temps des alertes en retour;

b. Consulter le CRCM pour obtenir des informations;

c. Échanger au sujet des activités suspectes, analyser le trafic de la VAT et donner des conseils sur des tâches particulières avec l'équipe de surveillance;

d. Fournir des tâches au détachement de RECO;

e. Fournir des VAT – Analyse après action à l'équipe de la criminalistique cybernétique;

f. Demander des balayages de vulnérabilité particuliers à l'équipe de soutien de l'évaluation des vulnérabilités d'entreprise;

Ébauche

g. Fournir une évaluation et des recommandations aux « clients » et échanger des informations relatives aux demandes de vulnérabilité du réseau;

h. Recevoir les résultats des tests de pénétration du Centre d'essais et de développement classifiés de VIS du DIIGI.

Une représentation des interactions de l'équipe de RECO et de l'échange de renseignements/d'informations avec les intervenants est fournie à la figure 13 de l'annexe A.

2.4.5.3 **Flux de travail de l'équipe de RECO**

L'équipe de RECO utilise plusieurs flux de travail, comme on peut le constater à l'annexe A. Ces flux de travail sont les suivants :

Figure 21 – Flux de travail lié à la découverte des actifs;

Figure 22 – Flux de travail lié au balayage des cibles;

Figure 23 – Flux de travail lié à l'évaluation de la vulnérabilité;

Figure 24 – Flux de travail lié au test de pénétration du système/réseau;

Figure 25 – Flux de travail lié à l'émulation des tests.

2.4.6 **Équipe de la criminalistique cybernétique**

L'équipe de la criminalistique cybernétique fournit des services spécialisés d'analyse numérique au MDN et aux FAC. Elle fournit également une analyse technique des nouvelles cybermenaces et des techniques de maliciels utilisées par les adversaires pour pénétrer les réseaux du MDN et des FAC. En plus de l'analyse des maliciels, la section de la criminalistique cybernétique est chargée de maintenir ses relations et de collaborer avec d'autres organismes en ce qui concerne les évènements de cybersécurité.

2.4.6.1 **Activités clés de l'équipe de la criminalistique cybernétique**

Les activités clés réalisées par l'équipe de la criminalistique cybernétique sont définies dans le tableau 3.

Tableau 3 – Activités de l'équipe de la criminalistique cybernétique

Saisie de données par image (par exemple, saisie de données à partir des appareils visés)	
Image du disque complet	Une image physique (exacte, copie secteur par secteur d'un appareil média) ou logique (toutes les données actives sur une partition logique – pas de fichiers supprimés) du dispositif de stockage original.
Image de dispositif amovible	Une image physique (exacte, copie secteur par secteur d'un appareil média) ou logique (toutes les données actives sur chaque partition – aucun fichier supprimé) du dispositif original.

Ébauche

Image d'un appareil mobile	Récupération/recherche de documents, d'images, de vidéos, de coordonnées et peut-être d'informations de courriel et d'informations de localisation selon le type d'acquisition de l'appareil mobile.
Saisie de fichiers/dossiers	Copie exacte et inchangée (le cas échéant) des fichiers et/ou dossiers du dispositif original.
Analyse des évènements du système	
Analyse antivirus avec les derniers moteurs antivirus mis à jour	Les balayages s'effectuent sur des dispositifs utilisant au moins cinq des moteurs indiqués ci-dessous : • Symantec endpoint protection • Avast • Avg • Kaspersky • McAfee • Avira
Enquête sur la sécurité des opérations (SECOP).	• Utilisation inappropriée des comptes admin • Complexité du mot de passe • Mauvaises pratiques de recyclage (réutilisation d'un système sans imagerie appropriée, nettoyage, etc.)
Exécution d'une enquête sur la vulnérabilité hors ligne	• Vérification des nœuds pour des vulnérabilités particulières • Vérification des pratiques exemplaires en matière de sécurité
Analyse des maliciels	
Balayages des antivirus	Détermination si le fichier est malveillant ou non. Comparaison avec les bonnes/mauvaises valeurs de hachage (le cas échéant).
Analyse dynamique	Liste des modifications apportées au système pour tenir compte d'éléments tels que les changements apportés au système de fichiers, au registre, aux connexions réseau, etc. et créer des signatures pour une détection plus poussée.

Ébauche

Analyse statique	Rétro-ingénierie pour déterminer les capacités potentielles ainsi que pour détecter les techniques de brouillage et de cryptage à intégrer afin de concevoir des outils de cryptage des canaux de C2 et des signatures pour la détection.
Examen des journaux des micrologiciels	• Détermination des détails pour les informations générales; à savoir si le micrologiciel lui-même est crypté ou non. • Comparaison entre les micrologiciels fournis par le fabricant et les micrologiciels fournis pour l'analyse.
Analyse du fichier de configuration	
Analyse complète de l'image du micrologiciel	
Inclusion de l'analyse des maliciels sur plusieurs fichiers trouvés dans une même source	Une liste de tous les fichiers des dispositifs fournis avec une réponse vraie ou fausse quant à leur caractère malveillant ou non; si une sortie détaillée pouvait être fournie selon une enquête normale d'analyse des maliciels par fichier malveillant.
Analyse de la sécurité des transmissions (TRANSEC)	
Balayage des mots clés/restrictions	Désignation de fichiers/dossiers faisant l'objet d'une restriction particulière ou contenant des mots clés précis. La liste des restrictions doit être fournie par le client.
Utilisation de matériel amovible	Liste des fichiers associés à l'appareil, y compris la méthode et le calendrier de transfert (le cas échéant).
Accès au réseau de partage	Détermination de l'accès à des dossiers/fichiers précis du réseau, y compris la date, l'heure, le compte d'utilisateur et les modifications apportées à ces dossiers/fichiers.
Recherche sur la prévention des incidents	
Recommandations pour l'atténuation des incidents	

En plus des services énumérés dans le catalogue des services de l'équipe de la criminalistique cybernétique, l'équipe fournit des recommandations d'atténuation et des capacités de recherche pour la prévention des menaces.

2.4.6.2 **Interaction et échange de renseignements/d'informations avec les intervenants**

Les interactions de l'équipe de la criminalistique cybernétique et l'échange de renseignements/d'informations avec les intervenants comprennent ce qui suit :

a. Recevoir des tâches des Ops CD, mais aussi fournir des rapports sur les incidents et les tâches;

b. Fournir aux unités du MDN les informations recueillies par l'équipe d'intervention immédiate de la cyberdéfense pour évaluer la situation et acquérir des artefacts, conformément aux ordres de mission;

c. Fournir une aide technique à la GRC (section de la criminalité technologique) par l'intermédiaire de l'UNCE en de rares occasions;

d. En de rares occasions, fournir une aide au CCC pour l'analyse des logiciels et du matériel;

e. Collaborer avec l'équipe de la criminalistique cybernétique de SPC, le SNEFC et l'UNCE sur tous les cas de criminalistique cybernétique;

f. Participer à des exercices avec les Alliés deux à trois fois par an.

Une représentation des interactions de l'équipe de la criminalistique cybernétique et de l'échange de renseignements/d'informations avec les intervenants est fournie à la figure 14 de l'annexe A.

2.4.6.3 **Équipe de cyberprotection (ECP)**

Lors de l'intervention en cas d'incident et de l'analyse de celui-ci, les ingénieurs en sécurité doivent se rendre sur place et saisir de grands ensembles de données provenant des réseaux faisant l'objet de l'enquête pour les analyser hors ligne sans produire d'indications que le réseau est en cours d'analyse. Les équipes de la criminalistique cybernétique et d'intervention en cas d'incident du MDN doivent se rendre dans des endroits éloignés pour procéder à l'acquisition de données sur place et à l'analyse locale des informations de la criminalistique cybernétique afin de fournir à la chaîne de commandement du MDN des informations sur les systèmes concernés et d'évaluer les répercussions sur l'environnement.

2.4.7 **Équipe de soutien des systèmes de détection des intrusions**

L'équipe de soutien des systèmes de détection des intrusions est chargée de fournir un soutien en tout temps pour les éléments suivants :

a. Configuration, essai et déploiement de divers systèmes de détection des intrusions (SDI) et d'outils d'analyse sur les capteurs/serveurs SDI du CORFC pour tous les réseaux surveillés par les FAC;

b. Configuration, essai et déploiement de divers capteurs/serveurs SDI sur tous les réseaux;

c. Mise à jour et mise à niveau des suites SDI, au besoin;

d. Soutien des logiciels/du matériel SDI et maintenance du matériel SDI (Security Onion, Sourcefire, conçus précisément pour le CORFC).

2.4.7.1 **Activités clés de l'équipe de soutien des systèmes de détection des intrusions**

Les activités clés réalisées par l'équipe de soutien des systèmes de détection des intrusions sont les suivantes :

a. Déploiement/maintenance des outils SDI d'entreprise – Comprend la configuration, les essais et le déploiement des outils sur les capteurs, le déploiement des capteurs et la maintenance du matériel/des logiciels);

b. Mise au point des capacités SDI (Remarque : certains outils commerciaux ne fournissent pas les données nécessaires à une analyse approfondie, l'équipe de soutien des systèmes de détection des intrusions mettra au point des outils internes pour répondre à des besoins particuliers).

2.4.7.2 **Flux de travail de l'équipe de soutien des systèmes de détection des intrusions**

L'équipe de soutien des systèmes de détection des intrusions utilise deux flux de travail distincts, présentés à l'annexe A. Ces flux de travail sont les suivants :

Figure 26 – Flux de travail du système de détection des intrusions (SDI);

Figure 27 – Flux de travail lié à la mise au point des capacités SDI.

2.4.8 **Équipe de soutien de l'évaluation des vulnérabilités d'entreprise**

L'équipe de soutien de l'évaluation des vulnérabilités d'entreprise effectue la gestion des vulnérabilités et des risques sur des réseaux sélectionnés au moyen de l'IP360. L'équipe de soutien de l'évaluation des vulnérabilités d'entreprise procède à un balayage du réseau au moyen de profils précis à intervalles réguliers (trois fois par an, en plus d'un balayage non programmé) et selon les besoins. L'équipe de soutien de l'évaluation des vulnérabilités d'entreprise traite les rapports de balayage pour détecter les vulnérabilités et crée des billets GSTIE pour les mesures à prendre.

2.4.8.1 **Activités clés de l'équipe de soutien de l'évaluation des vulnérabilités d'entreprise**

Les activités clés réalisées par l'équipe de soutien de l'évaluation des vulnérabilités d'entreprise sont les suivantes :

a. Effectuer des balayages de routine sur les réseaux du MDN et des FAC – Sur l'IRSC, les balayages de routine sont effectués trois fois par an, en plus d'un balayage non programmé, à la recherche de mauvais mots de passe, de correctifs périmés, d'applications inactives/anciennes qui auraient dû être supprimées, etc.;

b. Traiter les rapports de balayage et détecter les vulnérabilités – Pour éliminer les faux positifs, regrouper les cas semblables et créer un billet GSTIE pour mesure à prendre;

c. Créer des billets GSTIE à l'intention des équipes de soutien en TI respectives pour qu'elles y donnent suite;

d. Mettre à jour les bases de données historiques pour tous les rapports d'analyse.

2.4.8.2 **Flux de travail de l'équipe de soutien de l'évaluation des vulnérabilités d'entreprise**

Le flux de travail utilisé par l'équipe de soutien de l'évaluation des vulnérabilités d'entreprise est présenté à l'annexe A, à la figure 28 – Flux de travail lié à l'évaluation des vulnérabilités d'entreprise.

Ébauche

2.5 Élaboration de l'instruction – Ensembles de compétences, rôles et possibilité de cyberexercices

Les cyberopérateurs constituent l'épine dorsale de la cyberforce. Ils sont le personnel, à tous les niveaux de grade, dont le rôle principal est de « […] *[mener] des cyberopérations défensives et, lorsque cela est nécessaire et faisable, actives. Ils sont en liaison avec des ministères et des agences gouvernementales ainsi qu'avec des alliés du Canada, avec qui ils collaborent afin d'accroître la capacité du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) à offrir un cyberenvironnement sécuritaire. Les cyberopérateurs surveillent les réseaux de communication des FAC afin de détecter des tentatives d'accès non autorisé et d'intervenir. Ils offrent aussi un soutien numérique répondant aux besoins opérationnels de la Marine, de l'Armée de terre, de l'Aviation et des intervenants interarmées*[10] ». Les cyberopérateurs ne sont pas des techniciens de TI, et les cyberforces ne sont pas le personnel de TI.

Il ne faut pas confondre la profession de cyberopérateur avec celle de technicien des systèmes d'information et de télécommunications aérospatiales (SITA), de spécialiste des systèmes de communication et d'information de l'Armée de terre (SSCIAT), d'opérateurs d'équipement d'information de combat (Marine) (OP EICM) et les professions des communicateurs navals (COMM N). Ces groupes professionnels militaires s'occupent principalement de la configuration, de l'installation, de l'exploitation et de la maintenance des réseaux de communication et de l'ITI, tandis que les cyberopérateurs se concentrent sur la surveillance et la protection de l'ITI contre les menaces hostiles et le refus de l'utilisation du cyberespace par les forces hostiles. Cela dit, étant donné leur connaissance des cybermenaces et des méthodes d'attaque, les cyberopérateurs sont souvent consultés par le personnel des groupes SITA, SSCIAT, OP EICM et COMM N pendant les phases de configuration, d'installation, d'exploitation et de maintenance des réseaux de communication et de l'ITI afin d'aider à la mise en place de mesures de sécurité améliorées et d'établir de meilleures positions défensives. En outre, il est impératif que les activités de routine et de services de TI d'entreprise soient pleinement intégrées aux activités de la cyberforce afin d'assurer l'efficacité des cyberopérations et de réduire le potentiel de cyberdommages collatéraux.

2.5.1 Compétences des cyberopérateurs

L'École d'électronique et des communications des Forces canadiennes (EECFC) à Kingston, en Ontario, est l'école désignée pour l'instruction du groupe professionnel des cyberopérateurs. Les cyberopérateurs certifiés affectés au CORFC participent à un programme de formation en cours d'emploi (FCE) complété par des cours spécialisés fournis par l'industrie et adaptés au rôle et à la progression de la personne.

Les cyberopérateurs sont formés et entraînés à l'art de la cyberguerre, et plus particulièrement à ce qui suit :

a. La nature du cyberespace et du cyberdomaine;

b. Les menaces, les acteurs de la menace et leur incidence sur le cyberespace;

[10] Site Web de carrières des Forces armées canadiennes – Aperçu du cyberopérateur, https://forces.ca/fr/carriere/cyber-operateur/

c. Les principes et techniques de détection, de reconnaissance, d'identification et d'attribution de toutes les natures des entités cybernétiques;

d. Les principes et techniques des opérations cybernétiques offensives, y compris les mesures de cyberexploitation, la cyberattaque et les cyberfeux;

e. Les principes et techniques des opérations cybernétiques défensives, y compris les mesures défensives internes et les mesures d'intervention (MI);

f. Les tactiques, techniques et procédures pour :

   i. La coordination, le commandement et le contrôle du soutien cybernétique;

   ii. La cyberreconnaissance;

   iii. La cybersurveillance;

   iv. La criminalistique cybernétique;

   v. L'analyse de la cybermenace;

   vi. Les fonctions du centre des opérations de cybersécurité.

2.5.2 **Rôles du cyberopérateur (niveaux 1, 2 et 3)**

2.5.2.1 **Analyste subalterne**

Le rôle principal d'un cyberopérateur de niveau 1 est de travailler au sein d'un centre d'opérations de cyberdéfense pour détecter et suivre les activités des entités cybernétiques dans la zone d'opérations cybernétiques assignée en vue de classer les entités comme suit : humaines ou non humaines, amies, ennemies ou autres. Au besoin, un cyberopérateur de niveau 1 peut être chargé de participer à des tâches liées à la cyberreconnaissance, à la cybersurveillance, à la criminalistique cybernétique, au renseignement sur les cybermenaces, aux mesures relatives à la cyberexploitation ou aux cyberattaques, aux cyberfeux et aux cybercontre-mesures. Au besoin, le cyberopérateur de niveau 1 peut être chargé d'appuyer la conception, la mise au point et la mise en œuvre de TTP et de cyberoutils nouveaux ou améliorés pour des tâches liées à la cyberreconnaissance, à la cybersurveillance, à la criminalistique cybernétique, au renseignement sur les cybermenaces, aux mesures relatives à la cyberexploitation ou aux cyberattaques, aux cyberfeux et aux cybercontre-mesures.

2.5.2.2 **Analyste intermédiaire**

Le rôle principal d'un cyberopérateur de niveau 2 est de travailler au sein d'un centre d'opérations de cyberdéfense afin d'obtenir une caractérisation précise des cyberentités détectées par tout acte ou moyen, de manière à pouvoir prendre des décisions en temps réel et en toute confiance, y compris l'engagement d'armes. Au besoin, un cyberopérateur de niveau 2 peut être chargé de participer à des tâches liées à la cyberreconnaissance, à la cybersurveillance, à la criminalistique cybernétique, au renseignement sur les cybermenaces, aux mesures relatives à la cyberexploitation ou aux cyberattaques, aux cyberfeux et aux cybercontre-mesures. Au besoin, le cyberopérateur de niveau 2 peut être chargé d'appuyer la conception, la mise au point et la mise en œuvre de TTP et de cyberoutils nouveaux ou améliorés pour des tâches liées à la cyberreconnaissance, à la cybersurveillance, à la criminalistique cybernétique, au renseignement

Ébauche

sur les cybermenaces, aux mesures relatives à la cyberexploitation ou aux cyberattaques, aux cyberfeux et aux cybercontre-mesures.

2.5.2.3 **Analyste principal**

Le rôle principal d'un cyberopérateur de niveau 3 est de travailler au sein d'un centre d'opérations de cyberdéfense pour guider et diriger les actions des cyberopérateurs de niveau 1 et de niveau 2 afin de compléter l'analyse de la situation cyberopérationnelle par une recommandation concernant les mesures appropriées en cas de cyberexploitation ou de cyberattaque, les cyberfeux et les cybercontre-mesures. Au besoin, le cyberopérateur de niveau 3 peut être chargé de planifier, de diriger et d'exécuter des tâches détaillées liées à la cyberreconnaissance, à la cybersurveillance, à la criminalistique cybernétique, au renseignement sur les cybermenaces, aux mesures relatives à la cyberexploitation ou aux cyberattaques, aux cyberfeux et aux cybercontre-mesures. Au besoin, le cyberopérateur de niveau 3 peut être chargé de concevoir, de mettre au point et de mettre en œuvre des TTP et des cyberoutils nouveaux ou améliorés pour des tâches liées à la cyberreconnaissance, à la cybersurveillance, à la criminalistique cybernétique, au renseignement sur les cybermenaces, aux mesures relatives à la cyberexploitation ou aux cyberattaques, aux cyberfeux et aux cybercontre-mesures.

2.5.3 **Exercices d'instruction collective**

De façon générale, le GOIFC et le CORFC en particulier ont exercé un rôle de mentor dans les activités cybernétiques d'instruction collective. Même si toutes les possibilités d'instruction ne sont pas énumérées dans le présent document, on peut affirmer que l'instruction joue un rôle décisif dans les possibilités d'exercices cybernétiques :

a. UNIFIED RESOLVE;
b. VILGILANT SHIELD;
c. ENTERPRISE CHALLENGE;
d. FABRIC SABRE;
e. STEADFAST COBALT;
f. COALITION WARRIOR;
g. CYBER COALITION;
h. UNIFIED VISION.

Il convient de noter que la principale lacune/le principal obstacle à la réalisation d'une instruction individuelle et collective est l'absence d'un environnement d'instruction virtuel aux niveaux II et III.

Ébauche

3 JUSTIFICATION ET NATURE DU CHANGEMENT

3.1 Facteurs de changement

Afin de fournir des pratiques exemplaires en matière de sécurité des réseaux, telles qu'elles sont décrites par le Centre canadien pour la cybersécurité, le MDN et les FAC doivent commencer par comprendre la composition du réseau et disposer d'une solide capacité à en découvrir les actifs. Les analystes du CORFC travaillent actuellement avec de nombreuses trousses d'outils. Ils doivent surveiller de nombreuses consoles pour être informés des nouvelles alertes, divers portails de services de renseignement sur les menaces afin d'obtenir des données sur les entités en cause, ainsi qu'un éventail d'outils de détection et de réponse installés aux points d'extrémité pour comprendre ce qui se passe lorsque ces derniers sont touchés. Le CORFC utilise des outils de flux de travail pour contrôler les processus de triage et d'enquête; ce travail exige souvent que l'analyste copie et colle (espace d'air) des données d'un outil à un autre, qu'il remplisse des formulaires et soumette des demandes de recherche ou qu'il téléverse des artéfacts aux fins d'analyse et d'entreposage. La CD-DAR permet d'automatiser bon nombre de ces tâches, de simplifier les processus et d'assurer une qualité et une cohérence reproductibles, même si les processus demeurent essentiellement les mêmes. L'élimination partielle ou complète de ce type de processus manuel répétitif aura une incidence directe sur la productivité des analystes de la cybersécurité. Ceux-ci pourront alors consacrer plus de temps à des problèmes plus épineux et prioritaires qui exigent une expertise humaine.

De plus, on sait que les systèmes de surveillance de la sécurité génèrent un grand nombre d'alertes pour la plupart considérées comme de « faux résultats positifs » (ou tout simplement non pertinentes) après une enquête plus poussée. Le triage des alertes est actuellement effectué manuellement par les analystes qui peuvent commettre des erreurs. Le MDN et les FAC font face à des menaces de plus en plus agressives, comme des rançongiciels[11], où l'intervention efficace se mesure en secondes. Ce scénario oblige les organisations à réduire le temps qu'il leur faut pour réagir à ces incidents, habituellement en déléguant plus de tâches à des machines. La réduction du délai d'intervention, y compris le confinement des incidents et les mesures correctives, est l'un des moyens les plus efficaces de maîtriser les répercussions des incidents de sécurité. La CD-DAR fournira automatiquement un contexte aux alertes et ajoutera des renseignements clés pour permettre un triage manuel automatisé ou, à tout le moins, plus facile et plus rapide.

Le CORFC tirera parti de la CD-DAR pour réduire le temps nécessaire à la formation de nouveaux analystes de la cybersécurité. L'automatisation élimine la nécessité pour les analystes de connaître les détails des étapes manuelles à suivre pour chaque scénario. Les connaissances sont stockées et gérées dans la solution CD-DAR, ce qui réduira le besoin pour l'analyste de mémoriser le déroulement du processus et de le répéter constamment. Les analystes peuvent extraire des détails précis pour de nombreux scénarios, si le besoin se présente. Comme les solutions CD-DAR combineront la fonctionnalité des outils existants et des nouveaux outils et fourniront une ICSO intégrée, il ne sera plus aussi nécessaire de former chaque analyste de la sécurité pour chacun des outils.

[11] Le rançongiciel est un programme informatique malveillant conçu pour bloquer l'accès à un système informatique jusqu'à ce qu'une somme d'argent soit payée.

Il est connu que le nombre de cyberévénements et d'alertes de sécurité surpasse facilement le nombre de membres du personnel du cyberdomaine ayant les connaissances et l'expérience nécessaires pour enquêter sur ces événements afin de protéger l'intégrité du réseau informatique. Par conséquent, le MDN a de plus en plus de mal à demeurer à jour dans ce domaine en constante évolution. Qui plus est, les capacités de cyberdéfense inefficaces et désuètes font en sorte que la sécurité et la défense du MDN et des FAC demeurent vulnérables aux cybermenaces sans cesse grandissantes, ce qui augmente considérablement le risque pour les missions et les opérations.

3.2 Description des changements souhaités

Le MDN et les FAC ont besoin d'un système de cybersécurité complet pour répondre aux demandes des cyberopérations défensives dans un cyberespace contesté, et maintenir l'efficacité organisationnelle et opérationnelle. Ils comptent sur des outils autonomes et des processus manuels désuets en matière de cyberdéfense qui ne permettent pas de répondre pleinement aux cybermenaces de plus en plus nombreuses et diversifiées. En l'absence de solution CD-DAR intégrée, le MDN et les FAC verront leur capacité à défendre leurs réseaux de commandement et contrôle se dégrader, ce qui aura une incidence négative sur les capacités opérationnelles et pourrait avoir une incidence sur la sécurité et la sûreté du Canada et des Canadiens au pays et à l'étranger.

Les commandants et les opérateurs du MDN et des FAC ont besoin d'un système de cyberdéfense intégré leur permettant de prendre connaissance de la situation cybernétique et de répondre aux menaces hostiles et systématiques d'États-nations, de syndicats du crime organisé et de groupes terroristes.

Le projet de CD-DAR se définit par les lacunes en matière de capacités, c'est-à-dire les insuffisances ou les manques, qui sont énumérés et décrits ci-dessous, avec des références aux exigences obligatoires de haut niveau (EOHN) (section 4.2) qui y répondront.

3.2.1 Découverte du réseau

Les failles logicielles et la configuration inadéquate des composants du système d'information sont des vulnérabilités importantes des systèmes d'information qui permettent l'exploitation du système. Le SANS Institute, un organisme respecté de recherche et de formation en sécurité de renommée mondiale, avec la participation de la National Security Agency (NSA) et d'autres organisations nationales et internationales des États-Unis (US), tient à jour un rapport sur les principaux contrôles de sécurité pour les systèmes d'information.

Les quatre principaux contrôles sont les suivants :

a. Liste des appareils autorisés et non autorisés;

b. Liste des logiciels autorisés et non autorisés;

c. Configuration sécurisée du matériel et des logiciels sur les appareils mobiles, les blocs-notes, les postes de travail et les serveurs;

d. Évaluation continue de la vulnérabilité et restauration.

Afin de protéger un réseau, il doit y avoir un inventaire complet – et les interconnexions respectives – de tous les dispositifs matériels du réseau, comme les serveurs, les routeurs, les

commutateurs, les passerelles et les logiciels, y compris les versions ou les correctifs les plus récents qui se trouvent sur le réseau spécifié. À l'heure actuelle, la surveillance du réseau et la découverte d'appareils sont limitées pour le MDN et les FAC. Des plateformes permettant d'effectuer la découverte de réseaux sont mises à l'essai et utilisées de façon ponctuelle, couvrant des parties des réseaux du MDN et des FAC, mais pas le réseau complet. Le CORFC est appelé à intervenir en cas d'incidents concernant des systèmes non liés à l'entreprise dont il n'a pas connaissance, où 50 à 60 p. 100 des informations disponibles doivent être validées, et pour lesquels les demandes de changement sont soit dépassées, soit indisponibles. Des logiciels comme Nessus, Cyber Information and Incident Sharing System (CIICS) et Malware Information Sharing Platform (MISP)[12] se sont révélés capables de fournir une solution, mais ne sont pas utilisés de façon cohérente. La solution CD-DAR permettra de trouver les meilleures réponses possibles, d'assurer l'interopérabilité des plateformes de découverte de réseau et de couvrir toute la gamme des capacités de conception de produits. Bien que certains renseignements soient actuellement disponibles, la CD-DAR offrira un répertoire commun et exploitable. **Les lacunes en matière de capacité cernées dans la section « Découverte du réseau » sont corrigées par les EOHN 1, 7 et 8 (section 4.2).**

3.2.2 **Dépôt de cyberdonnées fiable**

Le MDN et les FAC ont besoin d'un dépôt de cyberdonnées (CDR) fiable qui agit comme entrepôt pour les cyberentités autorisées et les données d'événements relatif à leur cyberespace. Un CDR conserve toutes les données liées à la collection de toutes les cyberentités présentes dans le cyberespace du MDN et des FAC en plus d'une description de la relation entre ces entités en vue d'analyses des liens, d'analyses de vulnérabilités, de détection des intrusions, d'analyses criminalistiques, de collection, d'analyses de journaux et d'autres données provenant des réseaux de l'organisation, et d'autres tâches relatives à la cybersécurité. La base de données comprend une automatisation importante, ainsi que tous les outils de production de rapport sur les normes de l'industrie, de requête et d'analyse graphique.

La Cellule de renseignement sur les cybermenaces fournit des renseignements proactifs et réactifs pour améliorer les opérations de cyberdéfense. Pour effectuer une analyse, elle doit obtenir des données et des informations de différents systèmes et sources d'information ayant des niveaux de sécurité différents (de SANS CLASSIFICATION à TRÈS SECRET) ou comportant des mises en garde. Actuellement, le Centre national de transfert de données au sein de l'État-major interarmées stratégique (EMIS) a la capacité de transférer des informations vers et depuis 29 réseaux différents pour l'ensemble du MDN et des FAC. Cependant, comme il ne s'agit pas d'une capacité cybernétique, ces informations demeurent inaccessibles pour la CD-DAR et la manière dont elles sont stockées et transférées à des fins de renseignement cybernétique est limitée. Par conséquent, le CDR doit également recueillir, stocker et maintenir toutes les sources et les renseignements cybernétiques de sources ouvertes et de services

[12] Nessus est un outil de balayage des vulnérabilités exclusif élaboré par Tenable Network Security; Cyber Information and Incident Coordination System (CIICS) est une application Web qui permet aux nations de partager des renseignements de cyberdéfense au sein d'une communauté fiable nommée NATO CIICS Federation. La plateforme de partage des menaces, Malware Information Sharing Platform (MISP), est un logiciel gratuit et de source ouverte qui facilite l'échange d'information et des renseignements sur les menaces, y compris les indicateurs de cybersécurité.

Protégé

gouvernementaux, alliés, militaires et contractuels, tout en fournissant une vue d'ensemble complète, exacte et à jour des menaces autant de nature cybernétique que non liée au cyberdomaine du MDN et des FAC.

Le CDR regroupe les renseignements à partir des outils et des produits existants qui ne sont pas interopérables et permet une corrélation globale pour les différentes activités liées à la cyberdéfense. Le composant est aussi la base pour produire une capacité de COD interopérable modulaire, souple et agile. Un dépôt central permettra aux commandants de prendre des décisions éclairées sur les mesures défensives à prendre. **Les lacunes en matière de capacité cernées dans la section « Dépôt de cyberdonnées fiable » sont corrigées par les EOHN 1, 2, 3, 4 et 6 (section 4.2).**

3.2.3 **Image commune de la situation opérationnelle (ICSO)**

Compte tenu de la complexité des environnements opérationnels modernes, il existe un besoin continu en matière de connaissance de la situation, de partage de l'information et de collaboration en temps réel, satisfait au moyen d'une capacité de gestion de l'espace de bataille cybernétique, plus connue sous le nom d'ICSO cybernétique. Une ICSO est une représentation visuelle interactive, partagée et dynamique des informations opérationnelles recueillies auprès de diverses sources qui peut être adaptée pour faciliter la connaissance de la situation, la planification en collaboration et l'aide à la prise de décisions. En outre, une capacité de gestion de l'espace de bataille cybernétique doit permettre aux commandants de repérer, de surveiller, de caractériser et de suivre une activité du cyberdomaine qui a lieu à la fois au niveau mondial et dans les ZResp, et d'intervenir en réaction à cette action.

Les capacités actuelles du MDN et des FAC ne disposent pas d'un point de vue central pour représenter l'état de l'environnement cybernétique ou pour évaluer les répercussions des cyberactivités. Ces capacités sont insuffisamment intégrées, moins réactives et considérées comme inadéquates pour ce qui est de fournir de l'information opérationnelle à l'appui des processus décisionnels efficaces du commandement. Une ICSO doit être souple et adaptée aux besoins de chaque commandant ou état-major, qu'ils soient stratégiques, opérationnels ou tactiques. Le CORFC utilise actuellement un logiciel interne sans aucune marge de manœuvre dans les points de vue opérationnels pour regrouper l'information destinée au commandant. De plus, cet outil est inefficace pour les réseaux déconnectés, intermittents et peu fiables, ou qui offrent des environnements ayant une capacité limitée (épisodiques). Par conséquent, la solution CD-DAR devra maintenir une connaissance de la situation, au moyen d'une ICSO, des alertes, des menaces et des mesures correctives dans l'ensemble du réseau de commandement du MDN et des FAC. Elle devra également alimenter la connaissance de la situation dans les processus de décision et d'exécution des interventions par des interfaces normalisées et des flux de travail automatisés à l'appui du soutien à la décision de l'élément de commandement, et la mise en œuvre des interventions selon les directives. **Les lacunes en matière de capacité cernées dans la section « Image commune de la situation opérationnelle » sont corrigées par les EOHN 1, 2, 4 et 6 (section 4.2).**

3.2.4 **Facteurs humains**

La solution CD-DAR abordera deux aspects particuliers des facteurs humains. Le premier est qu'une trop grande spécialisation est requise de la part des analystes de la cybersécurité, et le deuxième est la surcharge cognitive de ces derniers. La solution CD-DAR fournira une solution

intégrée de cyberdéfense qui allégera le fardeau de comparer manuellement l'information d'un outil à celle d'un autre. Cela réduira les connaissances détaillées et la spécialisation nécessaires pour maîtriser les divers outils de cyberdéfense. En outre, l'automatisation de la collecte, de l'analyse et de la corrélation des données et des informations relatives à la sécurité des réseaux provenant de multiples sources d'information (GC et alliés) permettra de réduire la surcharge cognitive des cyberopérateurs puisque le nombre de détections et d'identifications manuelles des menaces sera réduit. Les alertes de sécurité seront automatiquement classées par ordre de priorité avec des recommandations sur la façon de remédier aux menaces. La solution CD-DAR fera appel à des analyses de sécurité avancées qui vont bien au-delà des approches fondées sur la signature actuellement utilisées. Les technologies d'apprentissage automatique seront mises à profit pour évaluer les événements dans l'ensemble du réseau de commandement, détecter les menaces et prévoir l'évolution d'attaques, ce qui serait impossible à réaliser de façon manuelle. Ces analyses de sécurité seront conservées dans le CDR afin de permettre le partage au sein de la communauté de cybersécurité et elles comprennent :

a. des renseignements intégrés sur les menaces qui ciblent les mauvais acteurs connus en tirant parti des renseignements sur les menaces mondiales;

b. une analyse comportementale qui applique des modèles connus pour découvrir des comportements malveillants;

c. la détection d'anomalies au moyen du profilage statistique pour établir une base de référence historique afin de fournir des alertes sur les écarts par rapport aux bases de référence établies qui sont conformes aux vecteurs d'attaque potentiels.

Les lacunes en matière de capacité cernées dans la section « Facteurs humains » sont corrigées par les EOHN 2, 3, 5, 6, 8 et 9 (section 4.2).

3.2.5 Capacité de mener des enquêtes judiciaires

La section de la criminalistique fournit des services d'analyse numérique spécialisés au MDN et aux FAC. Elle fournit également une analyse technique des cybermenaces et des techniques de logiciels malveillants utilisés par les adversaires pour pénétrer dans le cyberdomaine du MDN et des FAC. En plus de l'analyse des logiciels malveillants, elle est chargée de tenir à jour les événements de cybersécurité et de collaborer avec d'autres organismes. À l'heure actuelle, lorsqu'une fuite de données se produit, l'enlèvement physique et le remplacement du matériel peuvent coûter des milliers, voire des millions de dollars au MDN et aux FAC. Grâce au projet de CD-DAR comme solution de rechange au remplacement du matériel physique, l'image d'un disque dur touché pourrait être envoyée à distance à un environnement de bac à sable[13] où la section de la criminalistique pourra faire des analyses et des enquêtes tout en permettant d'effacer le disque dur. Lorsque l'équipement est situé dans différentes régions géographiques et qu'il n'y a pas d'expertise d'analyse disponible sur place, les disques durs et autres équipements doivent être expédiés à une installation locale aux fins d'analyse. Ces disques peuvent être

[13] Dans le domaine de la sécurité informatique, un « bac à sable » est un mécanisme de sécurité qui permet de séparer les programmes en cours d'exécution, habituellement dans le but d'atténuer les défaillances du système ou les vulnérabilités du logiciel, sans risquer de nuire à la machine hôte ou au système d'exploitation.

endommagés au cours de l'expédition, ce qui peut entraîner des retards supplémentaires ou empêcher la mise en place d'une procédure appropriée et l'examen de preuves potentielles. La solution CD-DAR permet d'effectuer des analyses judiciaires immédiates et à distance, sans avoir à expédier l'équipement à travers le pays. Ainsi, le MDN et les FAC réaliseront des économies de temps et d'argent, tout en limitant les répercussions sur les opérations en cours. **Les lacunes en matière de capacité cernées dans la section « Capacité de mener des enquêtes judiciaires » sont corrigées par les EOHN 2, 3, 4, 5, 6 et 9 (section 4.2).**

3.3 Priorités parmi les changements

Dans le cadre de la *Politique sur la sécurité du gouvernement* du Conseil du Trésor, le GC intensifie ses efforts pour lutter contre les cybermenaces. Les divers ministères coopèrent et coordonnent leurs efforts, et le MDN et les FAC continueront de participer activement, notamment par le biais du projet de CD-DAR.

Le projet de CD-DAR va dans le sens de l'initiative nº 65 de PSE : « […] adopterons une posture plus délibérée dans le cyberdomaine en renforçant nos défenses et en menant des cyberopérations actives contre d'éventuels adversaires dans le contexte de missions militaires autorisées par le gouvernement. » Le projet de CD-DAR permettra de respecter cet engagement de PSE en fournissant des cybercapacités à l'appui des opérations militaires et en protégeant les réseaux et équipements militaires essentiels contre les cyberincidents. La nouvelle capacité remplacera notamment les processus manuels actuels et les multiples systèmes non intégrés par une solution intégrée, modulaire et évolutive qui assurera l'interopérabilité avec les autres ministères et les alliés. Elle sera composée de matériel, de logiciels et de processus opérationnels associés.

En outre, le projet de CD-DAR s'harmonise avec le cadre de cybersécurité complet et bien défini du National Institute of Standards and Technology (NIST), qui fournit une orientation et un ensemble de normes pour les mesures de sécurité recommandées concernant les systèmes d'information des organismes fédéraux. Les normes du NIST reposent sur les pratiques exemplaires tirées de divers documents, organisations et publications en matière de sécurité; elles sont conçues comme un cadre pour les organismes et programmes fédéraux nécessitant des mesures de sécurité strictes.

En plus de l'initiative nº 65 de PSE, le projet de CD-DAR s'aligne stratégiquement et est appuyé par les éléments suivants :

a. Applique le cadre des résultats ministériels (CRM) 4.6.1 du Gp GI sur les cyberprogrammes, afin de disposer de capacités de COD entièrement opérationnelles et interopérables à l'appui des opérations des FAC aux niveaux stratégique et opérationnel;

b. S'aligne sur la vision stratégique, les buts et les objectifs en matière de C4ISR puisque ce projet contribuera à sécuriser et à défendre le cyberespace pour les FAC;

c. Suit le guide de planification fonctionnelle de la GI/TI de la Défense, en particulier l'objectif selon lequel le ministère investit dans une technologie permettant de cerner rapidement les vulnérabilités et les menaces à la sécurité des TI et d'y remédier.

Ébauche

4 APERÇU DE LA SOLUTION CD-DAR

4.1 Objectifs opérationnels (résultats opérationnels)

La solution CD-DAR apportera un changement fondamental à la cybersécurité et à la cyberdéfense du MDN et des FAC en mettant en œuvre la capacité d'intervention complète en cas d'événements de cybersécurité complexes et en évolution. Elle répondra aux besoins immédiats et à long terme, tout en maintenant et en permettant l'application des exigences en matière de cybersécurité et de cyberdéfense. La solution CD-DAR permettra à la force cybernétique du MDN et des FAC de :

a. Communiquer aux intervenants participant aux cyberopérations le processus à suivre pour la saisie, l'analyse et l'atténuation des cybermenaces;

b. Déterminer l'efficacité globale des cyberopérations en intégrant rapidement la connaissance de la situation, la compréhension et les interventions dans les opérations des réseaux et les activités des cyberopérations;

c. Mettre en œuvre des systèmes de collecte efficaces permettant de saisir les flux de réseau et les incidents relatifs à la sécurité dans l'ensemble de l'infrastructure de réseau visée;

d. Acquérir une capacité de gestion de l'espace de bataille cybernétique, communément nommée ICSO, intégrée à la CGIEB du MDN et des FAC qui combine la connaissance de la situation de tous les éléments de force des missions et des opérations des FAC;

e. Détecter rapidement les changements de vecteurs d'attaque allant de l'application aux attaques physiques;

f. Prioriser la disposition de la menace grâce à un moteur de cybersécurité centralisé offrant des fonctions de corrélation avancées, une identification des menaces en temps quasi réel et des capacités d'analyse avancées;

g. Établir une corrélation entre les alertes de capteurs asynchrones et les modèles de comportement;

h. Reconnaître les comportements anormaux en temps réel;

i. Utiliser habilement des outils avancés d'aide à la décision autonome, avec l'intelligence artificielle (IA), conçus pour fournir une orientation tactique plus rapide et plus précise pour atténuer les menaces;

j. Répondre rapidement à la menace, aux événements et aux incidents en s'appuyant sur des technologies d'automatisation et de coordination;

k. Mettre en place les processus et les ressources humaines appropriées pour faire face aux menaces;

l. Effectuer des recherches sur ces attaques et les partager avec des collègues, tant au niveau national qu'international;

m. Évaluer le rendement grâce à des informations significatives sur les paramètres et à des outils de mesure fondés sur les indicateurs de rendement clés (IRC) qui favorisent l'amélioration continue;

Ébauche

n. Veiller à ce que les leçons retenues soient saisies ou appliquées.

4.2 Exigences obligatoires de haut niveau

La solution CD-DAR fournira des cybercapacités défensives pour surveiller et défendre les réseaux du MDN et des FAC, ainsi que des capacités sous forme de matériel, de logiciels, de formation, etc. conformes aux exigences obligatoires de haut niveau (EOHN) qui comblent les lacunes existantes en matière de capacités. Les EOHN établies sont définies dans le tableau 4 ci-dessous.

Tableau 4 – EOHN du projet de CD-DAR

EOHN	Titre abrégé	Description
1	Biens cybernétiques (découverte du réseau)	Capacité d'identifier et de suivre rapidement tous les biens (autorisés et non autorisés) connectés au réseau de commandement et d'évaluer leurs attributs en matière de vulnérabilité, de configuration, de risque et de conformité aux correctifs.
2	Cyberanalyse	Capacité de recueillir, de conserver et d'analyser continuellement des renseignements sur les cybermenaces dans l'environnement du réseau de commandement et de détecter et de caractériser les activités suspectes, ainsi que de fournir un contexte pour les évaluations des risques et des vulnérabilités en temps quasi réel.
3	Intervention cybernétique	Capacité d'identifier, de contenir et d'éradiquer une menace de façon adaptative et dynamique.
4	Commandement et contrôle dans le cyberespace	Capacité de maintenir la connaissance de la situation, au moyen d'une image commune de la situation opérationnelle, des alertes, des menaces et des mesures correctives dans l'ensemble du réseau de commandement du MDN et des FAC, et alimenter la connaissance de la situation dans les processus de décision et d'exécution des interventions par des interfaces normalisées et des flux de travail automatisés à l'appui du soutien à la décision de l'élément de commandement, et la mise en œuvre des interventions selon les directives.
5	Intégration de la solution CD-DAR	Capacité d'être intégrée (hébergée et exploitée avec des applications et un dépôt fiable) au réseau de commandement assigné en tant que système cohésif.
6	Interopérabilité cybernétique	Capacité d'échanger de l'information sur les vecteurs de cybermenaces et les analyses pour répondre aux exigences internes en matière de compatibilité ainsi qu'aux systèmes et à l'environnement réseau désignés d'autres ministères (AM), de pays faisant partie du Groupe des cinq ou de l'Organisation du traité de l'Atlantique Nord (OTAN) et d'autres organisations externes.
7	Cyberrésilience	Capacité d'assurer une surveillance localisée de l'architecture de réseau, des biens et de l'information sur les menaces, de réaliser une analyse et de prendre des décisions en matière d'intervention

EOHN	Titre abrégé	Description
		dans des environnements déployés où la connectivité n'est pas disponible, n'est pas fiable ou a une capacité limitée.
8	Évolution et développement continus des cybercapacités	Capacité d'évoluer continuellement en tant que réponse au changement (menace, politique, technologie) de l'infrastructure de réseau du MDN et des FAC (la criminalistique à distance et le confinement/l'assainissement font partie de cette intervention) avec une incidence minimale sur les systèmes connectés ou la modification de l'infrastructure de TI sous-jacente, des normes de base et des politiques.
9	Souplesse cybernétique	Capacité d'adapter la solution CD-DAR, peu importe l'emplacement ou la durée des biens d'entreprise statiques ou employés à des fins opérationnelles.

4.3 Vue opérationnelle (VO-1)

Le MDN et les FAC visent à mettre en place une architecture de sécurité conçue de manière cohérente qui assure la confidentialité, l'intégrité et la disponibilité dans l'ensemble de l'organisation et qui harmonise les objectifs de la mission et les risques. La sécurité est un processus qui inclut les ressources humaines, la technologie et les opérations (processus). L'intégration de ces derniers nécessite une approche holistique qui permettra au MDN et aux FAC de mesurer leurs objectifs de sécurité à l'aide d'un modèle de maturité sur la sécurité. Le cadre de cybersécurité du NIST vise à définir, à protéger, à détecter, à réagir et à récupérer, afin de décrire et de développer l'architecture de sécurité et sa gouvernance, et d'aligner les contrôles de sécurité de l'assurance des informations (AI).

L'architecture de sécurité du MDN et des FAC fournira un moyen d'automatiser les pratiques exemplaires de la cybersécurité, notamment les contrôles de sécurité critiques du Center for Internet Security. Le cadre de cybersécurité est utilisé pour couvrir l'ensemble des objectifs liés à la cybersécurité, sans être trop détaillé. Il est essentiel qu'une architecture de sécurité maximise la connaissance du réseau afin de soutenir de façon efficace et efficiente la COD. Il s'agit notamment d'avoir une connaissance du réseau, des données et des paramètres; le choix des outils permettra de s'assurer que ces éléments sont suffisamment représentés.

Le MDN et les FAC, comme la plupart des grandes organisations, transforment les infrastructures existantes en y ajoutant de nouvelles initiatives comme l'informatique en nuage, l'analyse des mégadonnées, la mobilité et les applications de l'Internet des objets. Tous ces changements présentent un certain nombre de défis en matière de sécurité des réseaux. Le MDN et les FAC ont besoin d'une architecture de sécurité des réseaux interopérable et intégrée qui soit davantage axée sur les menaces, qui offre une certaine souplesse, qui automatise les processus manuels et qui remplace les outils de pointe par des services de sécurité des réseaux interopérables. L'architecture de sécurité du MDN et des FAC comprend le C2 centralisé par l'entremise du CORFC, la gestion des actifs, la détection et l'application réparties, le partage des informations, les renseignements utilisables et les services de restauration. Elle doit tenir compte de nombreux facteurs, notamment l'efficacité, la disponibilité, l'élasticité, la souplesse, la résilience, la variabilité et la capacité. L'architecture de sécurité devrait également permettre de remplacer les solutions pour que de nouvelles technologies soient mises en place, telles qu'une

Ébauche

plateforme de sécurité résiliente, l'intelligence artificielle et l'analyse basées sur l'informatique quantique, les données intelligentes en matière de sécurité, l'analyse cognitive/sensible de la sécurité et la cybersécurité offensive, dès qu'elles seront disponibles.

La vue opérationnelle 1 (VO-1) présentée à la figure 8, élaborée conformément au Cadre d'architecture du MDN et des Forces canadiennes (CAMDN), est un graphique du concept opérationnel général qui met en évidence les principaux aspects de l'architecture de CD-DAR et fournit une description des influences internes et externes.

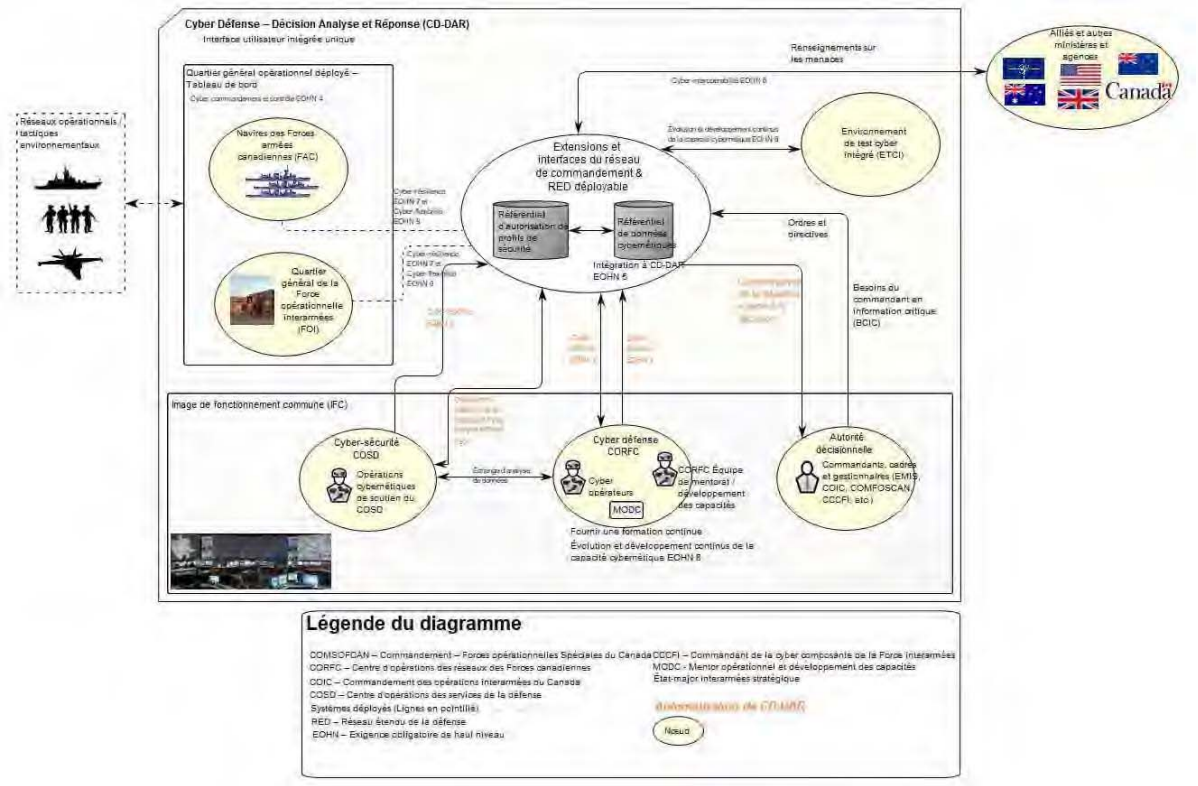


Figure 6 – Vue opérationnelle de haut niveau (VO-1)

L'objectif est de créer, d'équiper, d'organiser et de former un centre d'opérations en matière de cybersécurité capable de protéger les réseaux du MDN et des FAC dans l'environnement actuel, 24 heures sur 24, 7 jours sur 7, tout en offrant la formation initiale, la formation périodique, le perfectionnement professionnel et le mentorat des cyberopérateurs du MDN et des FAC qui appuieront les opérations de défense et de cybersécurité au pays et à l'étranger.

Selon le concept actuel des opérations, tous les cyberopérateurs et les autres utilisateurs (gestionnaires, cadres supérieurs, commandants et leurs états-majors) accomplissent leurs tâches dans un environnement intégré unique. Ces tâches comprennent, entre autres, le flux de travail, le suivi, l'analyse, les alertes, la production de rapports, la connaissance de la situation, les mesures d'intervention et l'instruction (individuelle et collective). Chaque cyberopérateur a accès à un outil de visualisation du tableau de bord commun, adapté à son rôle et à ses responsabilités particulières. Les membres du personnel comme les cadres supérieurs, les commandants, les gestionnaires et d'autres éléments des opérations du réseau du MDN et des FAC (comme la

Marine royale canadienne [MRC], l'Aviation royale canadienne [ARC], l'Armée canadienne [AC], le Commandement des opérations interarmées du Canada [COIC], le Commandement des Forces d'opérations spéciales du Canada [COMFOSCAN] et l'État-major interarmées stratégique [EMIS]) auraient également les droits et privilèges pour accéder à l'information et mener des actions en fonction des rôles qui leur sont attribués dans le cadre de la COD du MDN et des FAC. Il est fort probable qu'ils aient accès aux informations liées à la cyberdéfense grâce à la CGIEB, qui intègre tous les aspects d'une opération. Dans le but de remplacer les frégates de la classe HALIFAX parfois chargées d'exploiter le quartier général de la Force opérationnelle interarmées (QG FOI), la MRC fait actuellement l'acquisition du navire de combat de surface canadien qui sera équipé d'une capacité de CD-DAR afin de surveiller et de défendre ses propres réseaux ainsi que ceux des forces déployées relevant du QG FOI maritime. Des précisions seront présentées pendant la phase de définition du projet de CD-DAR.

Parmi les autres éléments principaux de cette vue opérationnelle de haut niveau (VO-1), mentionnons :

a. **Renseignements partagés sur les menaces :** Les renseignements sur les menaces sont une forme d'information importante ayant une influence sur la position du MDN et des FAC en matière de sécurité et de défense et sur celle de leurs partenaires;

b. **Données autorisées :** La capacité à reconnaître les renseignements acceptables dans le cyberespace du MDN et des FAC est essentielle pour détecter les situations inacceptables et y réagir. Par exemple, la définition des dispositifs autorisés doit être établie avant que des dispositifs non autorisés puissent être détectés et gérés;

c. **Automatisation :** Un des principaux objectifs de la solution CD-DAR est de favoriser au maximum l'automatisation du dispositif de sécurité et de défense du MDN et des FAC. Un effort opérationnel important sera nécessaire pour numériser les renseignements partagés sur les menaces provenant de multiples partenaires, les informations étant reçues sous divers formats manuels et lisibles par machine.

4.3.1 Environnement opérationnel, interopérabilité, souplesse et résilience

La solution CD-DAR fournira des capacités de cybersécurité et de cyberdéfense partout où les extensions et les interfaces du réseau de commandement et les systèmes du RED déployés sont accessibles. Cela a une incidence sur les environnements suivants :

a. **Environnement durable** : Cela comprend les emplacements au pays et à l'étranger lorsqu'il y a une gamme complète d'infrastructures de soutien disponibles, ainsi qu'une connectivité complète aux réseaux et systèmes de soutien. L'environnement opérationnel est robuste et fiable;

b. **Environnement épisodique** : Cela concerne tous les lieux de mission où l'infrastructure variera de robuste à limitée, et la disponibilité variera de fiable à non fiable. Ces conditions ajoutent des exigences de fonctionnement dans des situations déconnectées, intermittentes et à faible bande passante (limitée) et de reprise après de telles situations. Les environnements déconnectés, intermittents et limités requièrent un traitement autonome local, de nouveaux canaux de communication et une capacité à se rétablir sans problème lorsque la connexion est rétablie;

Ébauche

c. **Environnement de collaboration** : Comme la plupart des missions du MDN et des FAC sont menées dans des environnements de systèmes et parties multiples, les capacités de CD-DAR doivent être interopérables avec les réseaux et systèmes gérés par le MDN, les autres ministères et organismes, les alliés et d'autres partenaires internationaux. La solution CD-DAR tiendra également compte de la nécessité de traiter l'information dans divers domaines de sécurité et mises en garde;

d. **Cyberenvironnement** : Les faiblesses peuvent être exploitées et les répercussions liées à ces exploitations peuvent atteindre les réseaux qui nécessitent une réactivité maximale. Pour ce faire, on optimise habituellement l'automatisation des capacités de surveillance, de détection, d'analyse, de prise de décisions et d'intervention, ainsi que l'inclusion de processus et de systèmes souples pour s'adapter à un environnement de menace en évolution rapide.

Le cyberdomaine nécessite un ensemble solide et cohérent d'outils, de ressources et de capacités pour permettre au MDN et aux FAC de remplir leur mandat et de fonctionner efficacement dans un cyberdomaine contesté.

4.3.2 État-major de la cybersécurité et de la cyberdéfense

L'état-major de la cybersécurité et de la cyberdéfense du MDN et des FAC, qui se trouve surtout au CORFC, devrait être organisé en fonction des analystes de la sécurité, des scientifiques des données, des développeurs d'outils et des chasseurs de menaces. Les analystes de la sécurité travaillent à l'échelle interministérielle pour repérer et corriger les failles dans les systèmes, les solutions et les programmes de sécurité du MDN et des FAC, tout en recommandant des mesures précises qui peuvent améliorer la sécurité globale. Les spécialistes des données font appel à l'analyse des données, aux tests statistiques, à l'exploration des données et à l'IA – apprentissage machine/apprentissage profond (ML/DL) – pour interpréter des données volumineuses. Les développeurs d'outils créent des tableaux de bord personnalisés pour améliorer la connaissance de la situation cybernétique, des adaptateurs pour intégrer et convertir des données non structurées en données structurées, ainsi que des scénarios pour automatiser les tâches et opérations courantes et améliorer l'efficacité. Les chasseurs de menaces utilisent l'analyse d'hypothèses concurrentes (ACH) pour effectuer des recherches proactives et itératives dans les réseaux et les ensembles de données afin de détecter les menaces pouvant déjouer l'infrastructure de sécurité existante.

Apprentissage machine

« Processus par lequel une unité fonctionnelle améliore ses performances en acquérant de nouvelles connaissances ou aptitudes ou en réorganisant les connaissances ou les aptitudes dont elle dispose déjà. »

Banque de terminologie de la Défense, Fiche n° 21880

Ébauche

4.4 Modèle opérationnel de CD-DAR

La solution CD-DAR permettra au MDN et aux FAC de mener des opérations de cybersécurité et donnera au CORFC/COSD la capacité de fournir une connaissance de la situation cybernétique, de défendre les environnements de réseau du MDN et des FAC et de mener des COD. À cette fin, bien que plusieurs outils intégrés pour la cybersécurité soient nécessaires pour satisfaire aux exigences de la CD-DAR, les principaux éléments fonctionnels recherchés peuvent être regroupés comme suit :

Apprentissage profond

« L'apprentissage profond est une fonction de l'IA qui imite le fonctionnement du cerveau humain en traitant les données pour les utiliser dans la détection d'objets, la reconnaissance de la parole, la traduction de langues et la prise de décisions. Cette technologie est en mesure d'apprendre sans supervision humaine, à partir de données non structurées et non étiquetées. » [Traduction]

Investopedia, 24 nov. 2020

a. Capacité de maintenir la connaissance de la situation cybernétique, au moyen d'une ICSO cybernétique, des alertes, des menaces et des mesures correctives dans l'ensemble du réseau de commandement du MDN et des FAC, et d'alimenter la connaissance de la situation dans les processus de décision et d'exécution des interventions par des interfaces normalisées et des flux de travail automatisés à l'appui du soutien à la décision de l'élément de commandement, et la mise en œuvre des interventions selon les directives.

   Une ICSO doit être souple et adaptée aux besoins de chaque commandant, qu'ils soient stratégiques, opérationnels ou tactiques. Elle offre une marge de manœuvre aux vues opérationnelles pour consolider les informations destinées aux commandants. Elle fonctionne également sur des réseaux qui sont indisponibles, peu fiables, fournissant une connaissance de la situation cybernétique locale, ou qui ont une capacité limitée (épisodique);

b. Capacité de créer et de tenir à jour un dépôt des cyberdonnées (CDR) faisant autorité qui comprend des données de renseignements cybernétiques provenant de plusieurs sources à intégrer (hébergées et exploitées avec des applications et un dépôt fiable) dans le réseau de commandement désigné en tant que système cohésif. Le CDR comprendra également des ensembles de données provenant de diverses sources, permettant l'analyse d'un ensemble diversifié de données, y compris l'accès aux journaux du réseau pouvant être enrichis par des sources de données, notamment des données provenant de la GSTI/du COSD, de la base de données de gestion des configurations (BDGC), de SPC, de la Sécurité publique, des guides de mise en œuvre technique de la sécurité (GMOTS), de la configuration de base et d'autres sources d'exploitation du réseau;

c. Capacité d'effectuer une recherche automatisée ou sur demande de cyberentités et d'événements (CEED) afin de repérer et de suivre rapidement tous les biens (autorisés et non autorisés) connectés au réseau de commandement et d'évaluer leurs attributs en matière de vulnérabilité, de configuration, de risque et de conformité aux correctifs;

Ébauche

d. Capacité d'effectuer une surveillance automatisée de la cybersécurité afin de repérer rapidement la présence de cyberentités ou de comportements non conformes, d'événements, d'alertes, de vulnérabilités ou d'autres changements apportés à l'état des entités dans le cyberespace du MDN et des FAC;

e. Capacité d'effectuer les activités essentielles liées à la sécurité comme la gestion des biens, l'évaluation des vulnérabilités, le contrôle de documents, la gestion de la configuration et les fonctions du changement de configuration telles que l'évaluation de la sécurité et le processus d'autorisation;

f. Capacité de recueillir, de conserver et d'analyser continuellement des renseignements sur les cybermenaces dans l'environnement du réseau de commandement et de détecter et de caractériser les activités suspectes, ainsi que de fournir un contexte pour les évaluations des risques et des vulnérabilités en temps quasi réel;

g. Capacité d'effectuer la gestion automatisée des tâches (GT) pour identifier, contenir et éradiquer une menace de façon adaptative et dynamique;

h. Capacité d'utiliser un système intégré d'instruction opérationnelle. Les cyberopérateurs, les gestionnaires, les cadres supérieurs et les autres opérateurs sont formés et maîtrisent les tâches, les rôles et les responsabilités au sein du système intégré; cela inclut :

   i. une capacité de créer une simulation de menace, de pénétration et d'attaque opérationnelle pour exercer l'équipe de cyberopérateurs et évaluer leur état de préparation opérationnelle ainsi que leur efficacité;

   ii. une instruction axée sur les opérateurs individuels (tâches, rôles et avancement dans leur rôle);

   iii. une instruction axée sur les compétences et la validation des cyberopérateurs, opérateurs et civils dans le rôle qui leur est attribué autant au niveau individuel que collectif;

   iv. une instruction collective pour une capacité d'opération de défense et de cybersécurité. Ceci est une réplique d'un ensemble de systèmes d'exploitation avec des ensembles de données hors ligne pour permettre une gamme complète de fonctions et de scénarios réalistes à des fins de formation.

4.4.1 **Image commune de la situation opérationnelle (ICSO) cybernétique**

L'ICSO est l'interface principale que les cyberopérateurs, les gestionnaires, les cadres supérieurs et les commandants utiliseront pour exploiter la capacité de CD-DAR. Pour accéder à la CD-DAR, il faut d'abord obtenir des justificatifs d'identité vérifiés. Une fois les justificatifs d'identité vérifiés, les utilisateurs disposeront d'une représentation visuelle partagée, dynamique et interactive des renseignements opérationnels cybernétiques recueillis auprès de diverses sources, qui pourra être adaptée à leurs rôles et besoins respectifs afin de faciliter la connaissance de la situation, la planification commune et la prise de décision. L'ICSO permettra aux utilisateurs de détecter, d'analyser et de surveiller les cybermenaces; de produire des rapports; d'envoyer des notifications et d'en recevoir de la part d'autres ministères, des alliés et de tiers partenaires; de gérer les menaces, les événements et les incidents; et d'exécuter les interventions. Elle fournit également une connaissance de la situation concernant les biens, leur sécurité et

Ébauche

l'état de connectivité. Leur état inclut la capacité de repérer les cyberentités autorisées et non autorisées.

Le niveau de sécurité des environnements cybernétiques peut être superposé ou inclus dans l'ICSO des missions ou des réseaux, ce qui permet d'accéder à la représentation détaillée de la situation en matière de cybersécurité. L'ICSO fournit ce qui suit :

a. Des tableaux de bord personnalisables – plateformes basées sur les rôles;

b. Une capacité d'analyses temporelles pour détecter les menaces et les changements apportés à l'environnement au fil du temps;

c. Une capacité de transmettre des informations fusionnées et des renseignements exploitables vers le bas, y compris sur le plan tactique;

d. Une capacité de transmettre des informations fusionnées afin d'améliorer la prise de décision et de fournir des informations sur l'état des réseaux adverses;

e. Une capacité de mettre à jour la politique de sécurité et les renseignements sur les menaces en fonction des attaques détectées sur le réseau, afin de pouvoir protéger les systèmes contre les TTP des adversaires.

4.4.1.1 **Connaissance de la situation**

Pour améliorer la connaissance de la situation en matière de sécurité, les meilleures organisations ont recours à la cyberdéfense active en temps réel, c'est-à-dire que le personnel joue un rôle concret et actif pour repérer et contrer les menaces qui pèsent sur les systèmes. La cyberdéfense active vise à assurer la détection, la compréhension, la prise de décision et l'intervention en temps utile afin d'assurer la défense du cyberespace avant que l'adversaire ne soit en mesure d'atteindre son objectif. À l'inverse, une défense passive consiste à ajouter des logiciels ou du matériel au système dans le but de renforcer la sécurité, sans que le personnel intervienne systématiquement. On parle également de cyberdéfense proactive plutôt que réactive, et les bonnes organisations de sécurité pratiquent les deux. La cyberdéfense active fait appel à l'analyse de données volumineuses, à la science des données, à l'apprentissage machine et profond, à l'IA et à de nombreux autres processus et technologies. Ces fonctions de sécurité seront centralisées au centre opérationnel de cybersécurité du MDN et des FAC, qui assure la défense contre les activités non autorisées au sein du réseau de commandement, y compris les activités de surveillance, de détection, d'analyse, d'intervention et de rétablissement.

4.4.2 **Orchestration et automatisation de la sécurité et intervention (OASI)**

Une plateforme d'orchestration et automatisation de la sécurité et intervention (OASI) est utilisée pour effectuer la répartition des tâches, la gestion des bons et des flux de travail associés au contrôle, au suivi et à la gestion du travail et des priorités, ainsi qu'au cycle de vie des incidents et des opérations de sécurité. Utilisée par les cyberopérateurs et les gestionnaires appropriés au moyen de l'ICSO, l'OASI remplit les fonctions suivantes :

a. Fournir un accès unifié à la fonctionnalité fournie par la solution CD-DAR;

b. **Orchestration** – Comment les différentes technologies (propres ou non à la sécurité) sont intégrées pour fonctionner ensemble :

Ébauche

i. Organiser les tâches en fonction des pouvoirs, des niveaux d'expertise et des préférences de travail des cyberopérateurs, des commandants, du personnel de soutien et des autres rôles participants;

ii. Permettre l'exécution simultanée de tâches par le personnel autorisé;

c. **Automatisation** – Comment faire en sorte que les machines effectuent un « travail humain » axé sur les tâches. Soutenir et promouvoir l'utilisation la plus appropriée des tâches manuelles, lancées par l'utilisateur et lancées par l'ordinateur pour maximiser la productivité de l'utilisateur;

d. **Gestion d'un incident et collaboration** – Gestion complète d'un incident par des personnes. Permettre un accès et une exécution autorisés et simultanés des tâches au niveau local, national et international, y compris dans des lieux défavorisés;

e. **Tableaux de bord et rapports** – Visualisations et capacités de collecte et d'établissement de rapports sur les mesures et autres informations.

4.4.2.1 Mesures d'intervention

La dernière étape de toute cyberattaque consiste à limiter et à réparer les dommages et à mettre fin à l'intrusion. Il peut s'agir d'interventions manuelles (p. ex. restauration des données et des systèmes à partir d'un point de référence, reconfiguration du pare-feu, des listes blanches, des listes noires) ou d'interventions automatisées (p. ex. l'arrêt d'un service ou d'un lien réseau à l'aide de scénarios préparés, d'outils de gestion de réseau traditionnels ou de mise en réseau définie par logiciel [SDN] avancée). Le palier de décision récupère les mesures prises précédemment pour des anomalies similaires et le système présente des options. À mesure que le système est exploité, la bibliothèque de codes pour les interventions automatisées et semi-automatisées qui ont été préprogrammées (c.-à-d., intervention humaine) sera élargie, en particulier lorsque le SDN sera adopté. Le palier d'intervention constituera une bibliothèque de scénarios (guides opérationnels) ayant une incidence sur la décision.

4.4.2.2 Gestion des interventions en cas d'incident

Les gestionnaires des interventions en cas d'incident doivent être en mesure d'établir un ordre de priorité et de se concentrer sur les incidents critiques auxquels les équipes sont confrontées chaque jour. Ils doivent aider à coordonner et à informer les équipes interdisciplinaires dont font partie des membres d'autres organisations d'intervenants. Lorsqu'un incident se transforme en crise, l'équipe d'intervention doit être en mesure de répondre rapidement aux questions avec précision tout en se concentrant sur la résolution du problème. En outre, elle doit être capable de produire des rapports complets et des fonctions d'analyse qui transforment les données en informations exploitables afin d'apporter des réponses et d'améliorer les processus. Elle a besoin de capacités telles que les suivantes, sans s'y limiter :

a. Des caractéristiques chronologiques qui fournissent une vision élaborée, souple et personnalisable des tâches en suspens et des tâches achevées, ce qui donne un excellent aperçu de l'état d'avancement, qui peut à son tour être utilisé pour favoriser la responsabilisation;

b. Des tableaux de bord personnalisables pour fournir des moyens graphiques d'accéder aux données, de les visualiser et de les convertir en informations exploitables;

c. Des tableaux de bord analytiques présentant des mesures basées sur les répercussions à l'échelle de l'organisation – ils aident les organisations à mesurer l'incidence des opérations de sécurité sur l'atténuation des risques ou l'amélioration des situations de sécurité.

Une plateforme d'intervention en cas d'incident permet de résoudre des problèmes liés aux interventions tels que :

a. Comprendre les menaces internes et externes;

b. Élaborer un plan d'intervention en cas d'incident normalisé, documenté et reproductible;

c. Tester et améliorer de manière proactive les processus d'intervention en cas d'incident;

d. Mettre à profit le renseignement sur les menaces;

e. Simplifier l'enquête, le triage et les interventions en cas d'incident, y compris le maintien de la chaîne de possession légale pour récupérer les données;

f. Gérer et suivre l'état de tout incident en temps réel, y compris les incidents majeurs, afin de rendre compte et d'informer le commandant, les groupes intéressés et les tierces parties de la situation la plus récente;

g. Coordonner et automatiser les interventions en cas d'incident parmi les ressources humaines, les processus et les technologies utilisant plusieurs systèmes ou comptes;

h. Intégrer l'évaluation dynamique des risques et la gestion des risques dans le processus;

i. Protéger contre les changements non autorisés de la liste blanche, l'installation non autorisée de logiciels et le blocage de l'exécution non autorisée de logiciels par le dispositif;

j. Documenter la manière de corriger une vulnérabilité;

k. Installer automatiquement les correctifs pour tous les produits et systèmes;

l. Gérer les événements relatifs à la sécurité afin de permettre l'accès en fonction de l'autorisation de niveau de confiance, de l'accès aux installations, de l'accès au niveau du système grâce aux principales exigences d'autorisation d'instruction et de justificatifs d'identité, et de la correction des lacunes liées au comportement relatif à la sécurité par le biais de contrôles de sécurité automatisés;

m. Pour les conditions de sécurité des dossiers, appliquer les types de dossiers précisés et protéger la confidentialité, l'intégrité et l'authenticité des données au repos, en transit ou en cours de traitement par cryptographie;

n. Pour les activités anormales, fournir une capacité de détection et d'intervention des points d'extrémités (DIPE) pour réagir à l'installation de logiciels malveillants sous forme de menace persistante avancée (MPA) sur un dispositif de point d'extrémité;

o. Les mesures d'intervention seront signalées sur une base normalisée, personnalisée, programmée, à la demande et en fonction des événements. Des informations sur le

Ébauche

moment où les menaces ont été détectées pour la première fois et le temps nécessaire pour y remédier seront fournies en conséquence.

Les principales caractéristiques d'une plateforme d'intervention en cas d'incidence sont les suivantes : fournir des plans d'action pour aider à orchestrer les solutions à l'aide de flux de travail, et fournir des guides opérationnels permettant d'automatiser les interventions.

4.4.2.3 **Mise en place de politiques automatisées**

La solution CD-DAR apprend à reconnaître le comportement normal des systèmes du MDN et des FAC et établit ou met à jour automatiquement des politiques de sécurité lorsqu'elle découvre un comportement anormal jamais détecté auparavant. L'opérateur peut choisir de diffuser les politiques à certains ou à tous les agents dispersés qui pourront alors prendre les mesures appropriées, y compris la sécurité des points d'extrémité locaux ou l'application des normes de sécurité à l'échelle du réseau.

4.4.2.4 **Guides opérationnels dynamiques sur les cyberopérations défensives**

Les guides opérationnels précisent et automatisent les étapes détaillées, l'orientation ou les pratiques exemplaires pour traiter les résultats, tout en assurant une expérience cohérente entre les équipes. La solution CD-DAR comprendra un ensemble prédéfini de guides opérationnels qui pourront être partagés entre les autres ministères et les partenaires alliés; elle permettra également de personnaliser les guides opérationnels existants ou d'en créer de nouveaux. Ces guides opérationnels peuvent s'adapter aux conditions des incidents en temps réel afin de suivre la complexité et la sophistication en constante évolution des MPA ou des TTP de l'adversaire.

Les guides opérationnels dynamiques de COD permettent un niveau d'intervention en cas d'incident allant bien au-delà de celui des guides opérationnels statiques traditionnelles. Elles coordonnent les ressources humaines et les processus, en plus d'automatiser la technologie lorsque cela s'avère utile afin de renforcer les capacités des analystes de la cybersécurité et de les rendre plus rapides, plus efficaces et plus performants. Les guides opérationnels dynamiques de COD permettent de réduire le délai moyen de résolution des problèmes sans sacrifier l'exactitude.

À mesure qu'un incident évolue, la solution CD-DAR réévalue le plan d'intervention, enrichit automatiquement les données et ajoute ou supprime des tâches pour veiller à ce que le plan soit adapté à la situation. Grâce aux guides opérationnels dynamiques, elle peut modifier automatiquement le plan d'intervention en fonction des renseignements sur les menaces et de la reclassification de l'incident.

Lorsqu'un analyste ouvre un incident, les étapes initiales répétitives de triage, d'affectation et d'enrichissement de manière intelligente ont déjà été réalisées. Les guides opérationnels dynamiques récupèrent automatiquement les informations des systèmes connectés, puis les utilisent pour changer la propriété, enrichir les éléments et fournir aux analystes des données pertinentes au moment où ils en ont besoin.

4.4.2.5 **Éditeur visuel de guides opérationnels**

Les analystes de la cybersécurité sont des experts connaissant les processus de leur organisation basés sur les données et les renseignements, ainsi que les mesures à prendre. L'éditeur visuel de guides opérationnels (EVGO) fournit des assistants faciles à utiliser permettant aux analystes de

créer ou de personnaliser des guides opérationnels de COD en fonction des processus quotidiens axés sur les données, afin de créer des analyses prescriptives pouvant automatiser des décisions fondées sur des preuves et de coordonner des plans d'action automatisés dans l'écosystème cybernétique de l'organisation. L'EVGO permet aux développeurs et aux personnes qui ne le sont pas de créer et de personnaliser facilement des scénarios de COD complexes en utilisant la fonction « glisser-déposer »; l'EVGO génère automatiquement les codes nécessaires en temps réel.

4.4.3 **Instruction opérationnelle**

L'instruction opérationnelle en matière de CD-DAR sera un élément important d'instruction et d'intégration des nouveaux utilisateurs de la solution CD-DAR. L'objectif n'est pas de générer de nouveaux cyberopérateurs, mais plutôt de former ces derniers afin qu'ils puissent utiliser efficacement la solution CD-DAR pour accomplir les missions et les opérations de COD du MDN et des FAC. Puisque la fonction de CD-DAR est basée sur les rôles, les commandants, les cadres supérieurs et les gestionnaires acquerront les connaissances nécessaires quant à son utilisation selon leurs rôles et responsabilités en matière de COD. L'instruction opérationnelle périodique en matière de CD-DAR sera incluse dans le programme d'instruction des cyberopérateurs. Voir le paragraphe 4.7.2.4 pour les détails concernant l'environnement d'instruction.

Au départ, un stagiaire sera exposé à des scénarios simples avec un nombre limité de données à observer et de mesures à prendre, mais au fur et à mesure qu'il acquerra de l'expertise, le système d'instruction pourra augmenter la granularité des données et des mesures en conséquence. Inciter l'utilisateur à suivre des formations plus souvent, à acquérir continuellement de nouvelles compétences, quel que soit son niveau actuel, et à améliorer sa capacité d'observation, d'orientation, de décision et d'action (OODA) pour qu'elle soit plus rapide que celle de l'attaquant est un véritable défi.

4.4.4 **Surveillance de la cybersécurité**

La solution CD-DAR permettra de surveiller en permanence le réseau afin d'identifier la présence de cyberentités, d'événements, d'alertes, de vulnérabilités ou d'autres changements à l'état des cyberentités qui sont non conformes dans le cyberespace du MDN et des FAC.

Les activités essentielles liées à la sécurité (p. ex. la gestion des biens, l'évaluation des vulnérabilités, le contrôle des documents, la gestion de la configuration et les fonctions de gestion des changements, comme le processus d'évaluation et d'autorisation de la sécurité) sont réalisées par l'intermédiaire de la solution CD-DAR. Dans le cadre de la surveillance de la cybersécurité, les cinq (5) premiers contrôles de la sécurité critique (CSC) du centre de sécurité Internet (CSI) seront mis en œuvre grâce aux interactions avec le CDR. Ces CSC minimums essentiels sont les suivants :

a. Liste des appareils autorisés et non autorisés;
b. Liste des logiciels autorisés et non autorisés;
c. Configuration sécurisée des appareils d'utilisateurs finaux;
d. Évaluation continue de la vulnérabilité et restauration;
e. Utilisation contrôlée des privilèges administratifs.

La solution CD-DAR automatisera, dans la mesure du possible, la détection et l'identification des menaces, la conduite des analyses nécessaires pour déterminer le type de menace, le développement et la recommandation du meilleur plan d'action pour soutenir les décisions des commandants et le choix des mesures proportionnelles pour faire face à cette menace. Ce cycle d'élaboration des interventions en cas d'incident cybernétique est présenté en détail dans la figure 7 ci-dessous. La solution CD-DAR signale également les modifications apportées à la ligne de base au personnel de COD et aide ce dernier à évaluer les changements et les anomalies du système.

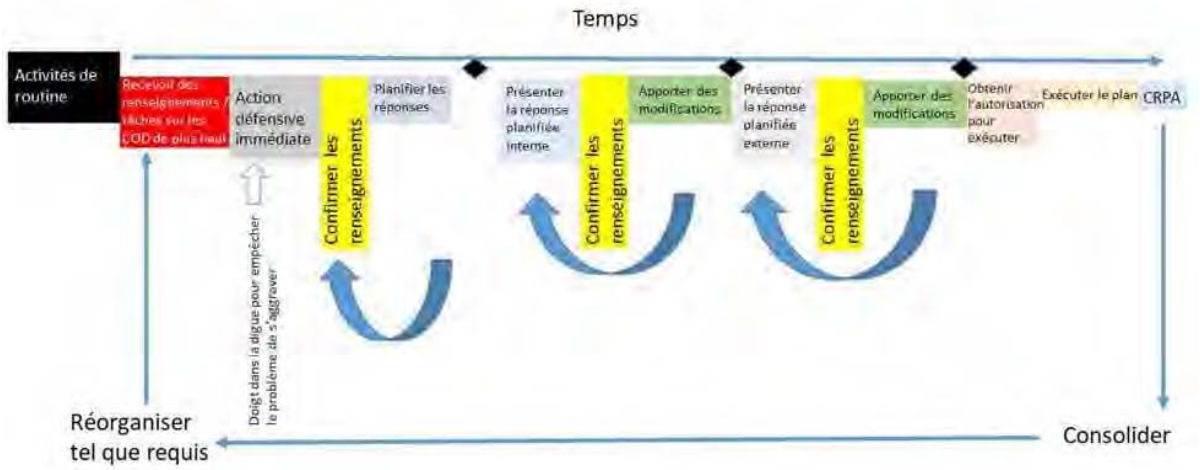


Figure 1 – Cycle d'élaboration des interventions en cas d'incident cybernétique

4.4.4.1 Apprentissage machine

La surveillance de la cybersécurité permet notamment de proposer des plans d'action pour les contre-mesures en fonction de la menace analysée. Les données sur les événements ou les anomalies sont présentées aux cyberanalystes afin qu'ils les analysent et prennent des mesures correctives. L'apprentissage machine peut être intégrée de deux manières : la détection et l'intervention. Dans le cas de la détection, les anomalies peuvent être liées à un comportement inhabituel ou à de véritables problèmes nécessitant une intervention. Les comportements jugés anormaux sans être malveillants sont utilisés pour mettre à jour la classification dans le moteur d'analyse de l'apprentissage machine qui est supervisé. Cela permet d'affiner la classification et de réduire le nombre de faux positifs, le terme « positif » désignant dans ce sens l'affirmation d'un comportement anormal. En conséquence, on encourage les utilisateurs à enregistrer les analyses qu'ils effectuent suite à une anomalie similaire (c'est-à-dire un rapport provenant de la même application analytique ou de la même liaison réseau, du même élément ou de la même application informatique) et les mesures qu'ils ont prises. Les analystes ou un système automatisé peuvent ensuite consulter les données enregistrées pour accélérer l'élaboration d'interventions futures.

Un moteur d'analyse de l'apprentissage machine apprend à reconnaître le comportement normal des systèmes au fil du temps et à corréler les événements provenant de divers domaines sensoriels pour établir une base de référence du système. L'apprentissage machine supervisé en continu est enrichi d'informations fournies par des opérateurs humains pour améliorer la précision du moteur.

4.4.4.2 **Gestion des biens**

La CD-DAR a besoin d'interfaces utilisateur et machine-machine pour consulter l'information dans la BDGC (intégrée dans le CDR si la BDGC du MDN et des FAC n'est pas encore prête lorsque la CD-DAR fournira ses capacités). Elle doit aussi pouvoir saisir des données dans la BDGC et récupérer de l'information pour l'utiliser dans d'autres applications et plateformes. La BDGC est « la source de mise en contexte » pour le réseau. Elle contient la liste de tous les composants matériels et logiciels autorisés ainsi que les configurations autorisées. La saisie des données se fait de façon manuelle et automatisée, le plus possible de façon automatisée à l'aide de moyens passifs et actifs dans le cadre de la découverte des biens. Les moyens actifs peuvent comprendre un agent qui utilise le système du client ou aucun agent. La méthode sans agent combine des analyses actives du système, des analyses authentifiées et non authentifiées et des analyses passives qui permettent de surveiller le trafic sur le réseau afin d'identifier les dispositifs et composants à l'aide d'analyses avancées, y compris l'apprentissage machine. Il se peut que certaines composantes de l'équipement existant soient trop fragiles ou ne prennent pas en charge les moyens actifs. Les renseignements comme le propriétaire du système et ses coordonnées, son emplacement, et la date de la dernière vérification sont des exemples d'attributs qui doivent être saisis manuellement. La CD-DAR doit aussi avoir l'option de contrôler manuellement le système ou d'entrer toute l'information qui est normalement entrée de manière automatisée. Par exemple, un commandant peut accepter le risque de dévier d'une configuration approuvée pour les impératifs opérationnels. Dans ce cas, la CD-DAR doit être capable de reconnaître la déviation comme une configuration autorisée pour le groupe en question afin d'éviter les fausses alertes ou d'empêcher le système de retourner automatiquement à la configuration originale.

4.4.4.3 **Gestion de la conformité**

Lorsque des contrôles de sécurité techniques sont en place, le cyberopérateur doit être capable de rendre compte rapidement de l'état de la conformité des groupes par rapport à toute norme de conformité, dans ses rapports quotidiens ou à la demande de vérificateur ou du directeur, à l'aide de la cyberimage commune de la situation opérationnelle. Cette fonction permettra à un officier de la sécurité de définir les écarts de conformité et de surveiller les mesures correctives qui sont prises.

4.4.4.4 **Gestion des vulnérabilités**

Les vulnérabilités des logiciels et des configurations peuvent être comparées aux guides de renforcement des configurations normalisées, comme les GMOTS et les points de repère du CSI, ce qui peut être fait automatiquement à l'aide d'analyseurs de vulnérabilités. Toutefois, ces analyseurs ne détectent pas les vulnérabilités matérielles ni les autres grandes classes de vulnérabilités (p. ex. les vulnérabilités se rattachant à l'architecture, aux personnes, aux relations de confiance).

Ébauche

Au chapitre de la gestion des vulnérabilités, les praticiens de la sécurité continuent d'avoir de la difficulté à déterminer lesquelles parmi les centaines et même les milliers de vulnérabilités dans leur réseau représentent un réel risque. Les méthodes traditionnelles ne tiennent pas compte de tous les facteurs de risque ni des autres mesures de sécurité d'atténuation dans l'établissement de l'ordre de priorité des risques. Les équipes de la sécurité comprennent donc mal la façon dont leur réseau et leur système d'impact des menaces risquent de gaspiller des ressources et des efforts à régler des problèmes que les pirates ne trouveront peut-être jamais ou ne chercheront pas à exploiter. Déroulement typique du travail en gestion des vulnérabilités : détection – établissement des priorités – prise de mesures correctives – suivi et surveillance.

Les capacités de gestion des vulnérabilités de la CD-DAR comprendront entre autres les fonctions suivantes :

a. Une console unique pour visualiser tout le profil de risque du cyberenvironnement, y compris les vulnérabilités et les vecteurs d'attaque potentiels dans un modèle visuel interactif;

b. Diminution des besoins de correctifs par la détection des menaces imminentes visant la mission;

c. Collaboration avec le COSD pour utiliser des solutions de correction efficaces, améliorer les techniques d'atténuation et de correction, et rendre compte de l'avancement ou de l'achèvement de l'application des correctifs;

d. Automatisation du suivi, de l'analyse et de la communication de l'avancement de l'évaluation des risques.

4.4.4.5 **Comportements attendus et inattendus des utilisateurs**

4.4.4.5.1 Gestion de l'identité et de l'accès

Le succès de la mission d'aujourd'hui dépend de la disponibilité en toute sécurité de ressources logicielles, notamment des applications, des données et d'autres services. Les processus et solutions de gestion de l'identité et de l'accès (GIA) constituent la première ligne de défense pour assurer un accès sécurisé aux services matériels et logiciels du réseau.

Une bonne solution de GIA doit comporter un contrôle d'accès basé sur les rôles (RBAC) et suivre le principe de droit d'accès minimal, mais peut aussi fournir une pleine gestion de l'identité (par exemple le modèle de Google), isoler, surveiller, enregistrer et contrôler des sessions privilégiées dans des systèmes critiques, des bases de données, des machines virtuelles, des conteneurs virtuels et autres.

La CD-DAR évaluera les comportements attendus et inattendus ainsi que les intrusions et prendra des mesures correctives, le tout en temps réel. Pour ce faire, elle apprendra les schèmes de comportement normaux de chaque réseau, dispositif ou utilisateur, mettra les données en corrélation pour déceler les déviations qui indiquent des menaces ou attaques en temps réel, et les mettra en quarantaine ou prendra des mesures correctives. Elle se servira du dernier renseignement classifié ou non sur les cybermenaces en conjonction avec l'apprentissage machine pour faire évoluer les modes d'attaque et les apprendre. Les extrants en temps réel serviront à éliminer les menaces avant que les adversaires n'atteignent leurs objectifs.

Ébauche

La détection comportementale de pointe se fait à l'aide d'analyses des mégadonnées sur des machines virtuelles avec des ressources de traitement évolutives en matière de puissance de calcul et de mémoire. Consultez le paragraphe 4.6.2 pour en savoir davantage sur les analyses des mégadonnées.

4.4.5 **Analyse de la cyberdéfense et prise en charge des décisions**

Il faut adopter une nouvelle approche novatrice en matière d'opérations de cyberdéfense, laquelle rattache la prévention des incidents de sécurité à la détection et à l'intervention, couvre les personnes, les processus et les éléments technologiques, est davantage centrée sur la pertinence opérationnelle, la réduction du temps de tenue des adversaires, le ralentissement de leur avancée, et l'accélération des activités d'intervention en cas d'incident. Cette approche doit créer un environnement plus dynamique qui permettra de mener méthodiquement et rapidement des enquêtes actives sur les intrusions en mettant continuellement à jour les contrôles de détection de sécurité à l'aide du nouveau renseignement sur les menaces (en provenance des autres ministères, des alliés et des partenaires de l'industrie) et en renforçant les recherches actives en temps réel à l'aide des recherches réalisées dans les données historiques pour déceler les intrusions.

L'objectif est d'unifier et d'intégrer une approche globale en matière de cybersécurité qui réduit considérablement l'exposition aux cyberrisques opérationnels. Cette approche permet une amélioration automatisée en continu des contrôles de sécurité et la mise en commun des procédures de recherche d'autres organisations et une automatisation partielle pour recueillir de l'information aux fins de contrôle humain, et, selon les besoins, l'approbation de la haute direction ou d'un commandant local.

Initialement, les cyberanalystes seront encore tenus au courant en ce qui concerne la prise de décisions et l'exécution des plans d'action. À mesure que s'amélioreront les technologies d'IA, les personnes seront mises au courant de la vérification et de la validation des analyses automatisées, de la prise de décisions (définition et sélection des plans d'action viables) et de l'exécution de la réaction. Les correctifs apportés à l'automatisation sont consignés et utilisés comme rétroaction pour accroître la précision et l'efficacité des COD. Ces correctifs aident les analyses de la sécurité à renforcer et même à automatiser leur compréhension d'une menace, ce qui leur permet de mieux comprendre les attaques les plus récentes et de se concentrer à d'autres priorités. La CD-DAR s'autorajustera continuellement pour réduire le nombre de faux positifs et de faux négatifs.

4.4.5.1 **Surveillance de la sécurité**

La CD-DAR appuiera la surveillance continue de la posture de sécurité du réseau, pour disposer d'un portrait clair de l'exposition aux risques liés à la sécurité au sein de l'organisation à l'aide d'un tableau de bord complet, des affichages présentant les paramètres de sécurité clés et axés sur l'incidence, les paramètres de rendement clés, les seuils statiques et dynamiques et les indicateurs de tendance.

Le moteur de surveillance de la sécurité permettra de recueillir et de relier rapidement une multitude de renseignements provenant de différents appareils dans le cyberenvironnement, par exemple les points d'extrémité, les périphériques réseau, etc., pour décider en fonction du risque s'il faut élever le niveau d'une alerte d'intérêt dans un incident, ce qui déclenchera le processus d'intervention en cas d'incident. Il permettra de mieux suivre les événements isolés qui ne

justifient pas nécessairement un examen approfondi, mais qui, lorsqu'ils sont examinés conjointement avec d'autres événements d'intérêt à l'aide d'analyses des mégadonnées, justifient peut-être une enquête plus poussée. Cela rend possibles la corrélation et l'analytique prédictive, notamment l'analyse comportementale de l'ensemble de la chaîne de cyberdestruction pour détecter et réduire les « faux négatifs », qui sont plus dommageables que les « faux positifs ».

4.4.5.2 **Recherche des cybermenaces**

La recherche des cybermenaces consiste en une recherche proactive et itérative dans les réseaux pour détecter et isoler les menaces qui échappent aux solutions de sécurité existante et persistent dans les réseaux. Les analystes de la recherche doivent utiliser les techniques manuelles ou assistées par ordinateur, contrairement aux détections automatisées des outils de sécurité comme la gestion des informations et des événements de sécurité (GIES). La recherche a deux buts principaux : 1) améliorer la détection et l'intervention automatisées en modélisant de nouvelles façons de détecter les activités malveillantes, puis en transformant ces modèles en détections et en interventions nouvelles et efficaces à l'aide d'organisation et d'automatisation, et 2) forcer les intrus dans les réseaux à rester absolument parfaits en tout temps pour persister dans les réseaux.

Une recherche efficace requiert des analystes possédant différentes compétences et expériences qui sont appliquées de façon systématique pour détecter les menaces malveillantes et malicieuses et les éliminer du réseau. Les chercheurs de menaces doivent adopter la pensée de l'attaquant, ce qui signifie qu'ils doivent savoir quoi chercher en fonction des étapes qu'ils suivraient s'ils étaient responsables de l'attaque. Par conséquent, les analystes de la recherche des menaces doivent être qualifiés en guerre offensive. Les chercheurs de menaces sont tenus de collaborer avec des intervenants qualifiés qui savent comment agir rapidement pour contenir une attaque.

Le résultat de la recherche est la création, la consignation et l'automatisation normale de procédures reproductibles ou des modèles.

4.4.5.3 **Détection des points d'extrémité et intervention**

La CD-DAR permettra aux COD d'assurer la visibilité complète des points d'extrémité, d'améliorer leur capacité de détecter les activités malveillantes et de simplifier les interventions en cas d'incident de sécurité. Les agents des points d'extrémité sont généralement intégrés dans les plateformes d'analyse des mégadonnées, du renseignement sur les menaces et de surveillance de la sécurité. Les agents des points d'extrémité appuient la capacité de recueillir les données télémétriques des points d'extrémité, comme les processus en exécution, les paramètres de registre, les fichiers actuellement ouverts, les connexions réseau actives, les détails matériels, comme l'unité centrale (CPU) et l'utilisation actuelle de la mémoire, et les comptes d'utilisateur actifs, etc. aux fins de traitement par analyse des mégadonnées. Les agents des points d'extrémité appuieront aussi les mesures d'intervention et la capacité de recueillir des données criminalistiques, comme des images ou fichiers sur mémoire ou disque dur, à l'appui des enquêtes criminalistiques.

4.4.5.4 **Renseignement sur les menaces**

Le renseignement sur les menaces (RM) se définit comme des connaissances fondées sur la preuve, par exemple le contexte, les mécanismes, les indicateurs, les répercussions et les conseils exploitables, concernant une menace ou un danger existant ou nouveau associé à des biens qui peuvent servir à des fins décisionnelles à l'égard de la réaction à cette menace ou à ce danger.

Les types qualitatifs de RM sont axés sur la prestation de services semblables à la distribution de nouvelles sur les campagnes, les outils, les techniques et les motivations des attaquants. Inversement, les sources quantitatives – les listes noires des domaines, les localisateurs de ressources uniformes (URL), les IP, les TTP, l'atténuation géoréférencée, le filtrage des protocoles par détection des anomalies, le retrait de paquets malformés, y compris les charges malicieuses et la limitation de débit (pour bien gérer les hausses radicales non malveillantes de la demande) – peuvent être utilisées en temps réel dans la surveillance des systèmes et aident à détecter et à bloquer l'activité liée à de mauvais sites connus.

Les diverses sources de RM comprennent des versions du gouvernement classifiées et non classifiées (p. ex. les Enhanced Cybersecurity Services [ECS] et l'Automated Indicator Sharing [AIS] du département de la Sécurité intérieure [DHS], Open Source, les fils commerciaux payants et le RM adapté en provenance de l'industrie).

Les cas d'utilisation suivants décrivent certaines façons dont la CD-DAR utilisera le renseignement sur les menaces :

a. **Renseignement organisé** – Transformer les données sur la menace en RM à l'aide du contexte et établir automatiquement l'ordre de priorité en fonction d'une cotation et d'une pertinence définies par l'utilisateur;

b. **Tendances en matière d'attaque** – Enquêter sur les attaques et assurer un suivi au fil du temps à l'aide des données pour améliorer la posture de défense du MDN et des FAC et les COD;

c. **Pivotement du renseignement** – Utiliser les connaissances sur les campagnes, les maliciels et les indicateurs pour reconnaître les attaques et adversaires s'y rattachant qui pourraient avoir une incidence sur les missions et les opérations;

d. **Enquêtes** – Appuyer l'établissement de la portée et les mesures correctives en mettant en corrélation les artefacts d'une enquête et une bibliothèque de menaces contenant des indicateurs et le contexte s'y rattachant;

e. **Recherche des menaces** – Permettre aux cyberopérateurs de chercher de façon proactive toute activité malveillante ou anormale qui n'a pas encore été repérée par les outils de sécurité automatisés du MDN et des FAC;

f. **Améliorer l'intervention en cas d'incident** – Avoir un accès mondial aux TTP des adversaires pour améliorer la qualité, la portée et la vitesse des mesures correctives;

g. **Renforcer les appareils de sécurité** – Rendre les outils de sécurité (p. ex. pare-feu, systèmes de détection d'intrusions [SDI], GIES, etc.), les capteurs et tout autre dispositif intelligent à l'aide de données exactes et pertinentes sur les menaces;

h. **Efficacité du RM** – Évaluer de façon rétrospective la précision, la vitesse et la pertinence de sources du RM comparativement à la pertinence de l'information qu'ils fournissent dans les incidents qui surviennent.

4.4.5.4.1 Renseignement externe sur les menaces

Le MDN et les FAC devraient utiliser des fils de type quantitatif proactif, p. ex. le Web caché, pour obtenir un renseignement très précieux sur les menaces, assez souvent utile pour une vaste

Ébauche

gamme d'objectifs potentiels, qu'il s'agisse d'organisation ou de personnes, autrement impossibles à obtenir à l'aide d'une surveillance conventionnelle.

La collecte et l'analyse du renseignement disponible sur le Web caché présentent une nouvelle occasion de comprendre et d'anticiper éventuellement les attaques. La CD-DAR peut utiliser ce type d'information pour quantifier le risque, et en définitive, déterminer quelles mesures les cyberanalystes devront peut-être prendre pour l'atténuer.

Le renseignement sur les menaces recueilli sur le Web caché ouvre une fenêtre sur les motivations, les méthodes et les tactiques des auteurs de menaces. Pour faire un usage optimal de ce renseignement, les COD devraient être avisées seulement lorsqu'une information nouvelle et pertinente est recueillie, et être en mesure de déterminer rapidement si ces développements nécessitent une enquête plus poussée ou une intensification pour orienter une prise de décision plus efficace.

4.4.5.5 **Évaluation des cyberrisques**

La CD-DAR utilisera la gestion dynamique des risques (GDR) pour recommander des mesures d'intervention individuelles ou des plans d'action complets, et évaluer leur efficacité, leurs coûts et leurs effets secondaires en ce qui concerne les objectifs de mission dans le cadre du flux opérationnel pour les interventions en cas d'incident. L'ajout de la GDR au flux opérationnel pour les incidents qui le nécessitent (c.-à-d. les incidents qui dépassent une certaine cote de risque) permettra de s'assurer que les mesures ou les plans d'action recommandés (y compris l'évaluation de leur efficacité, de leur coût et de leurs effets secondaires en ce qui concerne les objectifs de mission) sont traités avant que l'incident ne passe à la prochaine étape du processus d'intervention. La CD-DAR devra appuyer l'enrichissement automatisé des incidents à l'aide de toute information disponible sur l'évaluation dynamique des risques (EDR) pour mettre en contexte. Un cadre de travail souple permettra aux utilisateurs de diversifier leurs groupes d'actifs et d'identité pour que les besoins prioritaires puissent être placés dans ceux qui ont une plus grande incidence sur la mission en cas de compromission.

4.4.5.6 **Rétro-ingénierie des maliciels**

Les analystes de la sécurité effectuent une rétro-ingénierie des maliciels dans le but de comprendre leurs techniques d'exploitation, leurs techniques de brouillage, leurs méthodes de chiffrement, les communications de C2, l'attribution, la catégorisation et la mise en grappe, et bien d'autres. Les outils nécessaires pour appuyer les analystes seront intégrés dans le laboratoire de l'Environnement d'essai cyberintégré (EECI) (voir la section 4.7.2.3 pour obtenir des détails), et les exemples comprennent les suivants : saisie intégrale des paquets (saisie des paquets, appareils de sécurité, analyse des mégadonnées, etc.), signature et filtrage par motif, sources du renseignement sur les menaces, désassembleurs, émulateurs et virtualisation, fuzzing/exécution symbolique, et bacs à sable.

À l'avenir, plus d'approches axées sur l'IA feront appel aux coalitions de cybersécurité spécialisées, aux plateformes résilientes définies par la sécurité, aux données de sécurité intelligentes, aux objets intelligents de la cybersécurité et à l'analyse de sécurité cognitive/sensible.

ébauche

4.4.5.7 **Déni de service distribué**

La CD-DAR cherchera à fournir la capacité de répudier le trafic malveillant ciblant un groupe (humain ou non) avant qu'il ne passe par le réseau de transport, tout en permettant au trafic normal sur le réseau de faire passer le groupe visé et les autres utilisateurs/actifs sur le réseau, et à assurer ainsi la résilience du réseau qui permet au réseau et au groupe visé de fonctionner pendant la cyberattaque sans perte d'efficacité perceptible.

4.4.6 **Intégration de la CD-DAR**

L'architecture de sécurité du réseau de commandement se compose de nombreux outils et appareils de sécurité personnalisés et commerciaux que l'intégrateur de système principal (ISP) du projet de la CD-DAR devra intégrer dans les capacités de la CD-DAR. Ces outils seront indiqués à la phase de définition du projet, et pourraient comprendre des produits de la GIES, le renseignement sur les menaces, la recherche des menaces, les analystes de sécurité, l'explication de données/les mégadonnées, l'apprentissage machine, les outils d'analyse des maliciels, la saisie des paquets, le pipeline d'intégration continue/de déploiement continu (IC/DC), les opérations de développement de sécurité[14], le suivi et le signalement des incidents, la plateforme des opérations de sécurité et autres. Ces outils doivent fournir une architecture axée sur l'entraide qui fait appel à des normes protocolaires courantes comme STIX, TAXII et autres, mais qui appuie aussi les outils de création de scripts et l'automatisation. De plus, la CD-DAR aura besoin d'une capacité solide de suivi des incidents pour appuyer les exigences particulières de la défense en matière de réseau, par exemple :

a. Permettre une saisie d'information cohérente et complète dans l'ensemble des incidents pour chaque état des étapes du cycle de vie de l'incident, comme le triage, l'analyse, l'intervention, la conclusion et le signalement;

b. Consigner l'information structurée fournie par les analystes (catégorie de l'incident, heure de signalement), les données semi-structurées (utilisateurs et systèmes touchés) et l'information non structurée (exposé de l'analyste), ainsi que les notes horodatées;

c. Protéger les détails sensibles des constituants, et ainsi éviter de compromettre tout cas de menace interne ou d'ébruiter un incident prématurément ou aux mauvaises personnes;

d. Protéger les détails des cas même si la constitution générale est compromise;

e. Appuyer l'intensification et le contrôle d'accès fondé sur les rôles pour différentes sections au sein du CORFC/COSD;

f. Appuyer les tendances et les paramètres à long terme;

g. Incorporer des artefacts ou des indicateurs d'artefacts, comme des événements ou des échantillons de maliciels;

h. Utiliser la simulation pour mettre en pratique et déboguer le déroulement du travail et le processus d'intervention en cas d'incident dans le laboratoire de l'EECI qui

[14] Les opérations de développement de sécurité concernent l'inclusion des efforts et des pratiques exemplaires en matière de sécurité dans l'intégration et le déploiement en continu.

pourrait ne pas contenir de matériel de sécurité sans avoir une incidence sur la collecte de mesures et les rapports statistiques pour l'environnement de production.

4.4.7 **Dépôt de cyberdonnées (CDR)**

Le dépôt de cyberdonnées (CDR) est l'entrepôt pour les cyberentités autorisées et les données d'événements et les données évolutives à l'horizontale pour le cyberespace du MDN et des FAC. Il contient des données structurées et non structurées provenant de diverses sources existantes, p. ex. le MDN (GSTI/COSD, BDGC, GMOTS et d'autres sources d'exploitation des réseaux), les autres ministères (SPC, CSTC, Sécurité publique, etc.), les alliés (Groupe des cinq et les partenaires de l'OTAN) ou d'autres sources fiables, portant sur la collecte de toutes les cyberentités dans le cyberespace du MDN et des FAC, ainsi qu'une relation descriptive entre ces entités aux fins d'analyse des liens, d'analyse de vulnérabilité, de détection des intrusions, d'analyse criminalistique et d'autres tâches liées à la cybersécurité. La base de données comprend tous les outils normalisés de l'industrie pour la production de rapport, la recherche et l'analyse graphique.

Toutes les données et toute l'information sont normalisées en un modèle de données unifié et global fondé sur des normes, et mis à la disposition de toute application qui en a besoin. Les buts principaux du CDR sont de regrouper l'information provenant d'outils et de produits existants qui ne sont pas interopérables, et de permettre une meilleure corrélation globale pour les diverses activités de cyberdéfense. Il est aussi la composante centrale qui servira à l'établissement d'une capacité de COD modulaire, souple, agile et interopérable.

De plus, le CDR recueille, stocke et tient à jour un cyberrenseignement et un renseignement de toutes sources provenant de sources ouvertes, du gouvernement, des alliés, des forces armées et de services par abonnement dans le but de fournir un aperçu complet, exact et à jour des menaces visant le cyberdomaine du MDN et des FAC, qu'elles soient de nature cybernétique ou autre.

4.4.7.1 **Collecte des données**

La collecte de données ne devrait pas se faire en conformité avec les communications de contrôle. Les paquets devraient être saisis à l'aide d'un dispositif de saisie passive spécialisé, et en tirant profit des systèmes virtualisés. Cette méthode passive signifie que la CD-DAR n'ajouterait pas de latence aux communications et ne constituerait pas une autre surface d'attaque. L'échantillon de sources données comprend :

a. La couche de données du réseau, p. ex. paquets, flux, registres, divers SDI, etc.;

b. La couche de commande du réseau, p. ex. paquets, flux, registres, divers SDI, etc.;

c. La sécurité matérielle, p. ex. capteurs de sécurité matérielle, systèmes d'accès par carte, vidéo, audio, etc.;

d. La couche application, p. ex. indicateurs d'anomalie dans les données d'application des réseaux et de l'organisation, comme des sources de données image ou vidéo, etc.

4.4.8 **Cyberentités et découverte d'événements**

La CD-DAR établira et tiendra à jour un inventaire des cyberentités autoritaires et une base de données de configuration de toutes les cyberentités (matérielles et logicielles) dans le réseau de commandement. Ainsi, la CD-DAR doit avoir la capacité de découvrir, de recueillir et de stocker

Ébauche

toutes les données liées aux cyberentités et aux cyberévénements, et de les stocker dans le CDR. Ces données constitueront la base de référence avec laquelle la CD-DAR comparera les nouvelles cyberentités, qu'elles soient autorisées ou non, et pourra détecter les tentatives malveillantes d'infiltration des réseaux du MDN et des FAC. Ces tentatives d'intrusion peuvent provenir de pièces jointes à un courriel ou de petits dispositifs dotés de fonctions de connectivité. La CD-DAR doit être capable de se défendre contre ces attaques, d'identifier l'entité étrangère et de consigner l'événement au registre.

Les capacités de la CD-DAR permettront d'exécuter les analyses de découverte d'entités selon une routine prédéfinie, automatiquement lorsque les données d'une cyberentité sont modifiées, en réponse aux alertes données par les systèmes de surveillance, ou à la demande d'un cyberopérateur. Le système fera appel à ce qui suit : la collecte et la rétention de données brutes sur le trafic, le suivi du trafic du réseau et des détections d'événements en temps réel, le suivi de l'hôte et la détection d'événements en temps quasi réel, le suivi des activités et la détection d'événements en temps quasi réel. Le tout est appuyé par une saisie de l'ensemble des paquets à des points clés désignés dans le cyberespace du MDN et des FAC, dans la mesure du possible. Toute nouvelle cyberentité qui tente d'accéder au réseau de commandement sera consignée et analysée pour déterminer si elle représente une menace. Quant aux entités autorisées nouvellement consignées, elles feront l'objet d'un suivi continu dans le CDR et d'une surveillance visant à assurer la sécurité des opérations pour le réseau de commandement. Les capacités de la CD-DAR comprendront aussi un mécanisme d'exception pour accepter les changements légitimes mais hors norme aux biens de l'ITI dans l'intérêt de la prépondérance des besoins opérationnels des FAC.

Peu importe la source, les données faisant autorité seront numérisées de manière à permettre aux systèmes d'information de la CD-DAR de comparer automatiquement les données réelles et faisant autorité assez vite pour détecter les situations non autorisées dans les délais d'efficacité du système conformément à l'énoncé des besoins opérationnels (EBO) de la CD-DAR.

4.4.8.1 **Découverte des biens**

Pour que leurs COD soient efficaces, le MDN et les FAC doivent savoir qui et quoi sont connectés à ses environnements de réseau, y compris par le nuage et sur place, en tout temps.

La découverte des biens est réalisée de façon active et passive ainsi qu'en mettant à contribution les agents sur les clients dans la mesure du possible. Il se peut que ce ne soit pas possible ou pratique de placer un agent sur chaque client (p. ex. IDO ou dispositif hérité). La découverte des biens sans agent combine les analyses actives des systèmes, authentifiées et non authentifiées, et les analyses passives qui surveillent le trafic sur le réseau pour identifier les dispositifs et composants à l'aide d'analyses avancées, y compris l'apprentissage machine.

L'analyse passive fait appel à la collecte de données sFlow et NetFlow de tous les biens connectés ainsi que l'état de leur connectivité avec d'autres appareils dans l'environnement de réseau. Cette approche permet non seulement de reconnaître les biens connus, mais aussi les biens inconnus.

En plus de la découverte des biens, les adaptateurs seront utilisés pour recueillir de l'information sur le système aux fins de validation (conformité) du niveau de correctif de sécurité et de la configuration. Les analyseurs de vulnérabilité du réseau et des biens et les outils de configuration sécurisée seront utilisés pour gérer et surveiller l'état du réseau à mesure que des dispositifs

(matériels et logiciels) sont ajoutés ou retirés, ainsi que leur configuration sur le réseau, qui pourrait introduire des vecteurs d'attaque pour les adversaires.

La surveillance des biens axée sur les réseaux plutôt que les agents permet de veiller à ce que, lorsqu'ils se connectent au réseau, les biens soient identifiés et marqués. Les agents sur les appareils permettent la surveillance des changements de configuration et des violations des politiques qui ne peuvent être détectées à partir du réseau. La CD-DAR combinera ces approches pour fournir un point de vue global de tous les biens connectés au réseau et permettre d'agir rapidement s'il y a un bien indésirable ou mal configuré avant qu'ils n'exposent tout le réseau aux menaces.

4.5 Innovation

Cette section présente le concept et les technologies que le projet de la CD-DAR intégrera probablement dans les capacités ou considérera comme une évolution possible pendant la phase d'utilisation.

4.5.1 Mentorat opérationnel et développement de capacité (MODC)

Généralement, les systèmes de la GI/TI du MDN et des FAC sont entretenus à l'aide de l'acquittement des frais annuels d'entretien matériel et de licences de logiciels, comprenant parfois certains services techniques fournis par le DIIGI ou donnés en sous-traitance.

La CD-DAR est une capacité opérationnelle composée de personnes, de processus opérationnels (activités) et de technologie, tous aussi importants les uns que les autres. L'échec de l'un de ces composants pourrait entraîner des répercussions graves sur le succès de la mission. Par conséquent, le concept de Mentorat opérationnel et développement de capacité (MODC) est né. Il consiste en une petite équipe spécialisée de militaires, de fonctionnaires et de cyberopérateurs, ainsi que d'experts techniques contractuels installés dans les locaux de la capacité de fonctionnement. MODC prévoira et gérera l'entretien et l'évolution de la CD-DAR à titre de capacité en prenant les mesures suivantes :

a. Appuyer les opérations de cybersécurité en cours et les COD, au besoin;
b. Diriger et coordonner la modification ou la transformation opérationnelle des capacités de la CD-DAR en matière de cybersécurité de COD pour devenir une capacité opérationnelle de cybersécurité et de cyberdéfense de niveau de maturité 5 selon le NIST[15];
c. Encadrer les cyberopérateurs à tous les niveaux pour améliorer les compétences et renforcer les cyberopérations des FAC aux fins de maintien des compétences;
d. Appuyer l'établissement et la coordination de l'instruction individuelle et collective sur la cybersécurité et les COD;
e. Appuyer les exercices et l'expérimentation relatifs aux cyberopérations;
f. Entretenir et faire évoluer les outils logiciels cybernétiques et de l'ITI de la CD-DAR;

[15] National Institute of Standards and Technology (NIST), https://www.nist.gov/.

Ébauche

g. Intégrer les nouvelles technologies et les pratiques exemplaires.

L'équipe de MODC sera mise sur pied dès que sera atteinte la capacité opérationnelle initiale et durant la phase d'utilisation de la CD-DAR.

4.5.2 **Analyse des mégadonnées**

Le volume d'alertes de sécurité, de journaux et de paquets nécessaires pour mener à bien les missions des COD croît de façon exponentielle. La tâche de détection des activités anormales ou suspectes sur le réseau est devenue beaucoup plus difficile, plus particulière dans l'ensemble des multiples domaines de sécurité du MDN. Une analyse complexe et automatisée est requise pour gérer efficacement le volume élevé, la haute vitesse et la grande variété de sources de données. De plus, cette capacité pourrait remplacer ou renforcer l'outil coûteux de la GIES actuellement utilisé par le CORFC, car il pourrait offrir de meilleures capacités que la GIES.

Indicateurs de compromission et indicateurs d'attaque

La différence entre les indicateurs de compromission et les indicateurs d'attaque est la suivante : [traduction] « *les indicateurs de compromission sont les indicateurs traditionnels tactiques et techniques, souvent réactifs, communément utilisés pour la détection des menaces, tandis que les indicateurs d'attaque sont axés sur l'attribution et l'intention des auteurs de menace. Une autre façon de les conceptualiser est la prise en charge du QUOI (indicateurs de compromission) et du POURQUOI (indicateurs d'attaque) de la contextualisation de la menace* ».

Article de Ken Dunham,
Directeur principal, Renseignement technique sur les cybermenaces, OPTIV, 24 janvier 2019

Un principe fondamental de la réalisation d'une analyse des événements de cybersécurité est de s'assurer que les enregistrements de trafic qui pourraient être utiles dans un contexte de cybersécurité sont pris en considération, même lorsque cela pourrait nécessiter l'examen d'une grande quantité d'événements réseau. En consignant chaque action en temps réel, les indicateurs d'attaque montrent exactement comment un adversaire s'est infiltré dans l'environnement surveillé, a accédé aux fichiers, a éliminé les mots de passe, s'est déplacé latéralement dans le réseau et a éventuellement exfiltré des données. Les indicateurs d'attaque[16] représentent une position proactive dans laquelle les COD cherchent les signes annonciateurs d'une attaque, comme l'exécution de codes, la persistance, la furtivité, le C2 et le déplacement latéral dans un réseau. Les indicateurs de compromission comprennent les empreintes numériques, les domaines du C2 ou les adresses IP qui changent constamment. Comme les indicateurs de compromission sont des méthodes réactives de suivi de l'activité malveillante, il est fort probable que le réseau a déjà fait l'objet d'une intrusion lorsque celle-ci est enfin détectée. Par contre, les indicateurs d'attaque sont une série d'actions qu'un adversaire doit exécuter afin de réussir; ainsi, les indicateurs d'attaque se prêtent davantage à la découverte des TTP de l'adversaire. En surveillant ces grandes quantités de données, en réunissant les indicateurs et en les analysant, on peut déterminer comment un auteur de menace accède au

[16] « IoC and IoA: Indicators of Intelligence », article de Ken Dunham paru dans OPTIV, directeur principal, renseignement technique sur les cybermenaces, 24 janvier 2019.

réseau et déduire son intention. Par conséquent, aucune connaissance préalable des outils ou des maliciels (indicateurs de compromission) et aucun renseignement sur les menaces ne sont requis pour mettre fin à l'attaque pendant qu'elle est en cours. En fait, les indicateurs d'attaque peuvent détecter les attaques de maliciels sans fichier ou les attaques du jour zéro.

4.5.3 **Intelligence artificielle**

Les capacités de la CD-DAR feront appel à une analyse de sécurité avancée qui va bien au-delà des approches fondées sur la signature actuellement utilisées. Les technologies d'apprentissage machine et d'apprentissage profond seront utilisées pour évaluer les événements dans l'ensemble du réseau de commandement, détecter les menaces et prédire l'évolution des attaques, ce qui serait impossible avec les approches manuelles. Ces analyses de sécurité peuvent comprendre entre autres les suivantes :

a. Un renseignement intégré sur la menace qui cible les mauvais acteurs connus en tirant parti des renseignements sur les menaces mondiales;

b. Une analyse comportementale qui applique des modèles connus pour découvrir des comportements malveillants;

c. La détection d'anomalies au moyen du profilage statistique pour établir une base de référence historique afin de fournir des alertes sur les écarts par rapport aux bases de référence établies qui sont conformes aux vecteurs d'attaque potentiels.

4.5.3.1 **Réseau autorégénérant**[17]

L'autorégénération du réseau se produit lorsque des problèmes réseau se sont réglés sans intervention humaine, grâce à un outil d'automatisation du réseau qui détecte et règle les pannes, les échecs et les intrusions. L'autorégénération se produit généralement à l'aide d'une alerte de surveillance du réseau qui déclenche une mesure corrective donnée sur le réseau[18].

Les environnements complexes de réseau étendu (RE), comme le réseau de commandement, qui se trouve en de multiples endroits, permanents ou à l'occasion de déploiements, peuvent submerger les équipes de la TI. Dans ces environnements, même les systèmes de gestion centralisée peuvent être trop lents et trop lourds pour voir les besoins d'un grand nombre de cyberentités (matérielles, logicielles et humaines) et y répondre.

Le MDN et les FAC emploient un certain degré d'automatisation pour assurer des connexions fiables, entre autres à l'Infrastructure du réseau privé virtuel de la défense (IRPVD), surtout depuis le début de la pandémie de COVID-19. Cependant, il faut encore une équipe d'administrateurs et d'analystes des systèmes pour que le système fonctionne efficacement, et cette approche n'est ni évolutive ni durable.

Le MDN et les FAC ont besoin d'une solution qui peut détecter toute sorte d'anomalies et y répondre, partout sur le réseau de commandement, et qui nécessite plus qu'une simple

---

[17] Nirav Shah, « Using AIOps to Enable Self-Healing SD-WAN », NetworkWorld, 8 décembre 2020, https://www.networkworld.com/article/3600139/using-aiops-to-enable-self-healing-sd-wan.html.

[18] Kevin Jackson, « The Benefits of a Self-Healing Network », 29 août 2017, https://www.helpsystems.com/blog/benefits-self-healing-network.

Ébauche

automation. L'utilisation de l'intelligence artificielle pour les opérations informatiques (AI Ops) pour introduire l'apprentissage machine dans les opérations de la TI augmente le niveau d'automatisation. Ce système peut automatiquement observer le rendement d'application granulaire, surveiller les transactions et utiliser l'analyse des mégadonnées pour prendre des décisions complexes, en assurant la meilleure connexion possible — combinée à la capacité d'apporter des changements critiques au besoin pour maintenir la suprématie opérationnelle. L'ajout des AIOps permet une détection et une réponse automatiques dans l'ensemble des connexions, non seulement pour cerner les problèmes, mais aussi pour les régler en temps réel — avant qu'une application ou un utilisateur ne soit touché. Le système peut aussi apprendre les tendances du trafic et prendre des décisions et présenter des recommandations en temps réel pour optimiser le réseau en fonction de ces tendances.

Un système d'AIOps intégré est capable de consommer et de traiter de vastes ensembles de données pour détecter même les anomalies mineures sur le RE puis introduire une réponse sensée pour protéger la performance des applications, en s'assurant que l'application est à la disposition des utilisateurs quand ils en ont besoin. Le résultat combine la fiabilité, la connectivité, l'établissement de l'ordre de priorité des applications et les accords sur les niveaux de service (ANS) de performance avec les fonctions liées aux anomalies du RE pour normaliser, équilibrer ou corriger le trafic, ce qui créera une solution de RE autorégénérante. Les mesures qui peuvent être obtenues à l'aide de l'apprentissage machine comprennent les suivantes :

a. Précision = $\frac{\text{Nombre total de vrais positifs}}{\text{Nombre total de prévisions}}$

   Plus le nombre de faux positifs est élevé, moins le système est précis;

b. Rappel = Nombre total de vrais positifs prédits à partir du nombre total de vrais positifs présents dans la population/collection.

   Plus le nombre de faux positifs est élevé, plus le rappel est petit;

c. Délai de détection moyen (MTTD);

d. Délai moyen de réponse (MTTR).

La CD-DAR est la console de gestion centralisée qui sert à visualiser et à organiser la connectivité, ainsi qu'à gérer les fonctions avancées de routage et de sécurité, le tout à l'aide d'une console unique. Lorsque le CORFC disposera de sa propre IA, il pourra passer au crible des montagnes de données fournies par des appareils individuels dotés d'IA pour voir et détecter les anomalies et les menaces et y répondre.

4.6 Environnement de soutien en service (SES)

Au moment de la rédaction de cette version du CONOPS, le CONSOUT de la CD-DAR n'a pas encore été mis à jour, et les organisations responsables de chaque niveau de soutien indiquées ci-dessous n'ont pas encore été consultées ni confirmées.

Cette section décrit de manière générale les rôles et responsabilités des organisations de soutien à chaque niveau de soutien. Des précisions sont fournies dans le CONSOUT.

Ébauche

4.6.1 **Soutien de 1er niveau**

4.6.1.1 **Bureau de service national et Centres de gestion des services (CGS) :**

4.6.1.1.1 Rôles et responsabilités

Lorsque les utilisateurs finaux communiquent avec le Bureau de service, il est parfaitement logique que celui-ci tente de recueillir autant d'information et de diagnostics que possible au sujet de l'incident, et même qu'il règle le problème sur-le-champ, si possible. Cette méthode permettra de diminuer le délai de règlement des incidents mineurs, et les règlements dès la première communication accroissent la satisfaction des utilisateurs finaux.

Le personnel de soutien de 1er niveau sera géré par le superviseur du Bureau de service, qui servira de palier supérieur d'intervention, au besoin. Si le soutien de 1er niveau n'est pas en mesure de régler l'incident tout de suite, la responsabilité reviendra au soutien de 2e niveau.

4.6.2 **Soutien de 2e niveau**

4.6.2.1 **7e Groupe des communications**

4.6.2.1.1 Rôles et responsabilités

Le soutien de 2e niveau se compose généralement d'un personnel doté de compétences techniques plus avancées que le personnel du 1er niveau. Ils devraient avoir le temps pour se consacrer au diagnostic et à la résolution des incidents. Le soutien de 2e niveau se rendra auprès de l'utilisateur final au besoin, ce que le personnel du Bureau de service ne peut faire.

4.6.2.2 **Mentorat opérationnel et développement de capacité (MODC)**

4.6.2.2.1 Rôles et responsabilités

Pour que l'équipe de MODC puisse prévoir et gérer globalement l'entretien et l'évolution de la CD-DAR à titre de capacité, les fonctions de soutien fonctionnel et technique doivent être étroitement intégrées. Les responsabilités techniques de MODC comprendront entre autres les suivantes :

a. Appuyer les opérations de cybersécurité et les COD en cours, au besoin;
b. Diriger et coordonner la modification/la transformation technique des capacités de la CD-DAR en matière de cybersécurité et de COD;
c. Encadrer les spécialistes de la maintenance des cybersystèmes à tous les niveaux pour améliorer et maintenir les compétences;
d. Appuyer l'établissement et la coordination de l'instruction sur la maintenance des cybersystèmes;
e. Appuyer les exercices et l'expérimentation relatifs aux cyberopérations;
f. Entretenir et faire évoluer les outils logiciels cybernétiques et de l'ITI de la CD-DAR;
g. Intégrer les nouvelles technologies et les pratiques exemplaires.

Ébauche

Une entente liée à la prestation de services professionnels (probablement avec le fabricant d'équipement d'origine [FEO]/l'ISP) sera conclue en complément du MODC pour la prestation de services comprenant entre autres les suivants :

a. Services de soutien de bout à bout au pays pour la solution CD-DAR, pour assurer un fonctionnement, une surveillance et un soutien continus de tous les composants de la solution CD-DAR;

b. Accès à des ingénieurs et des analystes de la sécurité spécialisés;

c. Accès à des équipes de soutien et de développement de produits, au besoin.

4.6.2.2.2 Environnement d'instruction, d'exercice et d'expérimentation de la CD-DAR

Disposer d'un environnement d'instruction réaliste qui peut imiter un réseau opérationnel, ainsi que l'environnement de l'attaquant, est un grand défi. Le MDN et les FAC ont lancé un projet d'immobilisations pour obtenir un environnement d'instruction cyperopérationnelle (EICO). L'instruction périodique de la CD-DAR serait normalement intégrée dans l'EICO, toutefois, le projet a peu avancé et risque d'être annulé. Le cas échéant, le laboratoire de l'EECI mentionné au paragraphe 4.7.2.3 pourrait être configuré pour appuyer la tenue de l'instruction périodique de la CD-DAR jusqu'à ce qu'un environnement d'instruction du cyberprogramme soit établi pour le MDN et les FAC. L'environnement d'instruction de la CD-DAR comprendra entre autres les capacités suivantes : un simulateur de réseau, une interface utilisateur CD-DAR interactive, un mécanisme de cotation et un agent de l'équipe rouge de la cybersécurité.

Une analyse des besoins en perfectionnement professionnel (ABPP) sera réalisée pendant la phase de définition. Elle permettra d'examiner plus en profondeur les besoins relatifs à l'environnement d'instruction, ainsi que les opérations de la CD-DAR et les besoins du personnel de maintenance en matière d'instruction individuelle et collective.

Comme l'EECI fournira une représentation précise des domaines de production, il peut aussi servir à l'instruction des cyberopérateurs, du personnel des opérations et d'autres postes qui doivent améliorer leurs compétences et leur expérience en cybersécurité sans poser de risque pour l'environnement de production.

Un aperçu complet de l'environnement d'intégration peut être utilisé aux fins d'exercices de destruction (p. ex. équipe rouge/équipe bleue) et rapidement rétabli pour répéter les scénarios d'instruction. Des portions de l'environnement peuvent également être clonées pour devenir des enclaves d'instruction ciblée et spécialisée et d'évaluation.

L'EECI peut aussi servir à l'instruction et à l'expérimentation à l'occasion d'exercices réalisés à l'intérieur du MDN et des FAC, ou à l'extérieur avec d'autres ministères et alliés ou partenaires, comme les exercices CWIX et Bold Quest.

4.6.2.3 **Environnement d'essai cyberintégré (après la mise en œuvre)**

L'environnement d'essai cyberintégré (EECI) n'est pas un environnement unique, mais plutôt un ensemble d'environnements sur mesure, composé d'une infrastructure principalement virtuelle, et ayant des rôles précis concernant l'évaluation des produits et des technologies dans les bacs à sable, l'activité de développement des composants, l'intégration et la vérification, le soutien à l'instruction, aux exercices et à l'expérimentation (voir le paragraphe 4.7.2.2.2 ci-dessus pour obtenir des précisions), la mise en production de la solution CD-DAR et enfin le SES. En plus de

Ébauche

ses activités d'essai et d'évaluation (E et E), l'EECI fournira du soutien à un cyberlaboratoire médicolégal indépendant. Ces environnements sont décrits à la figure 8. Des précisions sur les divers rôles de l'EECI sont présentées dans le CONOPS de l'ingénierie de cybersécurité de l'EECI – CD-DAR.

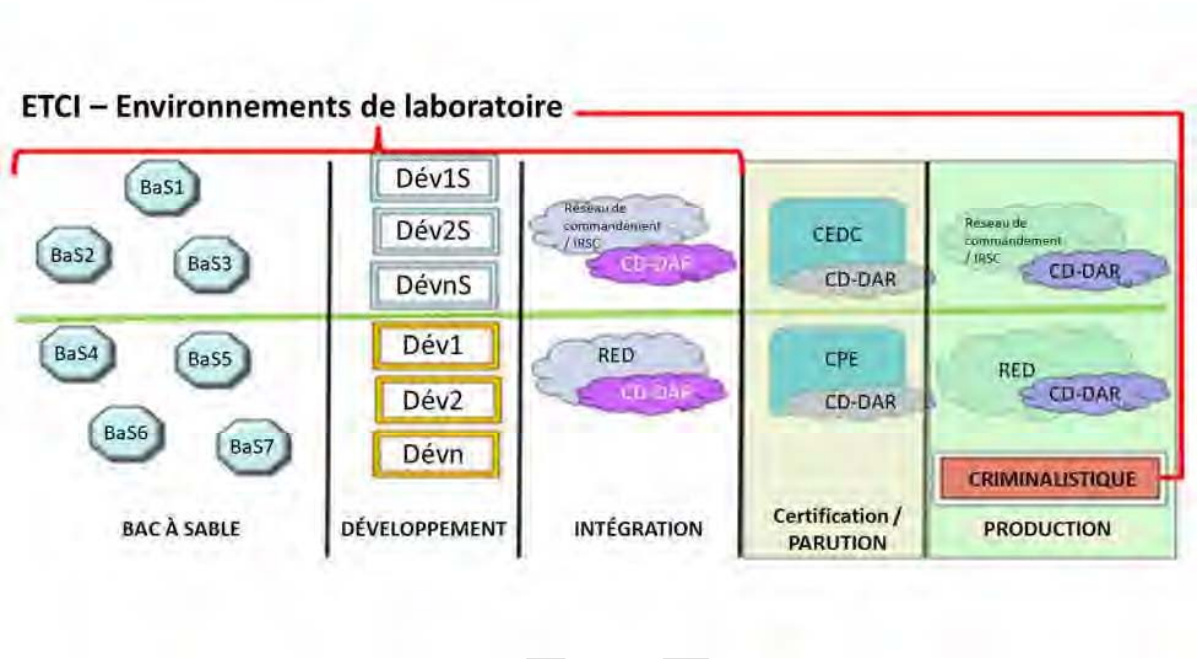


Figure 2 - Environnements de laboratoire de l'EECI

L'EECI servira à plusieurs fins au cours du cycle de vie du projet, et au-delà comme principal moyen de fournir le SES visant l'entretien et l'amélioration des capacités livrées (processus opérationnels et technologies) et d'appuyer l'instruction et le perfectionnement (personnes).

L'EECI fournira des services de recherche, d'essai et d'évaluation en matière de cybersécurité qui améliorent la posture du cyberdomaine du MDN et des FAC en matière de cybersécurité et s'attaquent au contexte changeant de la menace. Pour ce faire, l'EECI fournira un environnement évolutif et adaptable pour appuyer ce qui suit :

a. L'identification et la validation des menaces et des risques en matière de cybersécurité en simulant le cyberdomaine du MDN et des FAC pour déterminer l'incidence sur la mission du MDN et des FAC;

b. L'intégration des capacités, les outils et les technologies de cybersécurité pour protéger les systèmes d'information, les données et l'infrastructure, tout en répondant aux besoins stricts en matière de sûreté, de sécurité et de disponibilité;

c. La transition vers une surveillance en continu de l'environnement du système d'information pour détecter et prévenir efficacement les événements de cybersécurité

d. L'amélioration du processus pour intervenir et reprendre les activités en cas d'événements de cybersécurité et d'attaques, y compris les attaques avancées et persistantes livrées par des groupes criminels et des États-nations adversaires;

e. Le processus d'évaluation et d'amélioration de la résilience des systèmes d'information et de leur capacité de fonctionner et de réaliser la mission du MDN et des FAC, même lorsqu'ils sont touchés par un événement de cybersécurité ou une attaque.

L'EECI fournira un environnement qui aura les fonctions suivantes :

a. Simuler avec exactitude la performance de toutes les extensions et interfaces du réseau de commandement du MDN et des FAC, sur place ou en déploiement, et les systèmes du RED déployables identifiés, et fournir une représentation de base de la configuration gérée pour chaque facette de ces réseaux;

b. Évaluer, au sein des cyberdomaines du MDN et des FAC concernés, la performance des éléments suivants de façon fiable et exacte :

   i. Nouveau matériel ou logiciel,

   ii. Changements de configuration apportés au matériel ou aux logiciels déjà installés,

   iii. Ajouts ou changements apportés à la nature et au nombre d'utilisateurs autorisés,

   iv. Ajouts ou changements apportés aux points de présence et leurs emplacements,

   v. Effets sur la quantité de données ou la bande passante à n'importe quel point des réseaux,

   vi. Collecte des données du journal du système et des données de la GIES,

   vii. Distribution des données du journal du système et des données de la GIES;

c. Assurer une intégration dans les systèmes d'essai et d'évaluation de la GI/TI prévus ou existants du MDN et des FAC;

d. Améliorer la sensibilisation technique à la configuration et au fonctionnement des cyberdomaines existants du MDN et des FAC;

e. Améliorer la détection des vulnérabilités dans les cyberdomaines existants du MDN et des FAC.

4.6.3 **Soutien de 3e niveau**

4.6.3.1 **DIIGI**

4.6.3.1.1 Rôles et responsabilités

Le rôle du soutien de 3e niveau est réservé à un groupe technique interne dont les membres doivent posséder les connaissances requises (p. ex. soutien du réseau, soutien des bases de données, entretien du matériel, etc.).

Si la fonction du soutien de 3e niveau ne peut être fournie par le DIIGI, si l'expertise requise concerne un domaine très pointu, p. ex. les moteurs d'IA et les algorithmes, la demande passera au soutien de 4e niveau, soit à un ou des fournisseurs de service externes.

Ébauche

4.6.4 **Soutien de 4e niveau**

4.6.4.1 **Services contractuels d'un tiers**

4.6.4.1.1 Rôles et responsabilités

Les services de soutien technique sont requis pendant la durée de vie en service de la capacité de la CD-DAR et pourraient comprendre des recherches techniques et études d'ingénierie (RTEI), des services professionnels (entrepreneurs/consultants), et une autre capacité d'entretien de 4e niveau pour régler les problèmes non résolus au soutien de 3e niveau, ou pour faire évoluer les fonctionnalités de la CD-DAR.

5 CONCLUSION

La capacité de CD-DAR permettra à la cyberforce du MDN et des FAC de défendre la liberté d'action et les intérêts des FAC dans le cyberespace, et de produire des effets militaires dans un cyberenvironnement contesté et à l'aide de celui-ci, à l'appui des missions des FAC et des régions du cyberespace mondial utilisées par les alliés et les partenaires du Canada.

5.1 Incidences opérationnelles

La CD-DAR réalisera un inventaire électronique automatisé complet de tous les appareils matériels et les logiciels; fournira la capacité d'identifier et de suivre tous les biens (autorisés et non autorisés) qui sont connectés au réseau de commandement; évaluera leurs caractéristiques pour déceler leur vulnérabilité, leur configuration, leur risque et leur conformité aux correctifs. Le dépôt fiable et unique de la CD-DAR pour la collecte de données de renseignement sur les cybermenaces et les données de base des systèmes et des réseaux permettront la surveillance et l'analyse de la sécurité.

Les COD du MDN et des FAC seront exécutées à l'aide d'une interface utilisateur unique qui comprend un ensemble d'outils logiciels pour automatiser efficacement la détection des cybermenaces, et gérer les incidents et en assurer la traçabilité à l'aide de l'ensemble du processus d'analyse, ce qui réduira les connaissances et la spécialisation actuellement requise des opérateurs.

La CD-DAR offrira une vision centrale de l'ensemble du réseau pour évaluer les cyberactivités, le trafic, les écarts et les anomalies, et un portrait complet du contexte de la cybermenace. Elle automatisera, rationalisera et simplifiera les procédures pour alléger la surcharge cognitive des opérateurs, et rendra possible la réalisation à distance d'analyses criminalistiques et de confinement/correction.

La CD-DAR sera une capacité intégrée, modulaire et évolutive qui sera interopérable avec les plateformes existantes du MDN et des FAC ainsi qu'avec celles des autres ministères et des alliés. Cette nouvelle capacité établira et tiendra à jour la cybersécurité, la connaissance de la situation et l'analyse – qui seront toutes intégrées dans un système pour fournir une analyse fiable et contextuelle à l'appui des décisions et des mesures prises dans le cadre des cyberopérations du MDN et des FAC.

Ébauche

5.2 Incidences opérationnelles

Le CORFC demeure l'organisation responsable de la cyberdéfense au sein du MDN et des FAC. Sa mission est d'obtenir et de maintenir la supériorité dans la cyberzone de responsabilité du MDN et des FAC et de veiller à ce que la capacité des FAC d'utiliser l'ITI sans interruption ou interférence par les adversaires demeure intacte.

Le système de processus, de logiciels et de matériel de la CD-DAR pourra être utilisé par le personnel opérationnel existant du MDN et des FAC, y compris le personnel qui produit et consomme actuellement l'information de la CS, sans instruction excessive ou changement aux compétences des groupes professionnels qui exercent ces rôles. L'interface utilisateur unique intégrée et améliorée de la CD-DAR rationalise le processus opérationnel de cyberdéfense en général, restreint les besoins de connaissances spécialisées et le temps d'instruction requis.

La CD-DAR est une capacité « en coulisses » qui protège le réseau des tentatives d'intrusion non autorisées et malveillantes. Elle est indétectable par les utilisateurs autorisés du réseau de commandement lorsqu'ils y accèdent ou qu'ils l'utilisent.

5.3 Incidences pendant le développement et la livraison

En raison de l'importance du cyberdomaine pour les opérations et le fonctionnement du MDN et des FAC, le risque d'une interruption de service nuirait à la sécurité nationale du Canada. Les nouvelles capacités à acquérir dans le cadre de ce projet nécessiteront une connaissance intime et une interaction étroite avec le cœur même de l'ITI du MDN et des FAC. Ainsi, les objectifs du projet de la CD-DAR pendant le développement et la livraison sont les suivants :

a. Perturber le moins possible les opérations quotidiennes;

b. Au besoin, faire appel à l'expertise de la communauté des COD pour :

   i. Peaufiner et valider les exigences opérationnelles et fonctionnelles de la capacité,

   ii. Essayer et évaluer la capacité à mesure qu'elle évolue durant le cycle de vie du projet,

   iii. Appuyer les essais de réception de la capacité opérationnelle initiale (COI) et la capacité opérationnelle totale (COT);

c. Faciliter une transition harmonieuse et efficace de la cybersécurité et de la cyberdéfense à l'aide de la capacité de CD-DAR, par l'instruction et le mentorat ponctuels des utilisateurs de la CD-DAR;

d. Institutionnaliser un cadre de capacités de SES pour tenir à jour et optimiser les processus opérationnels des COD, les outils matériels et logiciels de la CD-DAR, et l'instruction périodique du personnel pour s'assurer que la capacité de CD-DAR demeure disponible, fiable et pertinente sur le plan opérationnel pendant toute la durée de sa vie utile.

Une équipe de MODC entièrement doté sera mise sur pied pour la COI, et aura atteint son efficacité optimale avant la COT, pour soutenir et faire continuellement et globalement évoluer la capacité de CD-DAR (personnes, opérations et outils), tout en fournissant une coordination

Ébauche

avec les autres ministères et les alliés pour assurer une interopérabilité continue et la synergie des efforts, afin de maintenir les performances optimales de la capacité et d'anticiper ainsi les menaces croissantes. L'équipe de MODC s'occupera aussi d'entraîner, de former et de guider les cyberopérateur, les gestionnaires et les directeurs dans l'agencement continu des activités, le perfectionnement des compétences, l'établissement de l'instruction collective et la coordination des exercices, afin de maintenir les compétences et de réaliser leurs missions.

Ébauche

Annexe A – Diagrammes d'interaction organisationnelle du CORFC

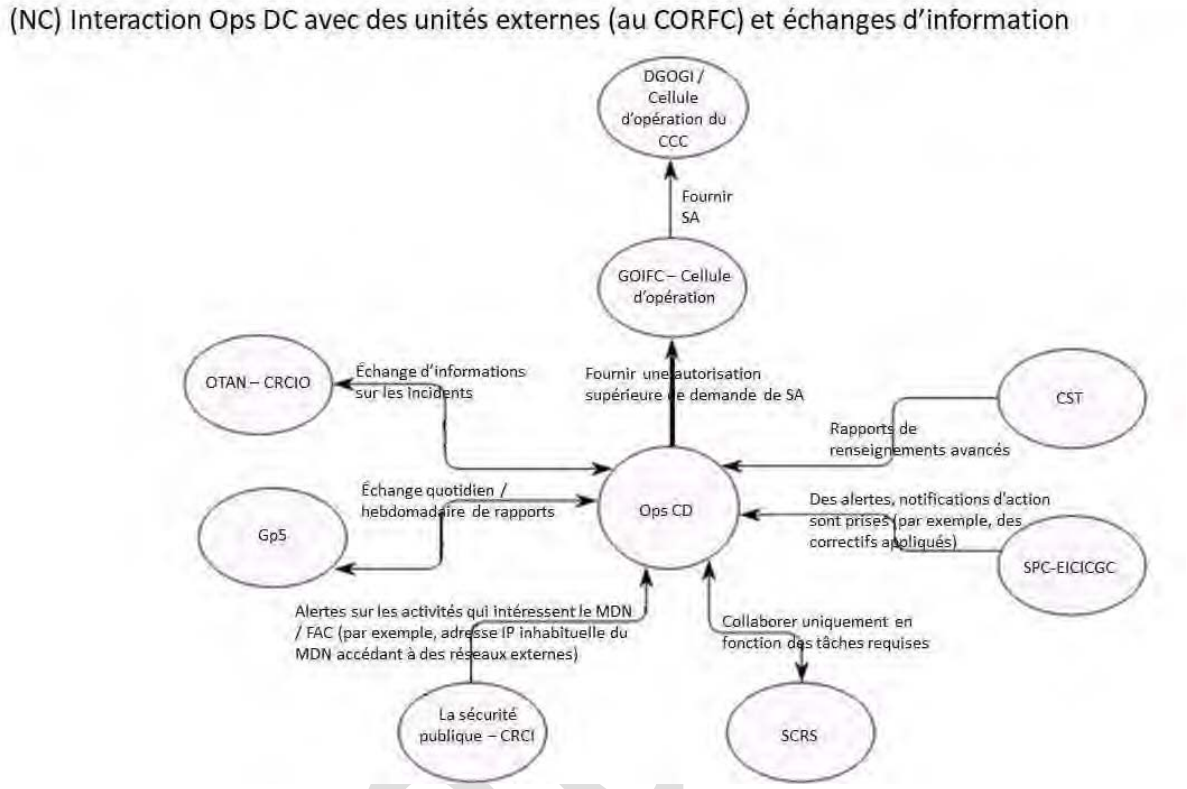


Figure 9 – Interaction avec les Ops CD et échange de renseignements ou d'information avec les intervenants

Ébauche

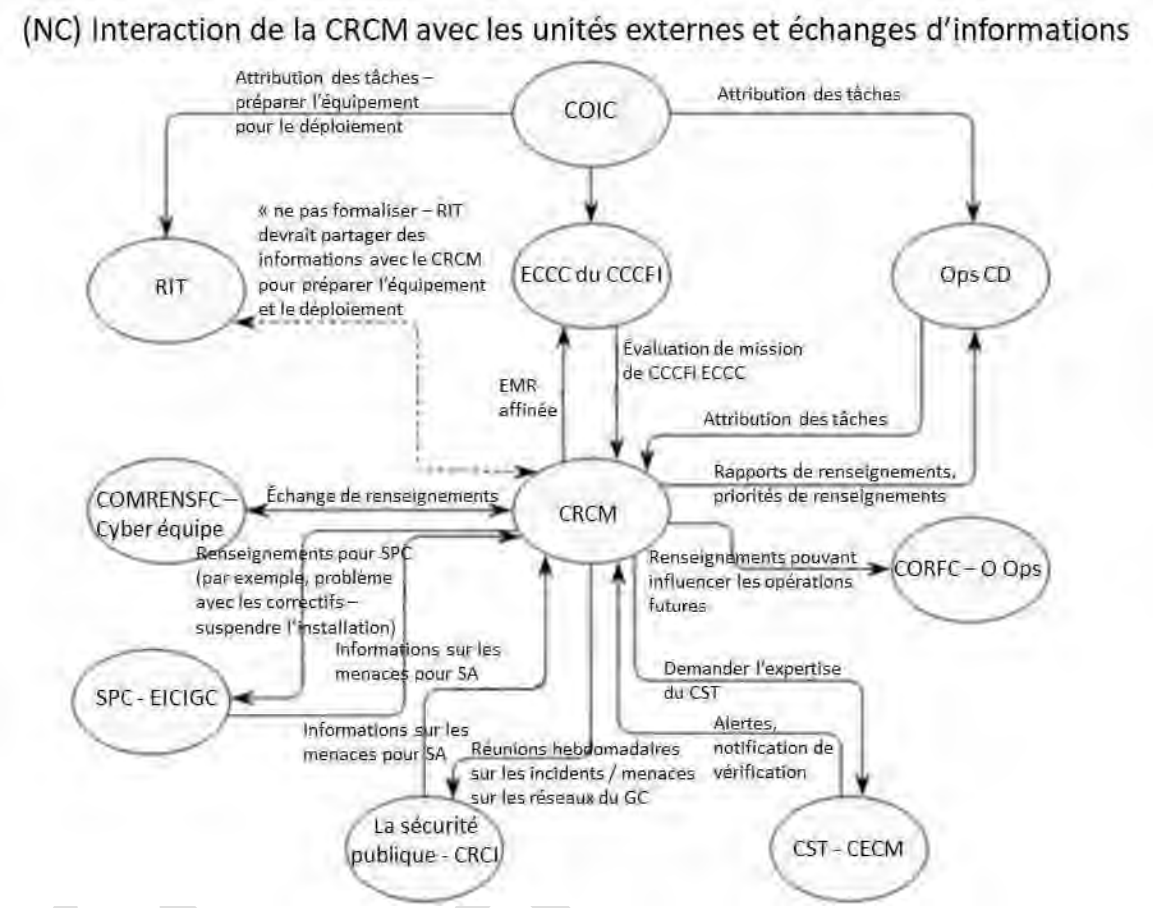


Figure 10 – Interaction avec la CRCM et échange de renseignements ou d'information avec les intervenants

Ébauche

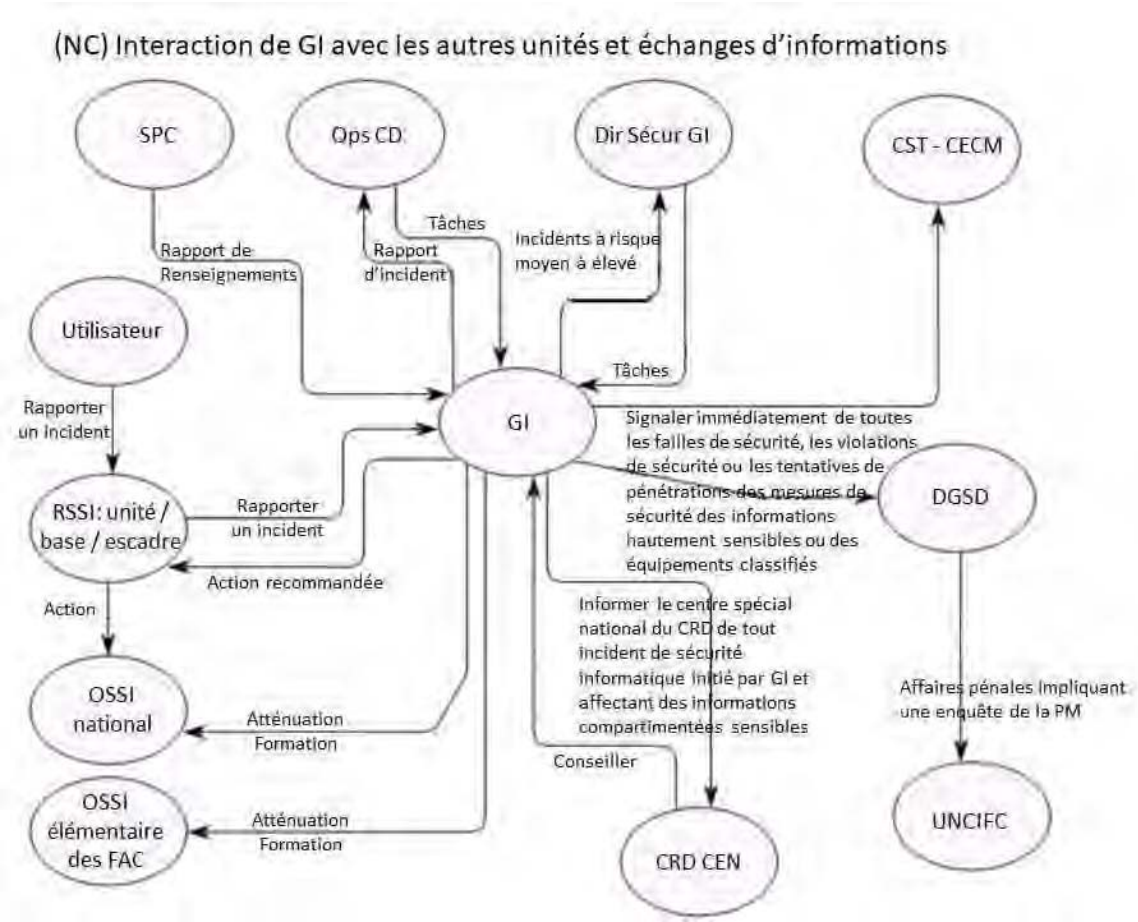


Figure 11 – Interaction avec l'équipe d'intervention en cas d'incident et échange de renseignements ou d'information avec les intervenants

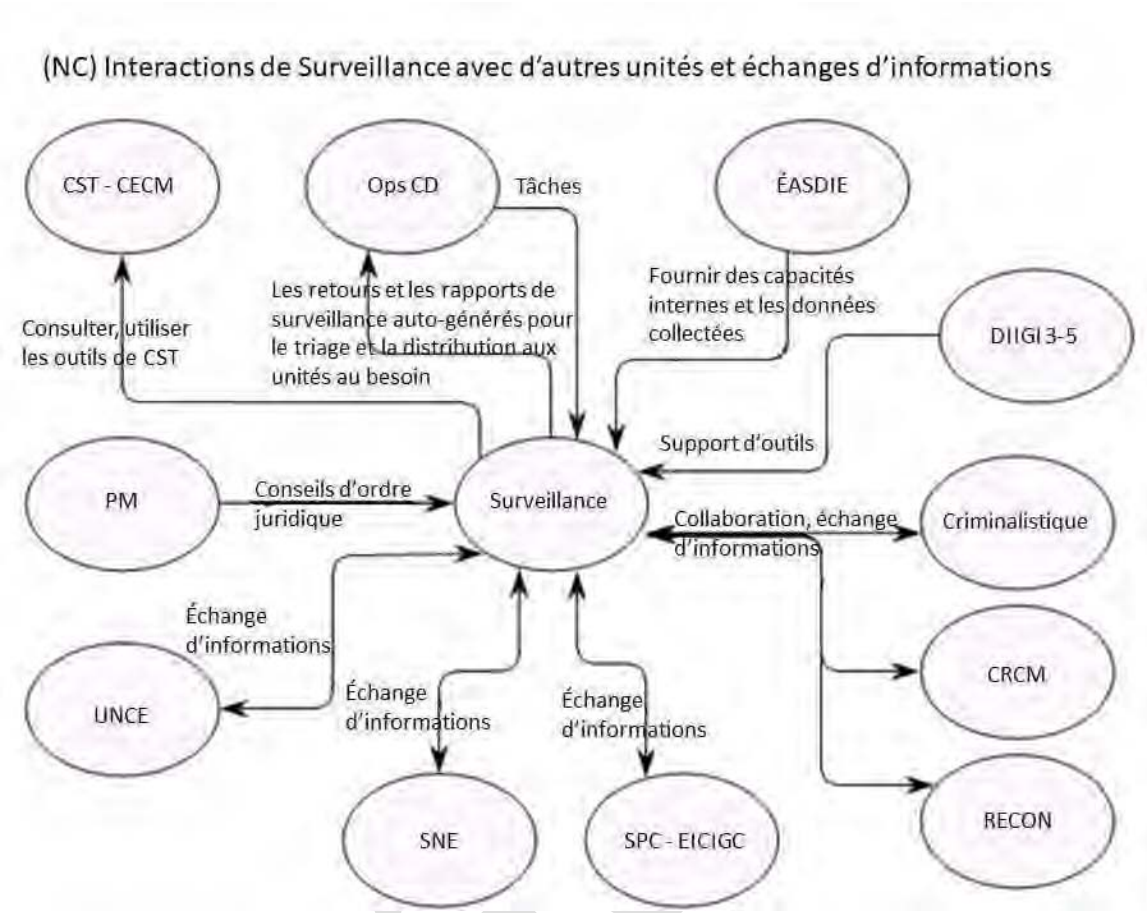


Figure 12 – Interaction avec l'équipe de surveillance et échange de renseignements ou d'information avec les intervenants

Ébauche

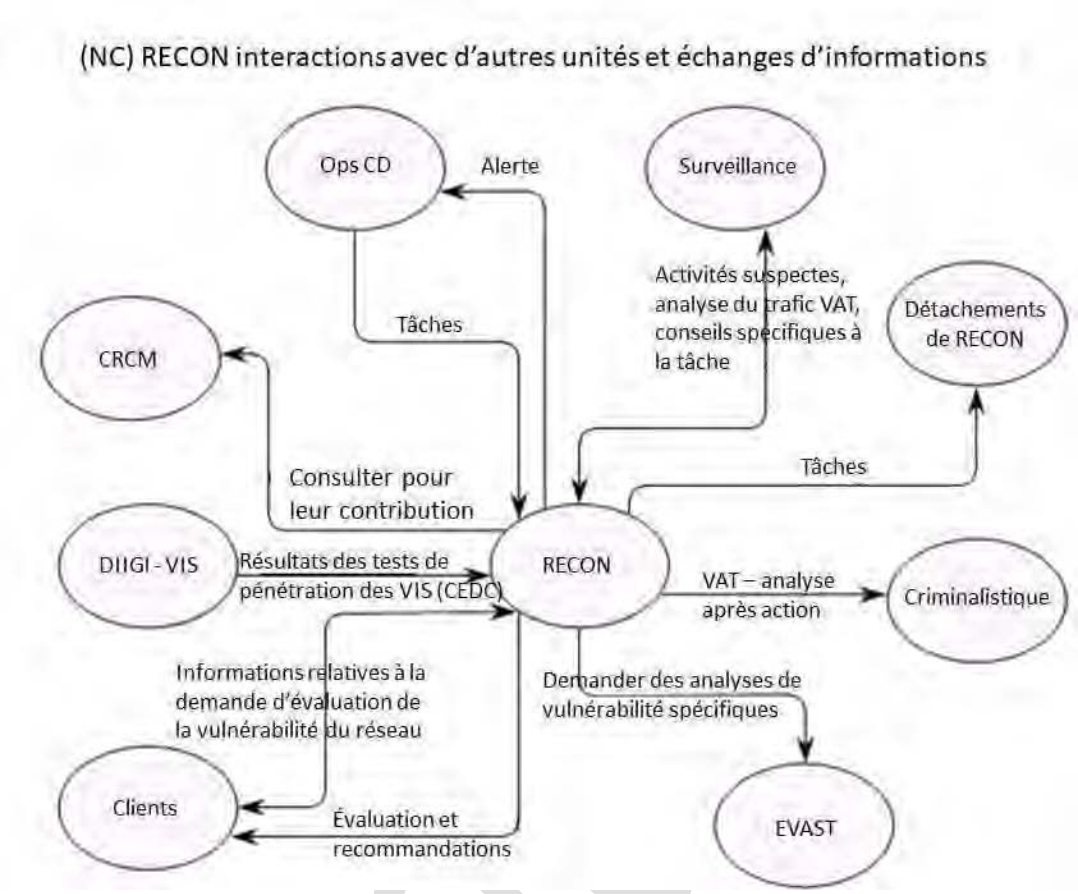


Figure 13 – Interaction avec l'équipe de reconnaissance et échange de renseignements ou d'information avec les intervenants

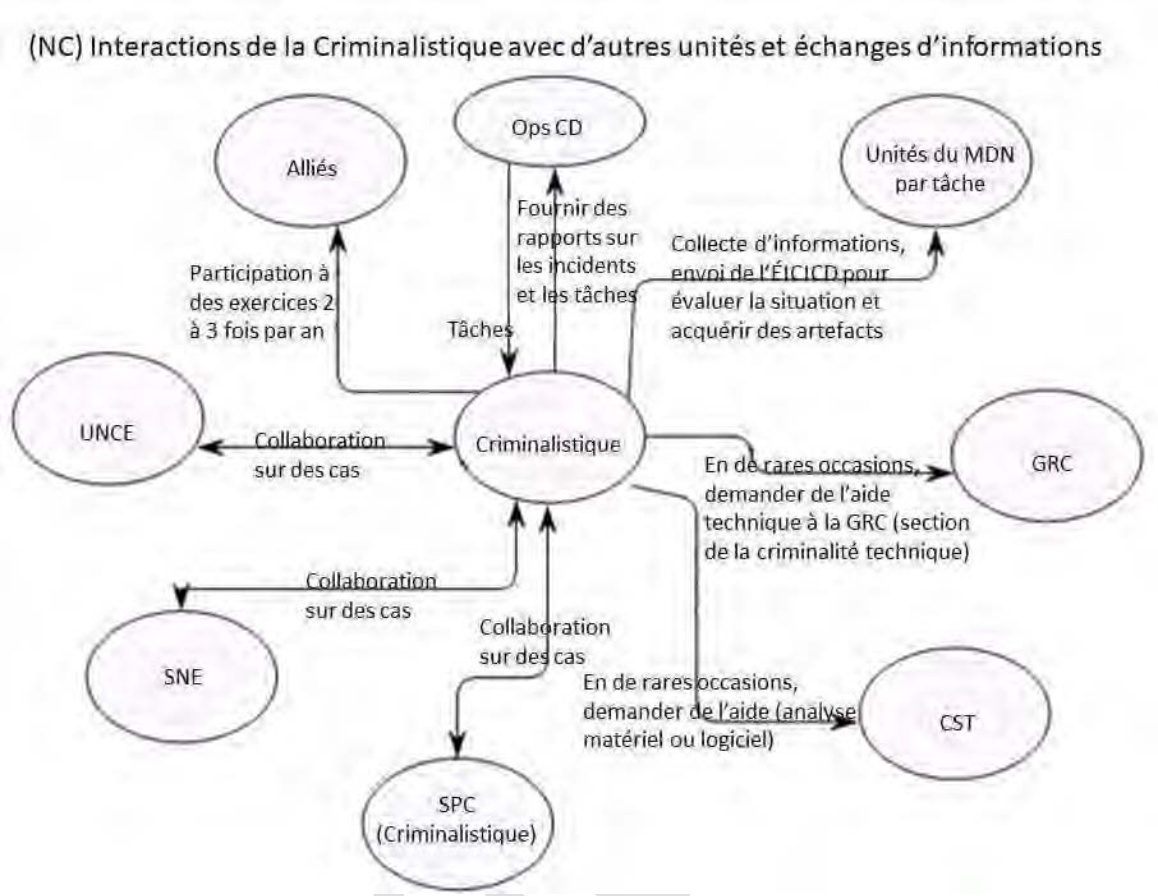


Figure 14 – Interaction avec l'équipe de criminalistique et échange de renseignements ou d'information avec les intervenants

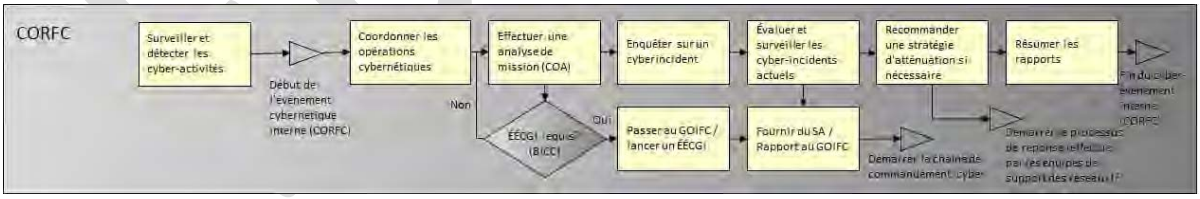


Figure 15 – Flux de coordination des cyberévénements des Ops CD

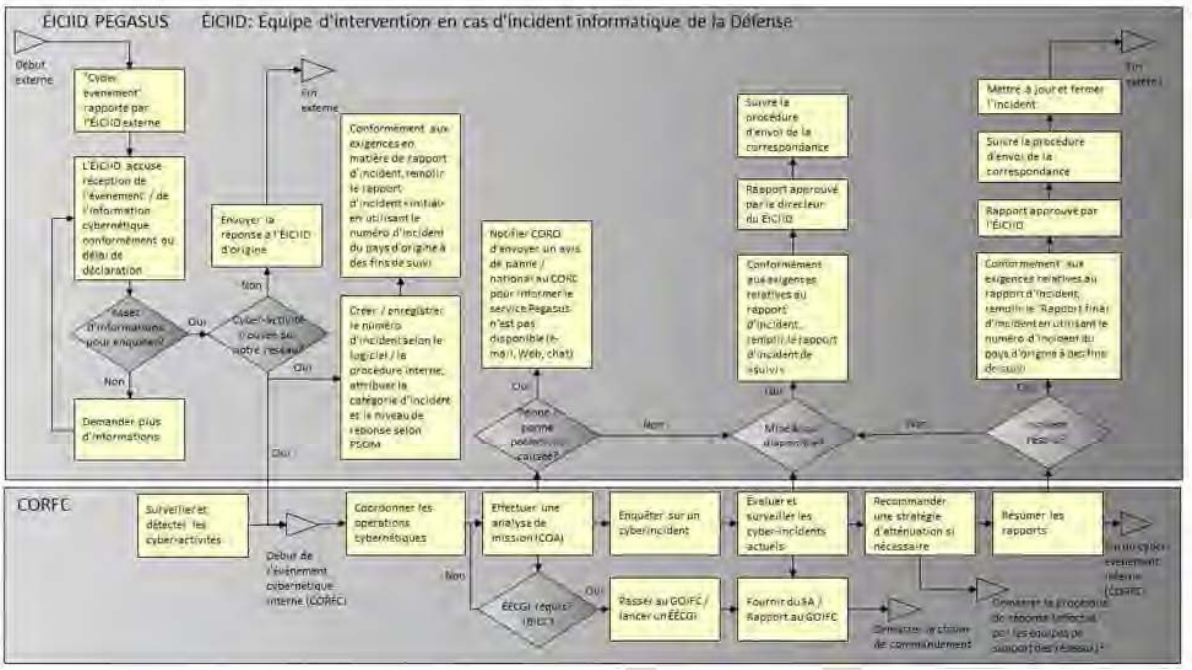


Figure 16 – Gestion des cyberévénements, y compris avec le Groupe des cinq sur Pegasus

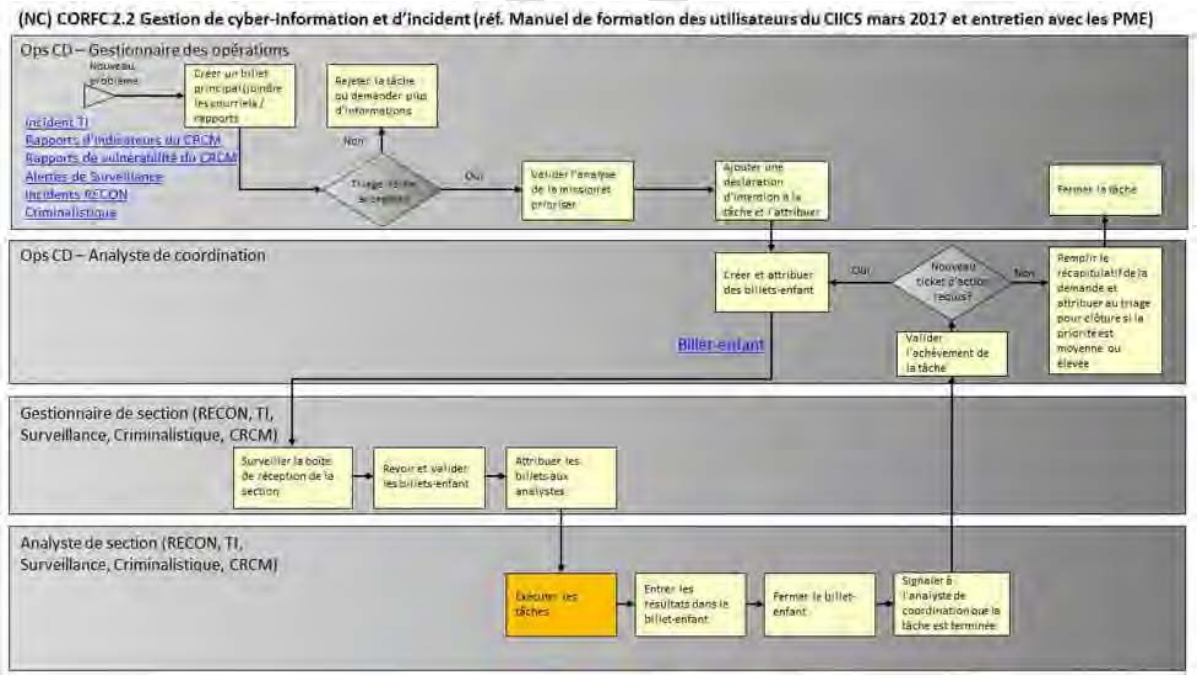


Figure 17 – Flux de gestion et d'acheminement de la cyberinformation

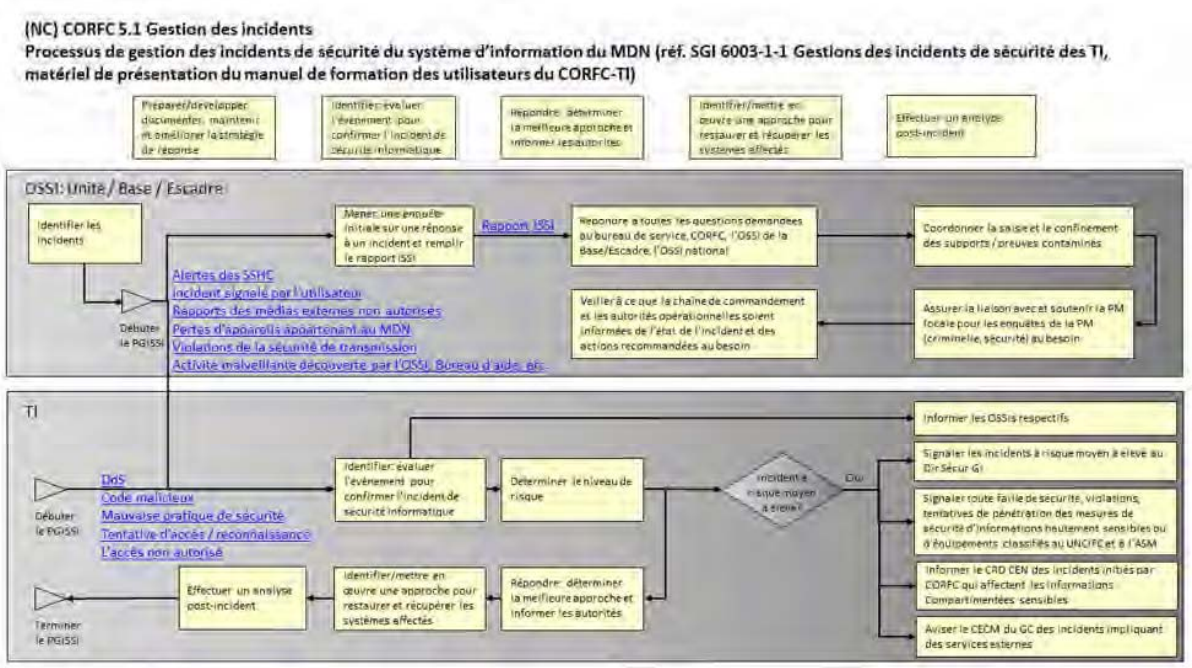


Figure 18 – Flux d'intervention en cas d'incident

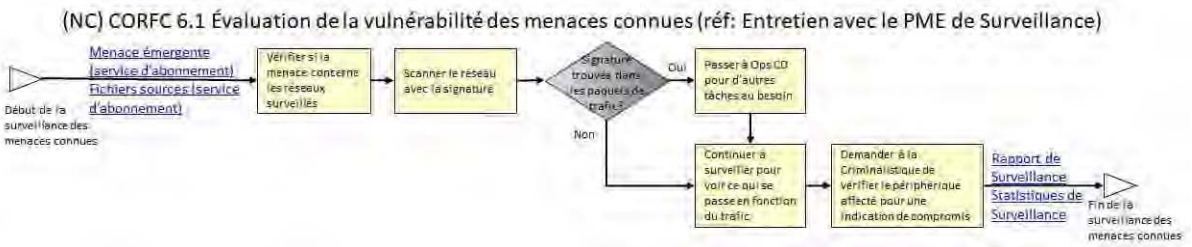


Figure 19 – Flux d'évaluation des menaces connues

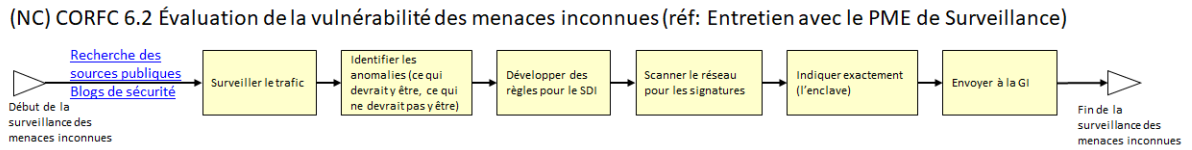


Figure 20 – Flux d'évaluation des menaces inconnues

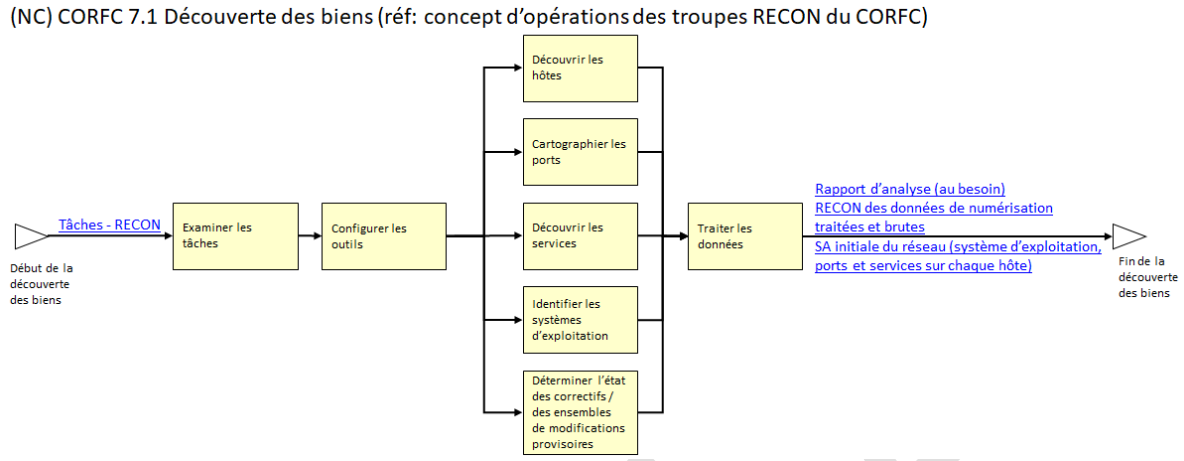


Figure 21 – Flux de découverte des biens

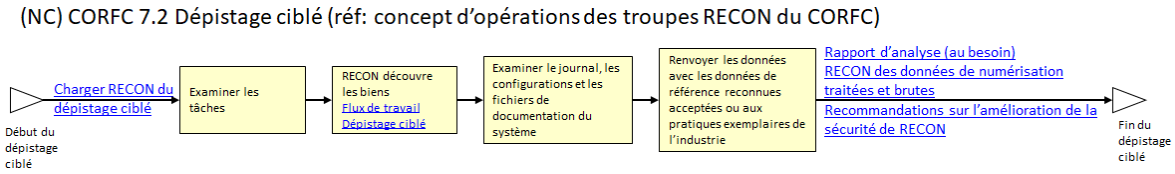


Figure 22 – Flux d'analyse d'objectif

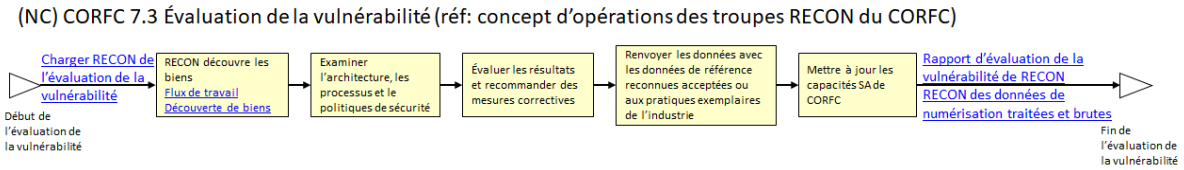


Figure 23 – Flux d'évaluation de la vulnérabilité

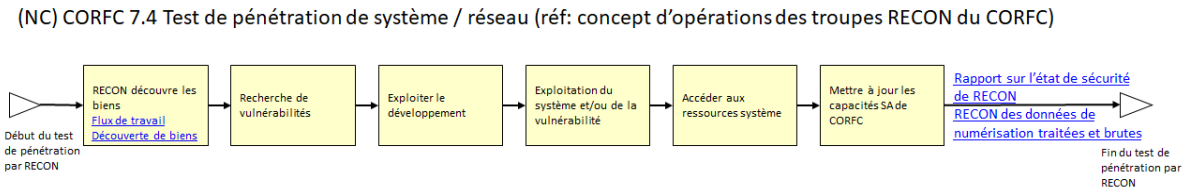


Figure 24 – Flux d'essai de pénétration de système ou de réseau

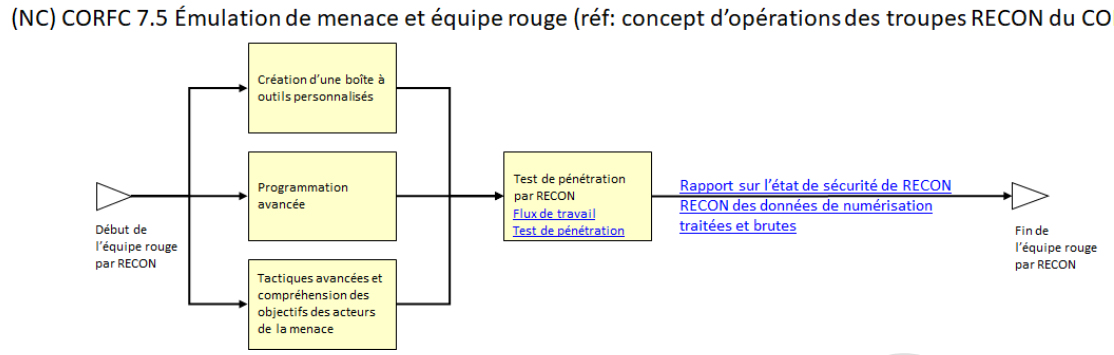


Figure 25 – Flux d'émulation de menace

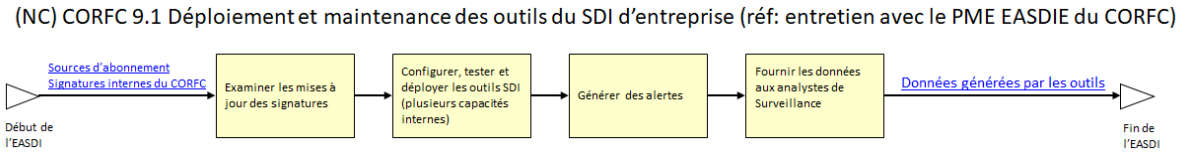


Figure 26 – Flux du système de détection des intrusions (SDI) de l'organisation

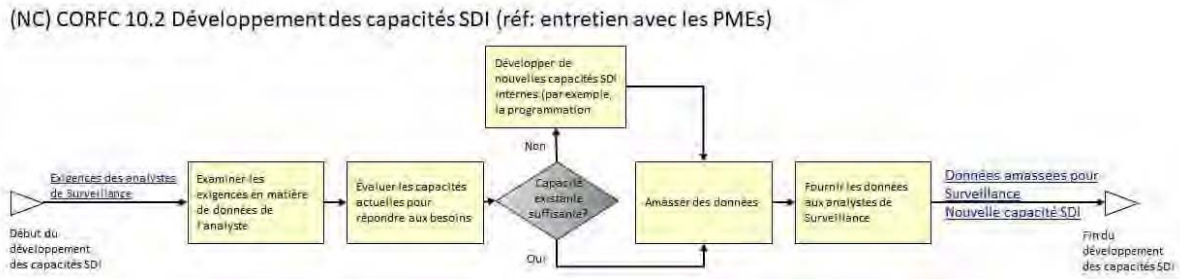


Figure 27 – Flux de développement des capacités du SDI

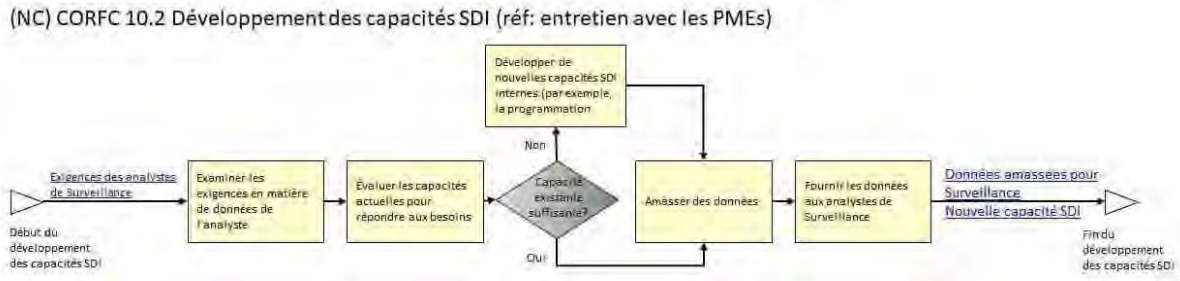


Figure 28 – Flux d'évaluation de la vulnérabilité de l'organisation

Annexe B – Liste d'abréviations

Terme	Description
7 Gp Comm	7e Groupe des communications
ABPP	Analyse des besoins en perfectionnement professionnel
AC	Armée canadienne
ACH	Analyse d'hypothèses concurrentes
AI Ops	Intelligence artificielle pour les opérations informatiques
AIS	Automated Indicator Sharing
ANS	Accord sur les niveaux de service
AO	Autorité opérationnelle
ARC	Aviation royale canadienne
AT	Autorité technique
ATEO	Analyse tactique de l'environnement opérationnel
AUS/NZ/UK/US	Australie/Nouvelle-Zélande/Royaume-Uni/États-Unis
BDGC	Base de données de gestion des configurations
BNGS	Bureau national de gestion des services
BSN	Bureau de service national
BTD	Banque de terminologie de la défense
C2	Commandement et contrôle
C4ISR	Commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance
CAM	Cyberassurance de la mission
CAMDN	Cadre d'architecture du ministère de la Défense nationale et des Forces canadiennes
CCCFI	Commandant de la composante cybernétique des forces interarmées
CCCS	Centre canadien pour la cybersécurité
CCEB	Combined Communications and Electronics Board
CCF	Commandant de la cyberforce
CCRIC	Centre canadien de réponse aux incidents cybernétiques
CCS	Connaissance de la cybersituation

Ébauche

Terme	Description
CCSéc	Cadre de cybersécurité
CD Ops	Opérations de cyberdéfense
CDA	Cyberdéfense active
CD-DAR	Cyberdéfense – Décision, analyse et réponse
CECM	Centre d'évaluation des cybermenaces
CEDC	Centre d'essais et de développement classifiés
CEM	Chef d'état-major
CEM Cyber	Chef d'état-major du cyberespace
CEMD	Chef d'état-major de la défense
CG	Centre de gravité
CGIEB	Capacité de gestion interarmées de l'espace de bataille
CGS	Centre de gestion des services
CIICS	Cyber Information and Incident Sharing System
Cmdt COMCYBER	Commandant du Commandement de cyberdéfense
CMR	Cadre ministériel des résultats
COD – AD	Cyberopérations défensives – Aide à la décision
COD – MDI	Cyberopérations défensives – Mesures de défense interne
COD	Cyberopération défensive
COI	Capacité opérationnelle initiale
COIC	Commandement des opérations interarmées du Canada
COMFOSCAN	Commandement des Forces d'opérations spéciales du Canada
COMM N	Communicateurs navals
COMRENSFC	Commandement du renseignement des Forces canadiennes
COMSEC	Sécurité des communications
CONOPS	Concept d'opération
CONPLAN	Plan de contingence
CONSOUT	Concept de soutien
CORFC	Centre d'opérations des réseaux des Forces canadiennes
COSD	Centre des opérations des services de la Défense

Ébauche

Terme	Description
COT	Capacité opérationnelle totale
COTS	Disponible sur le marché
Cpl	Caporal
Cplc	Caporal-chef
CPU	Unité centrale
CRCM	Cellule du renseignement sur les cybermenaces
CRD	Chef du renseignement de la Défense
CS	Chef de la sécurité
CS	Connaissance de la situation
CSA	Cybersécurité accrue
CSTC	Centre de la sécurité des télécommunications Canada
DAP	Directive d'approbation de projet
DC	Demande de changement
CDR	Dépôt des cyberdonnées
DCFC	Division cybernétique des Forces canadiennes
DCO	Domaine des cyberopérations
DdC	Demande de changement
DDCGI	Directeur – Développement des capacités (Gestion de l'information)
DDFOC	Directeur - Développement des Forces (Opérations cybernétiques)
DF	Développement des forces
DGDFCI	Directeur général – Développement des forces (Capacités d'information)
DGOGI	Directeur général – Opérations (Gestion de l'information)
DGRPGI	Directeur général – Réalisation de projets (Gestion de l'information)
DGSAE	Directeur général – Service des applications de l'entreprise
DGSD	Directeur général – Sécurité de la défense
DGTPSGI	Directeur général – Technologie et planification stratégique (Gestion de l'information)
DHS	Département de la Sécurité intérieure
DI	Demande d'information
DIIGI	Directeur – Ingénierie et intégration (Gestion de l'information)

Ébauche

Terme	Description
DIPE	Détection et intervention des points d'extrémités
Dir Sécur GI	Directeur – Sécurité (Gestion de l'information)
DP	Directeur de projet
DRPCC	Directeur – Réalisation de projets (Commandement et contrôle)
E et E	Essai et évaluation
É.-U.	États-Unis
EAS	Évaluation et autorisation de la sécurité
EBO	Énoncé des besoins opérationnels
ECCC	Élément de coordination de la composante cybernétique
EECI	Environnement d'essai cyberintégré
EF	Emploi d'une force
EFRD	Évaluation des facteurs de risque dynamiques
EGCGI	Équipe de gestion de crise en gestion de l'information
EICO	Environnement d'instruction cyberopérationnel
EIICD	Équipe d'intervention en cas d'incident de cyberdéfense
EIICGC	Équipe d'intervention en cas d'incident cybernétique du gouvernement du Canada (GC)
EIIID	Équipe d'intervention en cas d'incident informatique de défense
EITS	Équipe d'inspection technique de sécurité
EM	Expert en la matière
EMIS	État-major interarmées stratégique
EMR	Évaluation des menaces et des risques
EMSEC	Sécurité des émissions
EOCI	Équipe des opérations cybernétiques interarmées
EOHN	Exigence obligatoire de haut niveau
EPS	Évaluation de la posture de sécurité
ERC	Équipe responsable de la cyberprotection
ESEVO	Équipe de soutien de l'évaluation des vulnérabilités organisationnelles
ESSDI	Équipe de soutien des systèmes de détection des intrusions

Ébauche

Terme	Description
Exercice CWIX	Coalition Warrior Interoperability eXploration eXperiment eXamination eXercise
FAC	Forces armées canadiennes
FEO	Fabricant d'équipement d'origine
FOROP	Forces d'opposition
GC	Gouvernement du Canada
GE	Guerre électronique
GFRD	Gestion des facteurs de risque dynamiques
GI	Gestion de l'information
GIA	Gestion des identités et de l'accès
GIES	Gestion des informations et des événements de sécurité
GMTS	Guides de mise en œuvre technique de la sécurité
GOIFC	Groupe des opérations d'information des Forces canadiennes
GP	Gestionnaire de projet
Gp GI	Groupe de gestion de l'information
Gp5	Groupe des cinq
GRC	Gendarmerie royale du Canada
GSTI	Gestion des services de technologie de l'information
GSTIE	Gestion des services en technologie de l'information d'entreprise
IA	Intelligence artificielle
IC/DC	Intégration continue/déploiement continu
ICSO	Image commune de la situation opérationnelle
IdO	Internet des objets
Info	Information
IP	Protocole Internet
IRC	Indicateur de rendement clé
IRPVD	Infrastructure du réseau privé virtuel de la défense
IRSC	Infrastructure du réseau secret consolidé
ISP	Intégrateur de système principal
ITI	Infrastructure de la technologie de l'information

Ébauche

Terme	Description
LR	Leçons retenues
MDN	Ministère de la Défense nationale
MI	Mesure d'intervention
MISP	Malware Information Sharing Platform
MODC	Mentorat opérationnel et développement de capacité
MPA	menace persistante avancée
MPF	Mise sur pied d'une force
MRC	Marine royale canadienne
NCIRC	Capacité d'intervention en cas d'incidents informatiques de l'OTAN
NGP	Note de service destinée à servir de guide sur le programme
NIST	National Institute of Standards and Technology
NORAD	Commandement de la défense aérospatiale de l'Amérique du Nord
NSA	National Security Agency
NVD	National Vulnerability Database
OASI	Orchestration et automatisation de la sécurité et intervention
O Ops	Officier des opérations
ONU	Organisation des Nations Unies
OODA	Observer, orienter, décider, agir
OP EICM	Opérateurs d'équipement d'informations de combat (Marine)
Op	Opération
OPCOM	Commandement opérationnel
OPCON	Contrôle opérationnel
OPID	Officier principal de l'information de la Défense
Ops réseaux	Opérations de réseaux
Ops	Opérations
OPSEC	Sécurité des opérations
OSSI	Officier de la sécurité des systèmes d'information
OTAN	Organisation du Traité de l'Atlantique Nord
PA	Plan d'action
PF&DO	Posture de la force et disponibilité opérationnelle

Ébauche

Terme	Description
PM	Police militaire
PSE	Protection, Sécurité, Engagement : La politique de défense du Canada
QG FOI	Quartier général des forces opérationnelles interarmées
QGDN	Quartier général de la Défense nationale
RBAC	Contrôle d'accès basé sur les rôles
RC	Réseau de commandement
RE	Réseau étendu
RECO	Reconnaissance
RED	Réseau étendu de la Défense
Rens	Renseignement
RM	Renseignement sur les menaces
RMSC	Responsable ministériel de la sécurité des communications
RTEI	Recherches techniques et études d'ingénierie
RTI	Régiment des transmissions interarmées
S et C	Surveillance et conformité
SCRS	Service canadien du renseignement de sécurité
SDI	Système de détection des intrusions
Sdt	Soldat
SES	Soutien en service
Sgt	Sergent
SIC	Systèmes d'information et de communication
SIGINT	Renseignement d'origine électromagnétique
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
SNEFC	Service national des enquêtes des Forces canadiennes
SPC	Sécurité publique Canada
SPC	Services partagés Canada
SSCIAT	Spécialiste des systèmes de communication et d'information de l'Armée de terre
TECH SITA	Technicien de systèmes d'information et de télécommunications aérospatiales

Ébauche

Terme	Description
TI	Technologie de l’information
TRANSEC	Sécurité des transmissions
TTP	Tactiques, techniques et procédures
UNCE	Unité nationale de contre-espionnage
URL	Localisateur de ressources uniforme
VAT	Visite d’aide technique
VCEMD	Vice-chef d’état-major de la défense
VIS	Validation de l’ingénierie de sécurité
EVGO	Éditeur visuel de guides opérationnels
ZResp	Zone de responsabilité

Ébauche