



**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

Bid Fax: (819) 997-9776

**LETTER OF INTEREST**

**LETTRE D'INTÉRÊT**

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 sécurité et des opérations d'information

11 Laurier St. / 11, rue Laurier

8C2, Place du Portage

Gatineau

Québec

K1A 0S5

<b>Title - Sujet</b> Projet MGETFC	
<b>Solicitation No. - N° de l'invitation</b> W8476-196070/A	<b>Date</b> 2019-02-04
<b>Client Reference No. - N° de référence du client</b> W8476-196070	<b>GETS Ref. No. - N° de réf. de SEAG</b> PW-\$\$QE-015-27182
<b>File No. - N° de dossier</b> 015qe.W8476-196070	<b>CCC No./N° CCC - FMS No./N° VME</b>
<b>Solicitation Closes - L'invitation prend fin</b> <b>at - à 02:00 PM</b> <b>on - le 2019-05-13</b>	
<b>Time Zone</b> <b>Fuseau horaire</b> Eastern Daylight Saving Time EDT	
<b>F.O.B. - F.A.B.</b> <b>Plant-Usine:</b> <input type="checkbox"/> <b>Destination:</b> <input type="checkbox"/> <b>Other-Autre:</b> <input type="checkbox"/>	
<b>Address Enquiries to: - Adresser toutes questions à:</b> Picknell, Christine	<b>Buyer Id - Id de l'acheteur</b> 015qe
<b>Telephone No. - N° de téléphone</b> (819) 420-1761 ( )	<b>FAX No. - N° de FAX</b> (819) 956-6907
<b>Destination - of Goods, Services, and Construction:</b> <b>Destination - des biens, services et construction:</b> -	

Instructions: See Herein

Instructions: Voir aux présentes

<b>Delivery Required - Livraison exigée</b> See Herein	<b>Delivery Offered - Livraison proposée</b>
<b>Vendor/Firm Name and Address</b> <b>Raison sociale et adresse du fournisseur/de l'entrepreneur</b>	
<b>Telephone No. - N° de téléphone</b> <b>Facsimile No. - N° de télécopieur</b>	
<b>Name and title of person authorized to sign on behalf of Vendor/Firm</b> <b>(type or print)</b> <b>Nom et titre de la personne autorisée à signer au nom du fournisseur/</b> <b>de l'entrepreneur (taper ou écrire en caractères d'imprimerie)</b>	
<b>Signature</b>	<b>Date</b>

**Modernisation de la guerre électronique terrestre des Forces  
canadiennes (MGETFC)**

-

**Lettre d'intérêt**

**TABLE DES MATIÈRES**

PARTIE I: PROCESSUS RELATIF À LA LETTRE D'INTÉRÊT .....	3
1. INTRODUCTION.....	3
2. CONSIGNES À SUIVRE POUR RÉPONDRE À LA PRÉSENTE LETTRE D'INTÉRÊT .....	4
PARTIE II : SOLUTION MGETFC .....	7
1. CONTEXTE DE LA SOLUTION MGETFC .....	7
2. OBJECTIF DE LA PRÉSENTE LI.....	7
3. EXIGENCES EN MATIÈRE DE SÉCURITÉ.....	7
4. EXCEPTION AU TITRE DE LA SÉCURITÉ NATIONALE .....	8
5. LANGUES OFFICIELLES.....	8
6. APPROCHE EN MATIÈRE D'ENGAGEMENT .....	8
ANNEXE A – BESOIN .....	9
ANNEXE B – EXIGENCES OBLIGATOIRES DE HAUT NIVEAU .....	12
ANNEXE C – APPROCHE DE MAINTIEN EN PUISSANCE .....	17
ANNEXE D – INFORMATION DEMANDÉE À L'INDUSTRIE .....	19

## **OBJET ET CONTENU DE LA PRÉSENTE LETTRE D'INTÉRÊT**

La présente lettre d'intérêt (LI) porte sur le projet Modernisation de la guerre électronique terrestre des Forces canadiennes (MGETFC) pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). L'objet de la présente LI est d'orienter et de préparer l'industrie en vue d'éventuelles possibilités d'approvisionnement concernant le projet MGETFC et de recueillir des commentaires et la contribution en ce qui a trait à la portée, aux exigences, au calendrier, aux risques et aux coûts éventuels du projet. Le contenu général de la présente LI comprend :

**PARTIE I : Processus relatif à la lettre d'intérêt:** Renseignements sur le processus de la LI et la procédure que doit suivre l'industrie pour répondre à la présente LI

## **PARTIE II : Solution MGETFC**

**ANNEXE A :** Besoin du projet MGETFC

**ANNEXE B :** Exigences obligatoires de haut niveau

**ANNEXE C :** Approche du maintien en puissance

**ANNEXE D :** Information demandée à l'industrie

## **PARTIE I: PROCESSUS RELATIF À LA LETTRE D'INTÉRÊT**

### **1. INTRODUCTION**

Le projet de MGETFC en est à la phase précoce d'analyse des options, ce qui signifie que l'analyse de rentabilisation et la justification du projet sont encore en cours d'élaboration. Ainsi, aucune décision sur les concepts, les technologies ou les solutions n'a été prise. L'objectif de la phase d'analyse des options est de s'assurer que les cadres supérieurs du Ministère peuvent prendre une décision éclairée sur la meilleure façon de définir le projet (c.-à-d. mener la phase de définition) et, si cela est jugé approprié, mettre en œuvre le projet afin de réaliser la capacité requise.

L'intention est de mobiliser et de consulter activement l'industrie pendant les phases d'analyse des options et de définition afin d'assurer la réussite du projet. La rétroaction de l'industrie aidera l'équipe de projet du MDN et des FAC à définir ce qui suit:

- a. L'énoncé des besoins (EB) d'une manière compréhensible pour l'industrie et pertinente dans le contexte opérationnel du MDN et des FAC, et ainsi contribuer à bien décrire les besoins opérationnels;
- b. L'« art du possible » concernant les capacités en matière de MGETFC, l'évolution future au sein de l'industrie et la manière dont les grandes entreprises changent pour répondre à leurs besoins informatiques en évolution, ce qui permettra de bien définir l'EB, le budget et le calendrier requis pour atteindre les objectifs du projet (du point de vue technologique et industriel / de l'approvisionnement);
- c. Les répercussions sur les personnes, les processus et la technologie des diverses solutions proposées ainsi que les changements organisationnels qui seront nécessaires à l'appui de chaque solution conceptuelle;
- d. La stratégie d'approvisionnement la plus appropriée qui soit acceptable pour l'industrie pour fournir le bon équipement au MDN et aux FAC en temps opportun, obtenir le meilleur rapport qualité-prix, mettre à profit les achats pour créer des emplois et de la croissance, et simplifier les processus d'approvisionnement.

Le MDN et les FAC ne communiqueront pas avec les fournisseurs à la suite de cette LI. L'autorité contractante présentée à la section 2.7 pourrait communiquer avec l'industrie pour obtenir plus de renseignements à propos des réponses. Toute activité future de mobilisation ou d'approvisionnement de l'industrie sera diffusée publiquement.

#### **1.1 Nature de la présente lettre d'intérêt**

La présente n'est pas une demande de soumissions. La présente LI ne donnera lieu ni à l'attribution d'un contrat ni à la création d'une quelconque liste de fournisseurs. Les fournisseurs éventuels de biens ou de services décrits dans la présente LI ne doivent pas réserver de stocks ou d'installations ni affecter des ressources en fonction des renseignements présentés dans celle-ci. Par conséquent, qu'un fournisseur éventuel réponde ou non à cette LI ne l'empêchera pas de participer à un processus d'approvisionnement ultérieur.

De plus, la présente LI ne mènera pas nécessairement à l'acquisition des biens et services qui y sont décrits. La présente LI vise simplement à obtenir des commentaires de l'industrie sur les éléments qui y sont présentés.

## **2. CONSIGNES À SUIVRE POUR RÉPONDRE À LA PRÉSENTE LETTRE D'INTÉRÊT**

### **2.1 Nature et présentation des réponses demandées**

On rappelle aux répondants que ce document est une LI et non une demande de propositions (DP). Ainsi, les répondants sont invités à livrer leurs commentaires, leurs préoccupations et leurs recommandations quant à la façon dont les exigences ou les objectifs décrits dans cette LI pourraient être satisfaits. Ils devraient prendre soin d'expliquer toute hypothèse énoncée dans leurs réponses.

Les réponses ne seront pas utilisées à des fins d'évaluation compétitive ou comparative, et par conséquent, elles n'ont pas besoin d'être données dans un format aussi rigide que le seraient les réponses à une DP. Toutefois, pour faciliter l'utilisation et pour maximiser la valeur des réponses, le Canada demande que les répondants suivent le format présenté à la section 2.6.

### **2.2 Coûts relatifs aux réponses**

Le Canada ne remboursera aucuns frais engagés par les organismes pour répondre à la présente LI.

### **2.3 Traitement des réponses**

**Utilisation des réponses :** Les réponses ne feront pas l'objet d'une évaluation formelle; le gouvernement du Canada pourra utiliser les réponses reçues afin d'élaborer ou de modifier sa stratégie d'approvisionnement. Le Canada procédera à l'examen de toutes les réponses reçues. Le Canada peut, à sa discrétion, examiner des réponses reçues après la date de clôture de la LI.

**Équipe d'examen :** Une équipe d'examen composée de représentants du MDN et de Services publics et Approvisionnement Canada (SPAC) examinera les réponses. Le Canada se réserve le droit d'embaucher des experts-conseils indépendants ou d'utiliser des ressources du gouvernement du Canada, pour l'examen des réponses, s'il le juge nécessaire. Chaque réponse ne sera pas nécessairement examinée par tous les membres de l'équipe d'examen.

**Confidentialité :** Les répondants devraient indiquer les parties de leur réponse qu'ils considèrent comme étant exclusives ou confidentielles. Le Canada traitera ces réponses, conformément aux exigences de la *Loi sur l'accès à l'information*.

### **2.4 Communication avec l'industrie**

L'autorité contractante peut communiquer avec l'industrie pour obtenir plus de renseignements à propos d'une réponse.

### **2.5 Contenu de la lettre d'intérêt**

Les renseignements contenus dans le présent document évoluent constamment. C'est pourquoi les répondants ne doivent pas perdre de vue que de nouvelles exigences pourraient être ajoutées à toute demande de soumissions que publiera éventuellement le Canada. Les répondants ne doivent pas non plus supposer qu'aucune des exigences ne sera supprimée ou révisée. Les répondants sont donc invités à faire part de leurs commentaires sur tout aspect des exigences. La présente LI contient également des questions précises adressées à l'industrie.

### **2.6 Format de présentation des réponses**

**Page couverture :** si la réponse comprend plusieurs volumes, le répondant doit indiquer, sur la page couverture de chacun des volumes, le titre de la réponse, le numéro de la LI, le numéro du volume ainsi que la dénomination sociale complète du répondant.

**Page titre :** La première page suivant la page couverture devrait être la page titre. Celle-ci doit comporter

les éléments suivants:

- a. Le titre de la réponse et le numéro du volume;
- b. Le nom et l'adresse du répondant;
- c. Le nom, l'adresse et le numéro de téléphone du représentant du répondant;
- d. La date;
- e. Le numéro de la LI.

Nombre de copies : Le Canada demande que les répondants présentent leur réponse en format PDF [en version 2003 ou plus récente] non protégé (c.-à-d. sans mot de passe). Si la taille du document est inférieure à six mégaoctets (Mo), le Canada demande aux répondants de l'envoyer par courriel à [TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca](mailto:TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca). Si la taille du document PDF est égale ou supérieure à 6 Mo, le Canada demande aux répondants d'en enregistrer une copie sur deux clés USB et de les envoyer par la poste à l'agent des contrats dont les coordonnées figurent à la section 2.7.

Les réponses à la présente LI peuvent être rédigées dans l'une ou l'autre des langues officielles du Canada, soit en anglais ou en français.

## 2.7 Demandes de renseignements

Toutes les demandes de renseignements et autres communications relatives à la présente LI doivent être présentées uniquement directement à l'autorité contractante de SPAC. Comme il ne s'agit pas d'une demande de soumissions, le Canada ne répondra pas nécessairement par écrit et ne distribuera pas forcément les réponses à tous les répondants; toutefois, les répondants qui ont des questions concernant la présente LI peuvent les transmettre à:

Autorité contractante : Christine Picknell et Eliane Barnett

Services publics et Approvisionnement Canada  
Place du Portage III, bureau 8C2  
11, rue Laurier  
Gatineau (Québec) K1A 0S5  
Adresse courriel : [TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca](mailto:TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca)

**Veillez inscrire « MGETFC LI » à la ligne d'objet** pour ne pas occasionner de délai dans la réception des réponses.

Le courriel est la méthode de communication de préférence.

## 2.8 Présentation des réponses

**Date et lieu de présentation des réponses** : Les organisations souhaitant fournir une réponse doivent la remettre à l'autorité contractante indiquée à la page 1 de la présente LI, au plus tard à la date et à l'heure de clôture indiquées à la page 1 de la présente demande de soumissions.

La date de clôture de la LI n'est pas la date limite pour présenter des commentaires ou des contributions. Les commentaires et les contributions seront acceptés jusqu'au moment de la publication d'une demande de soumissions, s'il y a lieu.

**Identification de la réponse** : Chaque répondant doit s'assurer que son nom, son adresse et le numéro de la LI figurent lisiblement sur l'enveloppe contenant la réponse si envoyée sur clés USB par la poste.

**Renvoi des réponses :** Les réponses à la présente LI ne seront pas renvoyées.

## **2.9 Surveillant de l'équité**

Si un processus d'approvisionnement de solution MGETFC est enclenché, le Canada retiendra les services d'une organisation qui agira à titre de tiers indépendant comme surveillant de l'équité. Le rôle du surveillant de l'équité consistera à fournir une preuve d'assurance en matière d'équité, d'ouverture et de transparence des activités faisant l'objet de surveillance.

Le surveillant de l'équité devra notamment assumer les responsabilités suivantes:

- a. Surveiller le processus d'approvisionnement en totalité ou en partie (ce qui comprend notamment les processus liés à l'engagement et à la DP prévue);
- b. Faire part de ses commentaires au Canada sur des questions relatives à l'équité;
- c. Prouver l'équité du processus d'approvisionnement.

Veuillez noter que, dans le but d'exécuter ses obligations liées à la surveillance de l'équité, le surveillant de l'équité aura accès aux réponses de l'industrie et à la correspondance connexe reçue par le Canada à la suite de la présente LI. En outre, le surveillant de l'équité peut, à titre d'observateur, assister aux activités éventuelles de suivi en matière d'engagement et de passation de contrats.

## **PARTIE II : SOLUTION MGETFC**

### **1. CONTEXTE DE LA SOLUTION MGETFC**

Les FAC ont besoin d'une capacité de guerre électronique terrestre sous un commandement efficace qui peut détecter des activités et agir à l'intérieur du spectre électromagnétique, en plus d'assurer une protection en protégeant les forces amies contre les menaces électromagnétiques, et qui est durable grâce à des mécanismes adéquats de maintien en puissance.

Ces capacités contribueront à acquérir l'initiative et à surprendre l'ennemi par l'exploitation sélective ou en empêchant l'utilisation du spectre électromagnétique par l'ennemi, afin de comprendre son intention potentielle, de l'empêcher d'avoir une compréhension claire de l'environnement opérationnel, et de s'assurer qu'il ne peut pas nuire aux manœuvres amies au moyen de déclencheurs électromagnétique.

Le projet MGETFC est actuellement à la phase d'analyse des options : l'option de mise en œuvre préférée devrait être déterminée et sélectionnée d'ici l'été 2020. Cette phase sera suivie d'une phase de définition puis d'une phase de mise en œuvre; la capacité opérationnelle initiale est prévue pour juin 2025 et la capacité opérationnelle totale d'ici septembre 2027.

### **2. OBJECTIF DE LA PRÉSENTE LI**

La présente LI est publiée aux fins suivantes:

- a. Consulter l'industrie pour mieux comprendre les possibilités offertes et émergentes en matière de MGETFC d'infrastructure de technologie de l'information commerciale et de solutions de service;
- b. Obtenir des renseignements pour aider le MDN et les FAC à établir leurs besoins et aider au processus interne de planification et d'approbation pouvant mener à une demande de soumissions;
- c. Obtenir des renseignements pour aider le MDN et les FAC à regrouper éventuellement certains des produits livrables, afin qu'un fournisseur ou une équipe de fournisseurs puisse offrir une solution intégrée pour un sous-ensemble cohérent de produits livrables.

La présente LI ne signifie pas que le Canada a pris une décision définitive quant aux possibilités d'approvisionnement. Le MDN et les FAC peuvent décider de ne choisir aucune des solutions ou aucun équipement indiqués dans les réponses. En aucune circonstance, le Canada ne sera tenu responsable à l'égard d'un fournisseur ayant préparé une réponse à la présente LI.

### **3. EXIGENCES EN MATIÈRE DE SÉCURITÉ**

Aucune exigence relative à la sécurité n'est liée à la présente LI.

Toute mesure d'approvisionnement future prise en appui à la solution de MGETFC pourrait exiger que les fournisseurs détiennent une attestation de sécurité de niveau II (secret) et éventuellement une attestation de niveau III (très secret) émise par leur agence de sécurité nationale. Certains des fournisseurs pourraient aussi devoir respecter les exigences du gouvernement du Canada pour fournir des produits et offrir des services assortis de restrictions internationales.



#### **4. EXCEPTION AU TITRE DE LA SÉCURITÉ NATIONALE**

Afin de protéger les intérêts de sécurité nationale, le Canada invoquera son droit en vertu des accords commerciaux nationaux et internationaux d'utiliser une exception au titre de la sécurité nationale (ESN) dans le cadre du présent processus d'approvisionnement. L'ESN permet au Canada de soustraire un processus d'approvisionnement de certaines ou de l'ensemble des obligations d'un accord commercial visé lorsqu'il le juge nécessaire afin de protéger ses intérêts en matière de sécurité nationale ou des intérêts connexes indiqués dans le texte des ESN.

#### **5. LANGUES OFFICIELLES**

Tout marché futur visant une solution de MGETFC pourrait exiger que l'entrepreneur fournisse tous les documents ainsi que le soutien technique et le soutien aux clients dans les deux langues officielles.

#### **6. APPROCHE EN MATIÈRE D'ENGAGEMENT**

##### **6.1 Mobilisation de l'industrie**

Le processus de mobilisation de l'industrie commence avec la présente LI et prendra fin au moment où une demande de renseignements officielle, une DP ou un autre processus concurrentiel sera envoyé aux fournisseurs. Il est envisagé qu'une journée de l'industrie se tiendra à l'été 2019, les dates sont à être déterminées et seront affichées à titre de modification à la présente lettre d'intérêt. Une demande de renseignements plus détaillés suivra le processus de lettre d'intérêt, les réponses à la LI contribueront à l'élaboration de la journée de l'industrie et de la demande de renseignements.

La présente LI est publiée sur <https://achatsetventes.gc.ca/> afin de permettre à l'industrie d'échanger des renseignements avec SPAC et le MDN sur la situation actuelle du marché, les technologies disponibles et les capacités des fournisseurs.

Étant donné que le MDN et les FAC en sont à la phase précoce de l'analyse des options du présent processus d'approvisionnement, l'approche de mobilisation de l'industrie au-delà de la présente phase est toujours en cours d'élaboration.

## **ANNEXE A – BESOIN**

### **Modernisation de la guerre électronique terrestre des Forces canadiennes (MGETFC)**

#### **1. GÉNÉRALITÉS**

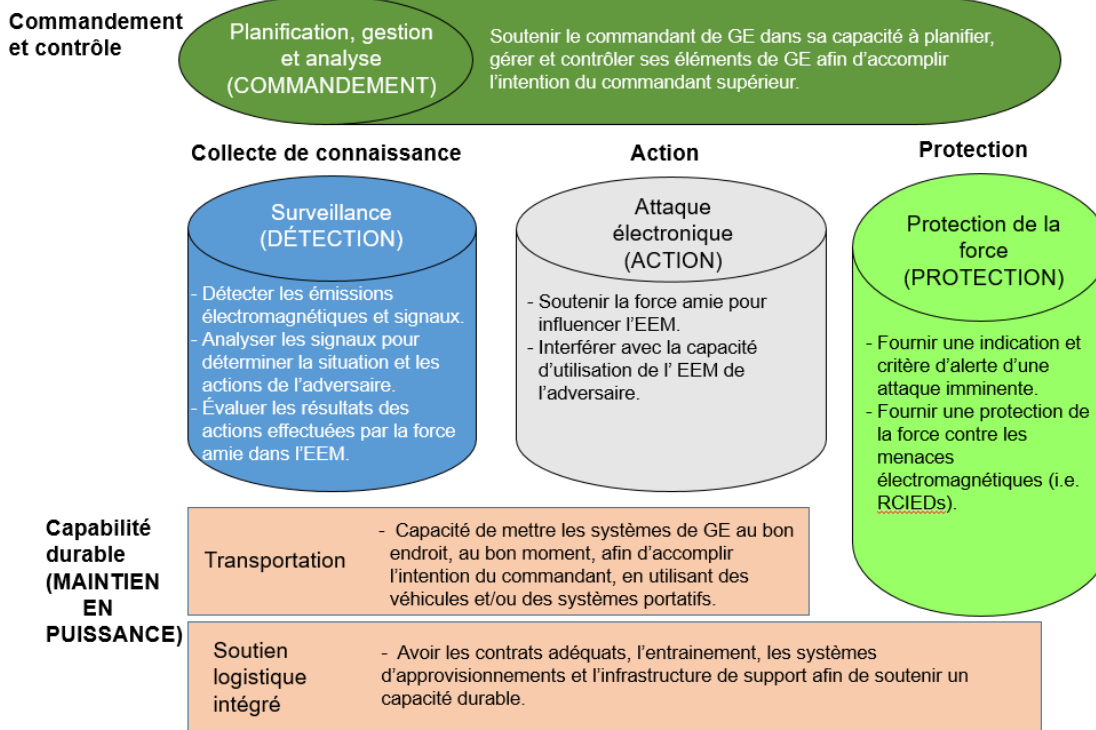
Les Forces armées canadiennes (FAC) doivent acquérir et soutenir les capacités décrites dans le projet de MGETFC et institutionnaliser celles-ci au sein de l'Armée canadienne (AC).

#### **2. CONTEXTE**

Les capacités assurées par le projet de MGETFC joueront un rôle clé dans quatre des huit missions fondamentales indiquées dans Protection, Sécurité, Engagement (PSE). Elles s'ajouteront aux autres systèmes des forces interarmées, terrestres, navales et aériennes des FAC actuellement en place ou qui sont mis en opération. Pour réussir à fonctionner dans l'espace de bataille actuel et futur de l'environnement électromagnétique (EEM), il faut être capable d'intégrer les cinq fonctions opérationnelles que sont le commandement, la détection, l'action, la protection et le maintien en puissance à l'intérieur d'une capacité complète de guerre électronique (GE). Cette capacité réduira l'efficacité des actions des ennemis dans l'EEM en limitant leur capacité d'intervenir et de manœuvrer, tout en préservant simultanément la capacité des FAC de mener des opérations continues. La capacité déployée du projet de MGETFC devra fonctionner dans un EEM très complexe et permettre à un commandant de comprendre l'espace de bataille de l'EEM, d'agir dans cet espace et de le contrôler en assurant une protection contre les menaces électromagnétiques hostiles et en réduisant le plus possible les interférences fratricides avec les systèmes des forces amies. L'option privilégiée consiste à se procurer des systèmes développés (communément appelés articles militaires standards ou «MOTS») qui sont conformes à la liste des exigences obligatoires de haut niveau (EOHN). L'industrie devra fournir les principales composantes du projet de MGETFC et assurer un soutien en service (SES) à long terme pour le système. Par ailleurs, il pourrait s'avérer nécessaire de gérer l'intégration des composantes fournies.

#### **3. PORTÉE DU PROJET**

Le projet de MGETFC combinera des éléments de chacune des cinq fonctions opérationnelles (commandement, détection, action, protection et maintien en puissance) en vue d'obtenir des capacités complètes, comme le montre la Figure 1 ci-dessous.



**Figure 1: Une capacité de guerre électronique complète**

La portée du projet de MGETFC devrait inclure les capacités de système suivantes :

- a) Le système doit être doté d'une capacité de commandement efficace englobant ce qui suit : comprendre l'EEM; importer et exporter des données entre des partenaires des forces stratégiques, interarmées et alliées; assurer une planification, une exécution et un contrôle efficaces des activités de GE et des activités cyber électromagnétiques (ACEM); permettre à la fois des opérations centralisées et réparties; réduire le plus possible les interférences entre les forces amies.
- b) Le système doit aussi détecter les signaux d'intérêt (SI) et faire en sorte que ceux-ci puissent être classifiés, analysés, exploités et situés géographiquement. Cela comprend la capacité d'importer/d'exporter des données au sujet de l'EEM par des échanges avec le système de commandement.
- c) Le système doit être capable d'agir dans l'EEM en permettant l'exécution d'opérations EM non cinétiques offensives, être en mesure d'interférer pour empêcher un usage par l'ennemi du spectre EM, être rattaché à la fonction de détection pour permettre une évaluation des actions amies dans l'EEM et pouvoir être contrôlé à la fois localement par l'opérateur et à distance depuis le système de commandement.
- d) Le système doit être capable de détecter, d'identifier, de cibler, de repérer géographiquement et d'engager (supprimer)<sup>1</sup> simultanément les menaces liées à l'EEM actuelles et nouvelles et de

<sup>1</sup> On peut donner comme exemple de suppression le fait de bloquer le lien entre la personne qui déclenche le dispositif et le déclencheur du dispositif explosif de circonstance télécommandé pour que la probabilité d'une détonation diminue considérablement.

permettre l'importation/l'exportation de données sur l'EEM par des échanges avec le système de commandement.

- e) Le système doit être institutionnalisé afin de respecter la doctrine de l'AC, la formation et le soutien afin d'assurer sa capacité à long terme.
- f) Le système doit soutenir à la fois les opérations embarquées et débarquées.
- g) Le système doit être en mesure d'opérer de concert avec les alliés/partenaires du Groupe des cinq (É.-U., R.-U., Australie et N.-Z.).
- h) Le système doit être suffisamment flexible pour s'adapter aux nouveaux types ou aux nouvelles catégories de signaux et de menaces tout en appuyant la gamme des opérations des forces amies d'une manière contrôlable et dynamique.
- i) Le système doit comprendre un soutien logistique intégré (SLI) et des pièces de rechange.
- j) Un soutien en service (SES) doit être fourni.
- k) Des services de gestion de projet et d'ingénierie doivent être fournis.

Le ministère de la Défense nationale (MDN) peut fournir, en tant qu'équipement fourni par le gouvernement (EFG), toute plateforme de système éventuellement requise pour l'ensemble des variantes de la MGETFC. Les soumissionnaires éventuels doivent tenir compte des coûts du matériel informatique, des logiciels et de l'intégration pour ce qui est de l'équipement propre au projet de MGETFC lorsqu'il est question de fusionner avec de l'EFG.

#### **4. ROLE ET FONCTION**

Le rôle du projet de MGETFC est de fournir une capacité de guerre électronique terrestre sous un commandement efficace qui peut détecter des activités et agir à l'intérieur de l'EEM, y compris la capacité d'interférer avec un usage par l'ennemi de l'EEM, en plus d'assurer une protection en protégeant les forces amies contre les menaces électromagnétiques, et d'être durable grâce à des mécanismes adéquats de maintien en puissance.

#### **5. CONTRAINTES**

Les propositions doivent offrir une capacité entièrement intégrée pour toute la liste des EOHN préliminaires contenues à l'annexe B.

#### **6. EXIGENCES**

Le projet de MGETFC repose sur un ensemble d'exigences relatives au fonctionnement et au rendement de haut niveau. La liste des EOHN préliminaires à laquelle un système proposé doit satisfaire se trouve à l'annexe B.

## **ANNEXE B – EXIGENCES OBLIGATOIRES DE HAUT NIVEAU**

### **Modernisation de la guerre électronique terrestre des Forces canadiennes (MGETFC)**

#### **1. GÉNÉRALITÉS**

Cette annexe contient les exigences obligatoires de haut niveau (EOHN) préliminaires s'appliquant au projet de MGETFC. Pour être retenues, les propositions doivent satisfaire à tous les éléments obligatoires indiqués au paragraphe 2.3.

#### **2. DESCRIPTION DE LA CAPACITÉ**

Les Forces armées canadiennes (FAC) ont besoin d'une capacité de guerre électronique terrestre sous un commandement efficace qui peut détecter des activités et agir à l'intérieur du spectre électromagnétique, en plus d'assurer une protection en protégeant les forces amies contre les menaces électromagnétiques, et qui est durable grâce à des mécanismes adéquats de maintien en puissance.

##### **2.1 But, rôle et emploi**

Le rôle de la capacité livrée par le projet de MGETFC est de permettre à un commandant de l'espace de bataille de manœuvrer à l'intérieur du spectre EM. Cela implique notamment d'assurer une liberté d'action en protégeant les éléments terrestres des FAC contre les menaces EM et en faisant mieux connaître l'EEM afin de permettre l'exploitation au profit des forces amies et d'empêcher les ennemis d'utiliser cet environnement.

Les opérations modernes se déroulent à un rythme soutenu et sont très complexes. Par ailleurs, il s'agit presque toujours d'opérations interarmées et/ou multinationales. Ainsi, il est essentiel d'instaurer et de préserver une connaissance de la situation chez le commandant afin que ses manœuvres à l'intérieur de l'EEM soient aussi flexibles que possible. Le projet de MGETFC offrira une capacité exhaustive très efficace englobant les cinq fonctions opérationnelles : commandement, détection, action, protection et maintien en puissance. Voilà qui viendra renforcer considérablement la capacité du commandant d'utiliser l'EEM et de contribuer au commandement et au contrôle efficace de ses forces.

La nouvelle capacité de GE de l'Armée canadienne peut être déployée dans différents types de missions couvrant le spectre de conflits – des engagements militaires en temps de paix aux opérations de combat d'envergure. Le Canada est un partenaire international actif; cela signifie que cette capacité sera souvent mise en application au sein de contextes de coalition. Il sera donc essentiel que cette nouvelle capacité soit souple afin qu'elle puisse être interopérable avec les principaux partenaires du Groupe des cinq.

##### **2.2 Organisation**

La structure organisationnelle utilisée pour la capacité de PROTECTION se fondera sur la taille des unités déployées, conformément à PSE. Les capacités de COMMANDEMENT, de DÉTECTION et d'ACTION dépendront de nos unités existantes de GE. La version finale de la future structure organisationnelle qui sera soutenue par le projet de MGETFC est en cours d'élaboration et sera définie par les groupes de travail actuels de Force 2021.

##### **2.3 Exigences obligatoires de haut niveau (EOHN)**

Chaque EOHN compte une description servant d'introduction, suivie des exigences détaillées.

### **2.3.1 Commandement de GE**

#### **2.3.1.1 Comprendre l'EEM**

Le système de commandement doit être en mesure d'intégrer toutes les données internes et externes relatives à la GE et aux activités cyber électromagnétiques (ACEM) et d'afficher une image commune de la situation opérationnelle (ICSO) du spectre visuel qui pourra être comprise par le personnel de commandement et le personnel d'état-major, après avoir suivi une formation minimale.

#### **2.3.1.2 Exporter et importer les données**

Le système de commandement doit être capable d'exporter et d'importer des données sur la GE/les ACEM par des échanges avec les partenaires des forces stratégiques, interarmées et alliées dans un ou plusieurs formats que ces partenaires peuvent utiliser.

#### **2.3.1.3 Planifier les opérations de GE**

Le système de commandement doit permettre la planification des opérations de GE à l'aide de l'ICSO et d'autres outils qui peuvent créer des produits dans des formats militaires standards. Ces produits seront exportés dans les systèmes suivants : systèmes de détection, d'action et de protection; systèmes de soutien du commandement interarmes en service.

#### **2.3.1.4 Exécuter et contrôler les opérations de GE**

Le système de commandement doit permettre l'exécution des opérations de GE au moyen d'une combinaison de processus automatisés, centralisés et répartis.

#### **2.3.1.5 Analyser l'interférence avec les forces amies**

Le système de commandement doit être capable de déterminer/quantifier le risque que les opérations de GE interfèrent avec les systèmes des forces amies.

### **2.3.2 Détection des activités de GE**

#### **2.3.2.1 Détecter les signaux d'intérêt (SI)**

La capacité de détection doit fonctionner à l'intérieur de la plage de fréquences indiquée et selon les types de signaux et les protocoles définis pour pouvoir détecter les SI.

#### **2.3.2.2 Catégoriser les SI**

Le système de détection doit être capable de catégoriser les SI en déterminant les caractéristiques générales des signaux et doit pouvoir importer/exporter des données au moyen d'échanges avec le système de commandement.

#### **2.3.2.3 Analyser les SI**

Le système de détection doit être capable d'effectuer une analyse détaillée des SI afin d'exploiter davantage les signaux et doit pouvoir importer/exporter des données au moyen d'échanges avec le système de commandement.

#### **2.3.2.4 Exploiter les SI**

Le système de détection doit comporter des outils permettant d'exploiter les SI afin de

développer des produits de renseignement et de pouvoir importer/exporter des données au moyen d'échanges avec le système de commandement.

#### **2.3.2.5 Situer géographiquement les SI**

Le système de détection doit être capable de repérer géographiquement les SI à l'interne/l'externe en travaillant en collaboration et pouvoir importer/exporter les données de localisation au moyen du système de commandement.

#### **2.3.2.6 Sonder l'EEM**

Le système de détection doit être capable de développer une connaissance générale de l'EEM et pouvoir importer/exporter les données de l'EEM au moyen du système de commandement.

#### **2.3.2.7 Enregistrer les SI**

Le système de détection doit être capable d'enregistrer les SI en vue d'une analyse plus approfondie.

### **2.3.3 Action relative à la GE**

#### **2.3.3.1 Exécuter des actions non cinétiques**

Le système d'action doit être capable d'exécuter des ACEM non cinétiques offensives.

#### **2.3.3.2 Cibler un usage de l'EEM par l'ennemi**

Le système d'action doit pouvoir fonctionner à l'intérieur d'une plage de fréquences, de niveaux de puissance, de types et protocoles de signaux de systèmes ennemis afin de pouvoir interférer avec leur utilisation de l'EEM.

#### **2.3.3.3 Interopérabilité du système**

Le système d'action doit être configurable afin de réduire le plus possible les effets et les interférences nuisibles relativement à d'autres systèmes électroniques nationaux et alliés (p. ex. commandement, contrôle, communication, informatique, renseignement, surveillance et reconnaissance; systèmes de lutte contre les véhicules aériens sans pilote; systèmes alliés; vétronique des véhicules).

#### **2.3.3.4 Contrôle du système d'action**

Le système d'action doit pouvoir être contrôlé, de façon autonome, à l'échelle locale par l'opérateur et à distance par le système de commandement.

#### **2.3.3.5 Configuration du système d'action**

Le système d'action doit être configurable afin que l'on puisse contrer les menaces nouvelles ou en évolution au moyen de logiciels et d'outils de développement pouvant être acquis qui permettront l'élaboration rapide de nouveaux fichiers de configuration.

### **2.3.4. Protection dans le cadre de la GE**

#### **2.3.4.1 Contrôle du système de protection**

Le système de protection doit pouvoir être contrôlé, de façon autonome, à l'échelle locale

par l'opérateur et à distance par le système de commandement.

#### **2.3.4.2 Détection des menaces relatives à l'EM**

Le système de protection doit permettre la détection de l'EEM et identifier les dispositifs représentant une menace, comme les déclencheurs des dispositifs explosifs de circonstance télécommandés.

#### **2.3.4.3 Ciblage de menaces EM**

Le système de protection doit pouvoir fonctionner à l'intérieur de la plage de fréquences et selon les types de signaux des déclencheurs de menace pour être en mesure de cibler les dispositifs.

#### **2.3.4.4 Localisation géographique**

Le système de protection doit pouvoir localiser géographiquement, en collaboration interne et externe, le signal du dispositif constituant une menace et pouvoir importer / exporter les données de localisation vers le système de commandement.

#### **2.3.4.5 Suppression des menaces de l'EEM**

Le système de protection doit permettre le blocage du lien entre les dispositifs représentant une menace pour l'EEM et réduire considérablement la probabilité que ces dispositifs soient utilisés comme prévu en gardant une distance sécuritaire minimum.

#### **2.3.4.6 Enregistrement de l'EEM**

Le système de protection doit être en mesure d'analyser et d'évaluer l'EEM de façon autonome, à l'échelle locale par l'opérateur et à distance par le système de commandement, afin de faciliter l'identification des changements apportés aux dispositifs représentant une menace et/ou aux tactiques, aux techniques et aux procédures de l'ennemi au moyen de registres et d'enregistrements.

#### **2.3.4.7 Interopérabilité du système de protection**

Le système de protection doit être configurable afin que l'on puisse minimiser les interférences nuisibles avec les autres systèmes électroniques.

#### **2.3.4.8 Configuration du système de protection**

Le système de protection doit être configurable afin que l'on puisse contrer les signaux de menaces EM nouveaux ou en évolution au moyen de logiciels et d'outils de développement pouvant être acquis, qui permettront l'élaboration rapide de nouveaux fichiers de configuration

### **2.3.5 Maintien en puissance dans la cadre de la GE**

#### **2.3.5.1 Formation**

La capacité doit être en mesure de soutenir la formation individuelle et d'opérer de concert avec les systèmes de formation collective (p. ex. simulation).

#### **2.3.5.2 Le soutien aux opérations**

La capacité doit être capable d'appuyer à la fois les opérations embarquées et débarquées



de manière intégrée.

#### **2.3.5.3 Soutien en service**

La capacité doit inclure des contrats de soutien en service comprenant un SLI, un soutien à la formation et un soutien d'ingénierie.

### **2.3.6 Commun**

#### **2.3.6.1 Compatibilité**

La capacité doit être en mesure de fonctionner dans un contexte de coalition en permettant l'échange de données sur la GE avec les partenaires du Groupe des cinq.

#### **2.3.6.2 Flexibilité**

Le système doit être capable de fonctionner dans un large éventail d'environnements de déploiement et d'emplacements et en fonction des types de signaux de menaces en changeant les bandes de fréquence, les niveaux de puissance et les fichiers de configuration en temps voulu.

## **ANNEXE C – APPROCHE DE MAINTIEN EN PUISSANCE**

### **Modernisation de la guerre électronique terrestre des Forces canadiennes (MGETFC)**

#### **1. GÉNÉRAL**

Le concept global de soutien en service misera sur une première période de soutien provisoire immédiatement suivie d'une période de soutien en service (SES) à long terme. Selon ce qui est prévu, le besoin en matière de soutien en service fera l'objet d'un processus concurrentiel en même temps que le besoin en matière d'acquisition.

#### **2. BESOIN PRÉLIMINAIRE EN MATIÈRE DE SOUTIEN EN SERVICE (SES)**

Le concept de SES du MGETFC est présentement en cours d'élaboration. Toutefois, certaines hypothèses peuvent être formulées concernant la forme et la fonction du concept de soutien en service :

- 2.1 Le concept de SES appuiera une conception d'équipement complexe. La conception des systèmes de MGETFC regroupera probablement de nombreux types d'équipement sur de multiples plateformes de véhicules, plateformes statiques et configurations portatives.
- 2.2 Le concept de SES viendra appuyer à la fois l'équipement matériel et les systèmes logiciels. Le projet de MGETFC comportera aussi un système Commandement, Contrôle et Visualisation propre à la guerre électronique (GE) qui devra faire l'objet de travaux de maintenance, de mise à niveau et d'amélioration tout au long de la durée de vie du système. Par ailleurs, chacune des configurations d'équipement et de plateforme sera probablement dotée d'interfaces utilisateurs graphiques spécifiques, de systèmes de contrôle, de systèmes de gestion des données accessoires et de systèmes d'intelligence artificielle spécifiques qui devront également faire l'objet de travaux de maintenance, de mise à niveau et d'amélioration. En outre, le matériel physique sous diverses formes et à différents niveaux de complexité nécessitera des opérations de maintenance, de mise à niveau et de remplacement.
- 2.3 Le concept de SES doit appuyer les opérations déployées. Bon nombre des systèmes de MGETFC seront orientés vers l'ennemi et seront utilisés de manière expéditionnaire. Par conséquent, le concept de SES doit s'accompagner de processus de maintien en puissance qui fonctionneront dans un contexte expéditionnaire.
- 2.4 Le concept de SES doit soutenir de l'équipement distribué dans l'ensemble de l'Armée canadienne (AC). Une partie de l'équipement et des systèmes du projet de MGETFC sera probablement distribuée à des unités autres que les unités de GE. Par conséquent, le SES doit desservir des utilisateurs qui ne possèdent pas de compétences techniques et qui sont géographiquement dispersés.

#### **3. BUT**

L'objectif de la présente annexe est de présenter le concept préliminaire de SES de la MGETFC afin d'aider les répondants à donner une rétroaction sur les besoins et les stratégies en matière de soutien en service à long terme.

#### **4. PORTÉE**

Le SES MGETFC est fondé sur le rendement et sur des incitatifs, et permet à la Couronne d'aller chercher un soutien en service à long terme dans les domaines suivants :

- 4.1 Gestion générale du programme;

- 4.2 Soutien d'ingénierie;
- 4.3 Soutien de l'approvisionnement;
- 4.4 Services techniques du parc de véhicules;
- 4.5 Gestion de l'information et des données;
- 4.6 Amélioration et gestion des logiciels; and
- 4.7 Développement et gestion des formes d'ondes;

## **5. CADRE DU CONCEPT DE SES**

Quoique le concept de SES MGETFC soit en cours de développement, les composantes du système incluront fort probablement, entre autres, les éléments suivants :

- 5.1 un ou plusieurs besoins en matière de maintien en puissance pour ce qui est des logiciels;
- 5.2 un ou plusieurs besoins en matière de maintien en puissance pour ce qui est du matériel informatique;
- 5.3 un ou plusieurs besoins en matière d'intégration du matériel informatique/des plateformes;
- 5.4 un ou plusieurs besoins en matière d'intégration des logiciels/du matériel informatique; and
- 5.5 un ou plusieurs besoins en matière de compatibilité et d'intégration des logiciels.

## **ANNEXE D – INFORMATION DEMANDÉE À L'INDUSTRIE**

### **Modernisation de la guerre électronique terrestre des Forces canadiennes (MGETFC)**

#### **1. GÉNÉRAL**

Cette LI est la première étape pour mobiliser l'industrie dans un processus de partage d'information itératif dans le cadre du développement d'une demande d'information. Les répondants potentiels sont encouragés à être innovant dans leurs méthodes de livraison de la capacité et options de soutien proposées.

#### **2. INFORMATION DEMANDÉE**

Basée sur les besoins détaillés dans ce document, cette LI a pour intention d'obtenir de l'industrie les informations suivantes:

- 2.1. Quelles solutions votre entreprise propose-t-elle pour aider le MDN à concrétiser les fonctionnalités présentées dans le concept MGETFC décrit à l'annexe A?
- 2.2. Fournir des commentaires en ce qui concerne la faisabilité de chaque EOHN détaillées à l'annexe B.
- 2.3. Si votre entreprise n'est pas en mesure de fournir la capacité en entier, fournir un plan qui inclut d'autres compagnies avec lesquelles elle pourrait potentiellement s'associer afin d'adresser toutes les EOHN.
- 2.4. Fournir une description technique de la solution proposée avec un énoncé de la capacité, illustrant comment la solution proposée peut atteindre les EOHN détaillées à l'annexe B.
- 2.5. Fournir tous détails disponibles sur la maturité de la solution proposée (i.e. niveau de préparation technologique, en service, etc.).
- 2.6. Optionnellement, fournir un estimé approximatif des coûts par composante listée dans l'annexe A, paragraphe 3, Portée du projet.

#### **3. MAINTIEN EN PUISSANCE**

Cette LI a pour but d'obtenir des suggestions des entreprises sur le maintien en puissance tel que décrit ci-dessous :

- 3.1. Fournir des suggestions sur comment la capacité peut être soutenue à travers son cycle de vie.
- 3.2. Fournir une rétroaction sur le maintien en puissance de la capacité tel que décrit dans l'annexe C.
- 3.3. Comment votre entreprise estime la durée de vie de la capacité?

#### **4. POLITIQUE DES RETOMBÉES INDUSTRIELLES ET TECHNOLOGIQUES (ITB)**

##### **4.1. Application de la politique des retombées industrielles et technologiques**

La politique des retombées industrielles et technologiques (RIT), y compris la proposition de valeur,

s'appliquera possiblement au projet de MGETFC. L'engagement pris au moyen de la lettre d'intérêt (LI) aidera à déterminer l'applicabilité de la politique des RIT et la façon dont le Canada peut recourir à ce marché pour en tirer un avantage économique.

#### **4.2. La politique des RIT, y compris la proposition de valeur (PV)**

La politique des RIT est un outil puissant qui sert à attirer des investissements. Les entreprises qui concluent des marchés d'approvisionnement en matière de défense sont tenues de mener des activités commerciales au Canada dont la valeur équivaut à celle du marché. La politique des RIT encourage les entreprises à s'établir au Canada ou à y accroître leur présence, à renforcer leurs chaînes d'approvisionnement au pays et à développer des capacités industrielles canadiennes.

La politique des RIT vise à soutenir la viabilité à long terme et la croissance du secteur de la défense du Canada, y compris les petites et moyennes entreprises de partout au pays, à stimuler l'innovation au Canada au moyen de la R-D, à soutenir le perfectionnement des compétences et la formation ainsi qu'à accroître le potentiel d'exportation des entreprises établies au Canada. 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 soumissionnaires 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.

Pour de plus amples renseignements sur la politique des RIT, visitez la page <http://www.canada.ca/rit>.

##### **4.2.1. Capacités industrielles clés**

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 du secteur de la défense à investir dans les Capacités industrielles clés (CIC). Les CIC s'harmonisent avec la politique de défense du Canada, Protection, Sécurité, Engagement, et le Plan pour l'innovation et les compétences en soutenant le développement des compétences et en favorisant l'innovation dans le secteur de la défense du Canada. Les CIC sont liées à des domaines de technologies émergentes qui présentent un potentiel de croissance rapide et des débouchés importants, à des capacités établies par rapport auxquelles le Canada est concurrentiel à l'échelle mondiale et à des domaines où la capacité nationale est essentielle à la sécurité du pays.

Le gouvernement a déterminé que cet approvisionnement nécessite des capacités dans les domaines de la **Cyberrésilience**, de **l'intégration des systèmes de défense** et de **l'intelligence artificielle**.

Comme il s'agit de compétences principales canadiennes, le Canada cherchera à stimuler les possibilités de grande valeur économique et les partenariats qui soutiennent la croissance de son secteur de la défense, ainsi qu'à accroître la participation à la chaîne d'approvisionnement et à développer les compétences et la formation pour l'industrie canadienne.

Voici les définitions des CIC concernées par ce projet:

##### ***Cyberrésilience***

La cyberrésilience couvre tous les aspects des secteurs de la sécurité nationale, civile et commerciale et pallie les vulnérabilités créées par l'expansion de la technologie de l'information et de l'économie du savoir. La cyberrésilience comporte des activités de conception, d'intégration et de mise en œuvre de solutions technologiques qui protègent l'information et les réseaux de communication. Ces technologies, parmi d'autres, doivent être axées sur le développement efficace des capacités en cybersécurité suivantes:

##### ***Sécurité de l'information***

La protection des données et des renseignements électroniques et numériques contre l'accès et

toute intrusion, l'utilisation, la divulgation, la perturbation, la modification, la consultation, l'inspection, l'enregistrement ou la destruction non autorisé;

### ***Sécurité informatique***

La sécurisation du contenu et la gestion des menaces (point terminal, messagerie, réseaux, Web, nuage), sécurité, gestion des vulnérabilités et des risques, gestion de l'identité et de l'accès et autres produits, (p. ex., des trousse de chiffrement et de gestion des jetons et des essais de vérification de produits de sécurité), ainsi que des services d'éducation, de formation et de connaissance de la situation;

### ***Sécurité des technologies opérationnelles***

La surveillance, mesure et protection des systèmes d'automatisation et de contrôle des processus industriels et connexes. La cyberrésilience peut comprendre la création d'outils et l'intégration de systèmes et de processus qui renforcent la sécurité des systèmes tactiques ou des grands réseaux, le chiffrement, la cyber-expertise et les interventions en cas d'incident, entre autres. Les capacités établies dans ce domaine pourraient s'appuyer de plus en plus sur l'IA à titre de technologie habilitante. Ainsi, des réseaux feraient usage de leurs défenses de façon autonome et dynamique contre les intrusions et se répareraient eux-mêmes après une perturbation.

### ***Intégration des systèmes de défense***

Conception et intégration de systèmes militaires complexes qui dépendent de l'intégration harmonieuse de multiples sous-systèmes pour fournir une capacité opérationnelle efficace. Ces capacités couvrent diverses plateformes militaires et permettent l'exploitation et la gestion d'armes, de systèmes de défense, de systèmes de commande et de contrôle, de capteurs, de systèmes d'appui à la prise de décision, des dispositifs de guerre électronique et des sous-systèmes de base des plateformes d'une manière hautement coordonnée qui est essentielle dans des conditions de combat très exigeantes. Ces systèmes doivent présenter de façon compréhensible et sûre l'information provenant de multiples sources aux opérateurs et appuyer la prise de décisions dans un environnement complexe. Cette définition ne vise pas les divers systèmes constitutifs (systèmes de lancement de missiles, radars, systèmes de guerre électronique, etc.) à intégrer dans un ensemble cohérent, mais vise plutôt les compétences et les capacités nécessaires pour réaliser l'intégration et créer l'interface utilisateur requise dans des systèmes complexes destinés aux missions.

### ***Intelligence artificielle***

L'intelligence artificielle, ou IA, couvre un éventail de technologies qui permettent à des machines de réaliser des tâches qui nécessitent habituellement l'intelligence humaine, telles que la reconnaissance des formes et de la parole, la traduction, la perception visuelle et la prise de décisions. L'IA s'appuie sur diverses disciplines, comme les algorithmes de recherche et l'optimisation mathématique, l'apprentissage machine, l'apprentissage approfondi, l'autoapprentissage et les réseaux neuronaux, en plus d'étendre les connaissances qui s'y rattachent. Elle allège la charge de travail des utilisateurs et automatise les tâches facilement répétables où ils doivent intervenir. L'IA permet d'envisager un meilleur rendement du personnel formé, de soustraire celui-ci à des environnements dangereux et de s'adapter plus rapidement aux changements dans l'environnement opérationnel militaire. Elle simplifie également de nombreuses activités, telles que l'analyse de quantités massives de données à l'appui du renseignement, de la planification des missions, de l'entraînement connexe, de la logistique, de la gestion opérationnelle, de la cybersécurité et de la cyberrésilience. L'intelligence artificielle a sa place dans de nombreux domaines liés à la défense et d'autres secteurs.

### **4.3. Secteur de la défense**

La Politique des RIT vise à promouvoir le développement économique et la viabilité à long terme des entreprises canadiennes chargées de la fabrication et de la prestation de produits et de services utilisés dans les applications de défense et de sécurité du gouvernement.

- 4.3.1. Veuillez décrire les activités de production ou les activités de service que votre société exerce dans les CIC de la cyber-résilience, de l'intégration des systèmes de défense et de l'intelligence artificielle. Veuillez indiquer quelles activités sont actuellement menées au Canada.
- 4.3.2. En vous basant sur les exigences obligatoires de haut niveau établies par le ministère de la Défense nationale, décrivez les travaux directs que votre entreprise prévoit entreprendre au Canada relativement à la production et à la maintenance du système MGETFC? Quelles sont les opportunités et les contraintes afin d'effectuer ce travail au Canada?

### **4.4. Développement des sources d'approvisionnement**

La Politique des RIT vise à améliorer la compétitivité de l'industrie canadienne en encourageant sa participation et en intensifiant la présence d'entreprises, y compris les petites et moyennes entreprises (PME).

- 4.4.1. À l'heure actuelle, dans quels secteurs de production et de prestation de services votre entreprise travaille-t-elle avec des PME canadiennes et quelle est la nature de la contribution de ces PME?
- 4.4.2. Quelles sont les opportunités et les contraintes pour les PME canadiennes de fournir des solutions au système MGETFC?

### **4.5. Développement des compétences et formation**

La Politique des RIT encourage le développement et le maintien d'une main-d'œuvre canadienne talentueuse, novatrice et caractérisée par une forte diversité par l'accès à la formation, à l'enseignement, aux occasions et aux programmes.

Exemples d'activités de développement des compétences et formation:

- a. les programmes en milieu de travail (p. ex. stages coop, placements professionnels);
  - b. les programmes d'apprentissage;
  - c. un nouveau programme ou un programme actuel de développement des connaissances d'un établissement postsecondaire;
  - d. la prise en charge des attestations de sécurité (p. ex. Très secret, ITAR) et des attestations de conformité à la cybersécurité pour les sociétés canadiennes, en particulier les petites et moyennes entreprises.
- 4.5.1. Quelles activités de développement des compétences et de formation votre entreprise offre-t-elle actuellement, et serait-il possible d'en étendre la portée aux Canadiens travaillant dans les CIC de la cyber-résilience, de l'intégration des systèmes de défense et de l'intelligence artificielle?
  - 4.5.2. Sur le plan du développement des compétences et de la formation, quelles difficultés votre entreprise entrevoit-elle relativement aux les CIC de la cyber-résilience, de l'intégration des systèmes de défense et de l'intelligence artificielle et comment votre entreprise cherche-t-elle à surmonter ces difficultés?

#### **4.6. Recherche et développement (R-D)**

La Politique des RIT encourage la recherche scientifique qui explore le développement de nouveaux biens et services, de nouveaux intrants à la production et de nouvelles méthodes de production des biens et services, ou de nouvelles façons d'exploiter et gérer des organisations.

- 4.6.1. Quels sont les secteurs prioritaires d'investissement en R-D de votre entreprise? Dans quelle mesure ces secteurs prioritaires sont-ils reliés dans les CIC de la cyber-résilience, de l'intégration des systèmes de défense et de l'intelligence artificielle?
- 4.6.2. Reconnaissant le rôle que jouent les établissements d'enseignement postsecondaire et les instituts de recherche publics dans la promotion de l'innovation au Canada, veuillez décrire les possibilités que votre entreprise envisage d'exercer au Canada avec ces organisations et les domaines de recherche spécifiques que vous poursuivriez.

#### **4.7. Exportation**

La Politique des RIT favorise la capacité des entreprises canadiennes, y compris les PME, à exploiter avec succès les marchés d'exportation, augmentant ainsi leur productivité et leur compétitivité sur le marché mondial.

- 4.7.1. Quel rôle l'approvisionnement en MGETFC joue-t-il dans le positionnement de votre entreprise et de sa chaîne d'approvisionnement canadienne en vue d'une croissance à long terme?
- 4.7.2. Dans quelle mesure pouvez-vous intégrer des entreprises canadiennes dans votre chaîne d'approvisionnement?
- 4.7.3. Dans quelle mesure des occasions existent-elles dans les CIC de la cyber-résilience, de l'intégration des systèmes de défense et de l'intelligence artificielle?
- 4.7.4. Est-il réalisable d'obtenir assez de droits de propriété intellectuelle et un mandat de production mondiale exclusif vous permettant d'exporter à partir d'entités exerçant des activités au Canada, y compris les filiales et les partenaires de la chaîne d'approvisionnement?
- 4.7.5. Veuillez décrire les difficultés ou contraintes rencontrées par la société dans le partage de la propriété intellectuelle avec des partenaires et des fournisseurs canadiens?

#### **4.8. Autres questions**

Y a-t-il d'autres CIC pertinentes dans le cadre du travail qui sera mené pour le projet MGETFC? Si oui, indiquez les CIC qui devraient être envisagées et la raison pour laquelle elles devraient l'être. Dans votre réponse, décrivez également la façon dont les CIC proposées accroîtraient les avantages de la proposition de valeur pour l'industrie canadienne.

### **5. EXPERIENCE**

Quelle est l'expérience de votre compagnie en ce qui concerne le support de besoins militaires?

- 5.1. Est-ce que votre entreprise a travaillé sur la livraison de besoins militaires auparavant?
- 5.2. Quelle expérience votre entreprise a en ce qui concerne la livraison ou le soutien de capacités de GE dans un contexte militaire?
- 5.3. Quelle expérience a votre entreprise en ce qui concerne le support à l'accès aux établissements militaires?



- 5.4. Est-ce que votre entreprise a de l'expérience avec le processus d'Évaluation et autorisation de sécurité (E&SA) ?

**6. FACTEURS ADDITIONNELS**

- 6.1. Quels facteurs additionnels devraient être considérés par le MDN dans le développement de la capacité?
- 6.2. Quelle est votre solution pour adresser ces facteurs?
- 6.3. Selon votre expérience, quels risques devraient être considérés lors de l'implémentation de la capacité?
- 6.4. Quelle est votre solution pour atténuer ces risques?

**7. MODÈLE DE RÉPONSE**

Les répondants peuvent utiliser le format qui leur convient afin de fournir l'information requise. Chacune des questions ci-dessus doit avoir une réponse ou une explication des raisons pour lesquelles une réponse n'est pas possible à ce moment.