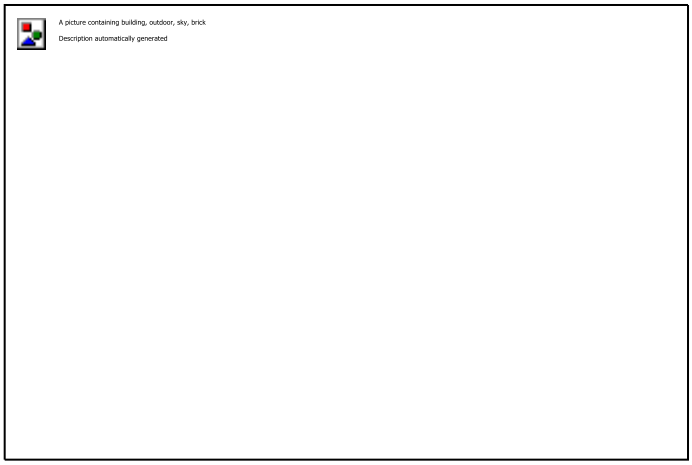
National Defence / Défense nationale

Canadian Forces College / Collège des Forces Canadiennes




# LES FAC DISPERSÉES ET LEURS TECHNOLOGIES DE L'INFORMATION NON CENTRALISÉES EN TEMPS DE PANDÉMIE

**Major Jean-Pierre Lapointe**

**JCSP 45**

**Solo Flight**

**Disclaimer**

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.



**PCEMI 45**

**Solo Flight**

**Avertissement**

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.



Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
2018 – 2020

SOLO FLIGHT

# LES FAC DISPERSÉES ET LEURS TECHNOLOGIES DE L'INFORMATION NON CENTRALISÉES EN TEMPS DE PANDÉMIE

**Major Jean-Pierre Lapointe**

## Table des matières

**Les FAC dispersées et leurs technologies de l'information non centralisées en temps de pandémie**

## Introduction

Au cours du présent essaie persuasif, je démontrerai que les FAC ne possèdent pas d'infrastructure de technologie de l'information (TI), de communication, de commandement et de contrôle leur permettant d'être efficaces au travail lorsque la vaste majorité de ses membres sont dispersés. Ceci est devenu apparent lors de l'avènement de la pandémie du COVID 19. En effet, Les FAC sont ancrées dans un modèle de travail traditionnel et obsolète axé sur une doctrine de TI centralisée basé sur des solutions et des technologies dépassées et insuffisantes qui devront s'adapter à l'époque actuelle. Ainsi, les lieux de travail organisationnels sont centralisés et le modèle de support des systèmes d'information et de communication (SIC) est lui aussi centralisé et non dispersé. En temps de pandémie, cette absence de moyens de communication adéquats force les membres des FAC et leur chaîne de commandement à être ingénieux ce qui n'est pas sans risque pour notre organisation. De ce fait, la mise en place de structures technologiques et cybernétiques capables de supporter une dispersion des membres des FAC est plus que nécessaire, ce qui de surcroit permettrait aussi de limiter les risques de fuite d'information et attaques cybernétiques sur les SIC et les membres des FAC.

Afin de démontrer ceci, je concentrerai mon analyse sous la lentille des aspects technologiques et le domaine du cyberespace liés aux systèmes non classifiés et protégés dans les contextes de travail avant et pendant la pandémie du COVID 19.

Les éléments de thèse suivants seront étudiés :

- La chronologie des événements démontre un état de préparation lamentable. Cette problématique force une improvisation et une adaptation risquée et discutable.
- La doctrine des FAC liée aux SIC ainsi que le modèle de travail actuel est fortement dépendant sur les équipements informatiques est fortement

centralisé selon une conceptualisation organisationnelle et structurelle. La dispersion totale devient alors impossible.

- Les besoins en échange d'information (BECI) et Besoins en support d'information (BESI i.e. services essentiels) ne rencontrent pas les besoins de la chaîne de commandement. Des moyens ad hoc sont mis en place afin de pallier ces lacunes.
- Il existe des défis supplémentaires relativement au travail dispersé et au télétravail lorsque non encadré et non proprement supporté. Ainsi, la sécurité informatique, la sécurité de l'information et les acteurs cybernétiques forment une triade du malheur. De plus, certaines technologies sont déjà utilisées par d'autres départements supportés par SPC mais le MDN n'y a pas adhéré. Pourquoi ?

**Chronologie des événements, préparation et pandémie**

L'analyse de la chronologie des évènements menant à la pandémie démontre un état de préparation lamentable du point de vue des SIC et de la capacité des FAC à opérer efficacement en mode de télétravail dispersé. Avant d'aller de l'avant, il importe de bien décrire cette capacité.

**Description de base du réseau étendu de la défense (RÉD) :**

Le RÉD actuel ne permets pas la dispersion. Ce réseau non classifié permet l'échange d'information pouvant aller jusqu'à protégé B et demeure la suite d'outils informatiques principale qui est utilisée par les FAC pour effectuer leur travail quotidien. Il est déployé dans tous les lieux de travail et les organisations des FAC. Il existe un moyen de se connecter à distance avec un ordinateur portable. Cette capacité se nomme « *infrastructure du réseau privé virtuel de la Défense – Transparente (IRPVD-T)* ». Ainsi, l'infrastructure déployée et statique partagent les mêmes points d'accès de connexion qui se servent de l'infrastructure de GPNET comme point d'entrée :

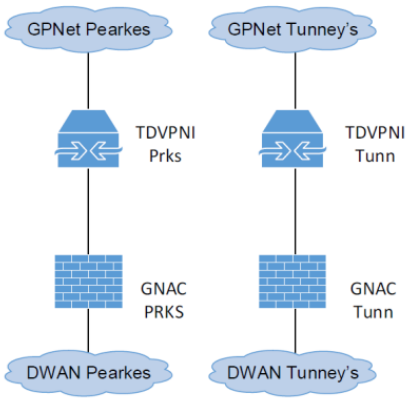



**Figure 1: Infrastructure actuelle de IRPVD-D (haut niveau)**

Afin de pouvoir accéder au IRPVD-D, l'usager doit posséder les éléments suivants :

- Un terminal du RÉD.
- Une connexion à Internet.
- Un lecteur de carte *Entrust*.
- Une carte *Entrust*. Cette solution d'authentification dite matérielle, se nomme Public Key Infrastructure (PKI) et permets d'accéder à l'infrastructure du RÉD au moyen de l'IRPVD-T. Il s'agit d'une authentification à deux facteurs[1] puisque l'usager s'authentifiera sur sa station en entrant son nom d'usager et son mot de passe (quelque chose qu'il connait) et devra par la suite utiliser sa carte (quelque chose qu'il possède (sa carte *Entrust* PKI)).

La prémisse de base est donc la suivante : Pour qu'un membre des FAC puisse accéder au RÉD à distance, il doit avoir toutes ces composantes comme préalable essentiel.

**Phase de préparation et d'Alerte de Op LASER**:

La première phase s'est résumée à la planification de l'atténuation et la surveillance normale des menaces pandémiques à l'échelle mondiale. Elle est considérée comme toujours active sauf si l'on passe à une phase supérieure[2]. La phase 2 consiste en un suivi actif de l'évolution de la menace pandémique et à l'adoption de certaines

[1] Site web de Entrust, consulté le 12 mai 2020, Lien
[2] Gouvernement du Canada, Ministère de la défense, site web consulté le 12 mai 2020, Lien

mesures de protection[3]. Au cours de ces deux phases, peu de directions seront communiqués. Lorsqu'émises, très peu ont fournis des détails quant à la préparation de solution technologiques capables de supporter le télétravail et se résument à un commentaire très général sur la « *mise à jour des plans de continuité des activités.* »[4] Cette continuité des opérations se résume malheureusement à un nombre très restreint d'options et de terminaux RÉD.

**Phase d'activation de Op LASER :**

Cette phase a été activée sur ordre du CÉMD le 13 mars 2020[5]. Elle a été caractérisée par la transmission généralisée et continue du virus dans la population générale et par le risque imminent ou l'existence d'un taux important d'absentéisme au travail. C'est à ce moment que le télétravail tel qu'on le connait aujourd'hui, a pris forme. À la suite de cette activation, le COIC a émis la tâche suivante au SMA GI : « *Confirm status of DVNPI to support working from home NLT 25 Mar 20.* »[6] Cette tâche et VÉM arrive environ 1 mois après l'identification d'une dégradation de service majeure émise en date du 27 février 2020 par DIMEUS alors que SMA GI demandait de limiter l'utilisation d'Internet et de l'IRPVD-T afin de résoudre les éventuels problèmes de bande passante.[7] À ce moment, le nombre d'usagers travaillant de la maison était accru pour cause de météo non clémente. Ce nombre d'usagers était cependant bien en dessous du

---

[3] Ibid.
[4] Gouvernement du Canada, Ministère de la défense, CÉMD, CANFORGEN NOVEL CORONAVIRUS (COVID-19) UPDATE / MISE A JOUR DU NOUVEAU CORONAVIRUS (COVID-19) CANFORGEN 039/20 SJS 017/20 031919Z MAR 20
[5] Gouvernement du Canada, Ministère de la défense, CÉMD, CDS Frag O 001 to CDS TASKORD – Op LASER 20-10 Ph 3 Activation, 13 Mar 20
[6] Gouvernement du Canada, Ministère de la Défense, CJOC, CJOC FRAG O 003 – OP LASER 20-01, March 2020, p. 8
[7] Gouvernement du Canada, Ministère de la Défense, SMA GI, Degradation of Services – NCR Service Desk Services – NCR – 27 February 2020 / Dégradation des services – Services du centre d'aide de la RCN – RCN – 27 février 2020

nombre élevé rencontré durant la pandémie. À la suite de cet avis de dégradation de services, un travail d'état-major et de planification des spécialistes en SIC a débuté afin de mieux comprendre les limites de l'infrastructure de l'IRPVD-T et afin de prendre action et d'améliorer la connectivité en cas de besoin. Le 2 mars 2020, SPC et le SMA GI ont dû fournir des options potentielles pour accroitre la capacité IRPVD-D et ce, en anticipation de la pandémie grandissante. Ainsi, les recommandations proposées (de nature majoritairement réseautiques), devaient permettre la connexion de 40 000 usagers concurrents (besoin de connectivité connu) et une redondance de 50% entre les deux sites décris en figure 1.[8] La recommandation du groupe d'experts consiste en une mise à jour rapide de l'infrastructure actuelle en empruntant des équipements dédiés à d'autres projets pour un coût total estimé à 2.5 millions de dollars.[9]

Durant l'attente de cette implémentation, des directions ont été émises par le CÉMD afin de limiter le nombre d'usagers concurrents sur IRPVD-D. Ainsi chaque niveau 1 ont par la suite été restreints avec un certain nombre maximal d'accès à respecter afin de pallier les limitations de la connectivité.[10] SPC et SMA GI ont par la suite émis un guide qui prônait l'utilisation de moyens alternatifs de communication afin de « *réduire l'impact sur le réseau commuté à distance de la défense (IRPVD-T), qui est réservé aux tâches/fonctions essentielles* » et « *afin de permettre d'assurer la sécurité de notre information lors du travail à domicile* »[11].

[8] Gouvernement du Canada, Service Partagé Canada, TDVPNI – Emergency Upgrade Options (Security), 4 March 2020, p.1
[9] Ibid. p.2
[10] Gouvernement du Canada, Ministère de la défense, CÉMD, CDS Frag O 001 to CDS TASKORD – Op LASER 20-10 Ph 3 Activation, 13 Mar 20
[11] Gouvernement du Canada, SPC et SMA GI, Guide de sécurité du MDN et de FAC pour le télétravail pendant l'intervention de COVID-19, 22 Avril 2020, p.1

Ce guide a été envoyé aux usagers environ 45 jours après que l'ordre d'activation de la phase 3 ait été signé par le CÉMD et ce, malgré le fait que : « *Only mission essential personnel will be allowed access to DVPNI* ».[12] Entre temps, beaucoup de membres ont improvisé et continuent de le faire avec les moyens à leur portée. L'incapacité des FAC à fournir des SIC robustes à ses membres confinés s'est traduite par un lourd fardeau de risques pour l'ensemble de l'institution et ses membres.

**Doctrine de travail et de systèmes d'information et de communication**

La façon avec laquelle les membres des FAC ont été habitué à travailler du point de vue des SIC de même que l'infrastructure globale supportant cette méthodologie est obsolète et nécessitera d'être entièrement repensée.

**Processus et concept**

La vaste totalité des processus liés à la méthodologie de travail des FAC est orientée selon une centralisation des lieux de travail qui elle, est axée sur les structures organisationnelles. Ainsi, chaque organisation partage une certaine méthodologie de travail basée sur le simple précepte qu'elles sont physiquement colocalisées et qu'elles ont accès à des stations de travail et des ressources communes pour accomplir leurs tâches. Le milieu de travail n'est donc pas conçu en fonction d'offrir le télétravail à grande échelle.

Le télétravail peut se définir comme étant « *un type de travail et/ou une prestation de services accomplis à distance et en ligne au moyen d'ordinateurs et de technologies télématiques*. » [13]

---

[12] Gouvernement du Canada, Ministère de la Défense, CJOC, CJOC FRAG O 003 – OP LASER 20-01, March 2020, p. 15

[13] Teleworking in the Context of the Covid-19 Crisis by Angel Belzunegui-Eraso and Amaya Erro-Garcés, Sustainability 2020, 1 May 2020, p.2.

Selon cette même définition, il existe trois types de télétravail à savoir :

| Type de télétravail | Utilisation de la technologie | Endroit |
|---|---|---|
| **Télétravail à domicile régulier** | Toujours ou presque tout le temps | De la maison au moins plusieurs fois par mois et dans d'autres endroits moins souvent que plusieurs fois par mois. |
| **Télétravail mobile élevé** | Toujours ou presque tout le temps | À au moins plusieurs fois par semaine dans au moins deux lieux autres que les locaux de l'employeur ou travaillant quotidiennement dans au moins un autre lieu. |
| **Télétravail occasionnel** | Toujours ou presque tout le temps | Moins fréquemment et / ou moins d'emplacements que Télétravail mobile élevé. |

**Table 1: Type de télétravail, source**[14]

Enfin, au-delà de toute la méthodologie de travail qui devrait être repensée, les auteurs Baruch et Nicholson mentionnent qu'il existe quatre facteurs qui influencent le télétravail : « *Facteurs individuels, facteurs liés à l'emploi, facteurs organisationnels et les facteurs familiaux et lié au domicile*. »[15] L'analyse de ces derniers devraient donc entrer dans l'équation menant à la solution pour les FAC.

**Gestion d'information**

En ligne avec les processus, la gestion d'information est un élément crucial à considérer dans la stratégie du télétravail puisqu'elle devrait permettre aux usagers d'accomplir toutes leurs tâches et de collaborer et partager l'information. Ainsi, la gestion de l'information peut comprendre « *le cycle des activités organisationnelles incluant: La collection d'information, l'analyse, la*

[14] Ibid p.3
[15] Baruch, Y.; Nicholson, N. Home, Sweet Work: Requirements for Effective Home Working. J. Gen. Manag. 1997, 23, 15–30

*catégorisation, la contextualisation, l'archivage, la collaboration, le partage etc. et ce, afin de supporter le modèle de travail des FAC.* »[16]

**Modèle de support**

Le modèle de support des SIC des FAC devra être repensé puisqu'il n'est clairement pas adapté à la pandémie à laquelle le monde fait face. Le modèle de support que nous connaissons au sein des FAC est vaste et utilise le cadre Information Technology Service Mangement (ITSM) qui incorpore certaines facettes des meilleures pratiques de *Information Technology Infrastructure Library 4* (ITIL). Il a été mis à place à partir de 2016 par la compagnie Calian pour des coûts supérieurs à 3 millions de dollars et l'implémentation s'est faite sur plusieurs années[17]. Il est clair que ce modèle imbriqué entre SPC et SMA GI devrait être complètement revu puisque : « *L'ITSM s'intéresse davantage à la façon dont les systèmes ou programmes sont utilisés par les usagers… et… Se concentre sur le service réel que le système fournit* »[18] et que ces derniers changeront selon la stratégie de télétravail choisie.

**Infrastructure**

Tel que mentionné dans la première section, l'infrastructure actuelle devra être repensée de façon à supporter le télétravail et ce, selon les modalités choisies par les FAC. Les capacités actuelles sont orientées d'une façon centralisée avec une redondance parfois même incomplète. Les plans liés à la continuité des opérations des FAC sont plus souvent qu'autrement liés à l'activation de sites alternatifs et centralisés plutôt que sur la connectivité dispersée de tous ses membres. Celle-ci

[16] Site web de Smartsheet, Information Management Strategies: From Punch Cards to Data Warehouses, and Looking to the Future with Big Data and AI, consulté le 13 mai 2020, Lien
[17] Site web de Calian, Calian Wins $3 Million DND Contract For Information Technology Service Management Support Services, June 13, 2016, consulté le 13 mai, Lien
[18] Varick D. Love / Lawrence R. Ness, Integrating ITSM into the Corporate Environment, Journal of Health Care Compliance, May–June 2016, p.6.

inclue de plus un nombre limité de terminaux permettant aux heureux élus de se connecter à distance. Enfin, les moyens alternatifs utilisés dans le contexte de la pandémie actuelle sont en majeure partie les moyens de communication personnels des membres. Les éléments suivants [19] (voir table 2 page suivante) devraient très certainement être analysés afin d'être aptes à répondre à la demande de connectivité dispersée.

| Série | Élément lié à l'infrastructure des TIC | Capacité actuelle des FAC | Commentaire |
|---|---|---|---|
| **1** | Application de connectivité et communication | Microsoft Outlook, SharePoint, etc. | En problématique et ne permettent pas un télétravail complet. |
| **2** | Technologie au niveau de l'usager et liée à l'accès à distance | Ordinateurs et ordinateurs portables | En problématique puisque nécessite que chaque usager ait un ordinateur portable en sa possession (ressources limitées). |
| **3** | Technologie liée à l'authentification et à l'identité | Carte Entrust PKI Authentication Windows | En problématique puisque nécessite que chaque usager ait un lecteur et une carte PKI. |
| **4** | Technologie liée à la connectivité à distance | Tunney's et Pearkes (voir figure 1), VPN | En problématique et nécessite une mise à jour.[20] |
| **5** | Technologie liée à la protection et à la sécurité | Tunney's et Pearkes (voir figure 1) | En problématique et nécessite une mise à jour. |
| **6** | Technologie réseautique | Tunney's et Pearkes (voir figure 1) | En problématique et nécessite une mise à jour pour permettre à plus d'usager de se connecter.[21] |
| **7** | Technologie centre de données | Supporte une quantité limitée d'usagers | En problématique et nécessite un concept lié à tous les éléments susmentionnés. |
| **8** | Politique de télétravail | Incomplète | En problématique et |

[19] Site web de ImproveIT, Getting started with Telework, consulté le 14 mai, Lien
[20] Gouvernement du Canada, Service Partagé Canada, TDVPNI – Emergency Upgrade Options (Security), 4 March 2020, p.3.
[21] Gouvernement du Canada, Email, Update from the Deputy Minister Regarding Flexible Work Arrangements and Leave / Mise à jour de la sous-ministre concernant les modalités de travail flexibles et les congés, 16 mars 2020, para 2

| | | | |
|---|---|---|---|
| | et gouvernance | | nécessite un concept. |

**Table 2: Lacunes liés à l'infrastructure des TIC, sources multiples**

**Besoin en communication et information**

En observant le type d'information que les membres des FAC ont besoin d'échanger entre eux, les planificateurs de SPC et ADM IM seront à même de traduire les exigences d'information opérationnelles (BECI) dans les détails requis pour la planification des SIC afin d'extrapoler les outils (BESI) qui supporteront la communauté d'usagers[22]. Cette analyse qui devra aller de pair avec la stratégie et le concept d'opération de télétravail pour les FAC est non seulement essentielle mais demeure la base (élément 1 de la table 2) de toute la planification requise en vue d'adresser les lacunes brièvement décrites table 2. Ainsi, en observant les lacunes actuelles de RÉD accessible via IRPVD-D et les moyens mis en place afin d'atteindre les exigences en BECI durant la continuité des opérations des FAC durant la pandémie, il devient apparent que la partie n'est pas gagnée. En effet, la majorité des usagers étant encouragée à utiliser les capacités alternatives[23] pour ne pas surcharger les capacités accréditées qui sont limitées.

[22] Minister of Defence of UK, Chiefs of Staff, Joint doctrine publication 6-00 Communication and Information Systems Support to Joint Operations, 3rd Edition, January 2008, p.1-1
[23] Gouvernement du Canada, Ministère de la defense, VCDS, Frago 002 to VCDS OP Order – OP LASER PH 3 ACTIVATION, 1st April 2020, p.13

Le tableau suivant résume la situation et montre les capacités alternatives.

| Série | BECI | Capacités actuelles accréditées des FAC | Capacités alternatives de contingence |
|---|---|---|---|
| **1** | Voie non classifiée | Via téléphone intelligents fournis par SPC ou SMA GI ou applications en ligne via appareils RÉD fournis par SPC ou SMA GI | Via téléphones intelligents personnels et solutions commerciales ad hoc sur appareils personnels. |
| **2** | Courriel | Via Microsoft Outlook ou Office 365 sous téléphones intelligents et appareils RÉD fournis par SPC ou SMA GI. | Office 365, Slack et messagerie personnelle via appareils personnels. |
| **3** | Échange de fichiers et collaboration | Via Courriel, SharePoint, Office 365 sur appareils RÉD fournis par SPC ou SMA GI. | GC Collab, Google Hangouts et solutions commerciales adhoc sur appareils personnels |
| **4** | Vidéoconférence non classifiée | Via DVCS (capacité très limitée) sous appareils RÉD fournis par SPC ou SMA GI. | Facetime, Webex, Microsoft Team, Zoom et solutions commerciales ad hoc sur appareils personnels ou enclave personnelles de téléphone intelligent fournis par SPC ou SMA GI. |
| **5** | Clavardage | Via Office 365, sous appareils RÉD fournis par SPC ou SMA GI messagerie texte via téléphone intelligents fournis par SPC ou SMA GI. | Slack, Office 365, solutions commerciales adhoc sur appareils personnels. |
| **6** | Suite de travail de base | Microsoft Office ou Office 365. | Office 365 et solutions commerciales ad hoc sur appareils personnels. |
| **7** | Besoins spécialisés | PeopleSoft, DRMIS, CFTPO, etc. | Aucune. |

**Table 3 : BECI et BESI des FAC en télétravail, source**[24]

[24] Gouvernement du Canada, SPC et SMA GI, Guide de sécurité du MDN et de FAC pour le télétravail pendant l'intervention de COVID-19, 22 Avril 2020, p.1

**Défis supplémentaires**

Outre les défis liés au manque de connectivité, il existe certains autres défis qu'il incombe

**Cybersécurité et sécurité de la technologie de l'information (TI)**

La protection des systèmes consiste à appliquer des mesures de sécurité pour la protection des communications, de l'information et d'autres systèmes électroniques, et des informations stockées, traitées ou transmises dans ces systèmes avec respect de (voir Table 4)[25]. Malheureusement, l'emploi de capacités alternatives et de contingence qui ne sont pas accréditées ne permettent pas de garantir les éléments ci-dessous puisqu'elles sont des « *mesures qui ont été prises hâtivement* » [26]:

| Série | Éléments | Définition |
|---|---|---|
| **1** | Confidentialité | Assurer que seules les personnes autorisées aient accès aux ressources échangées. |
| **2** | Intégrité | Garantir que les données sont bien celles que l'on croit être. |
| **3** | Disponibilité | Assurer de maintenir le bon fonctionnement du système d'information. |
| **4** | Identification et authentification | Assurer que seules les personnes autorisées aient accès aux ressources. |
| **5** | Non répudiation | Garantir l'impossibilité, pour une personne ou pour toute autre entité engagée dans une communication par voie informatique, de nier avoir reçu ou émis un message. |

**Table 4: Objectifs de la sécurité des SIC**

[25] NATO, Directive on the protection of communication and information system (CIS) handling non-classified NATO information, 6 November 2019, p.1-2

[26] The Star, Web conferencing platforms at risk of being lure for phishing emails: consultant, David Paddon The Canadian Press, March 27, 2020, consulté le 21 mai, Lien

C'est donc un flirt avec le risque qui est en cours durant la pandémie et ce, malgré toutes les recommandations du Centre canadien pour la cyber sécurité[27]. En l'absence de solutions en place et en temps opportun, les FAC ont été acculées au pied du mur comme la plupart des nations et industries. C'est pour cette raison que SPC et SMA GI ont accéléré le déploiement de Office 365 (solution accréditée)[28] qui respecte les aspects liés aux objectifs décrits en Table 4 en plus d'offrir un monitoring du réseau puisque les menaces cybernétiques sont toujours présentes et en recrudescence à cette époque difficile[29]. En absence de solution de télétravail unifiée, accréditée et défendue, nulle organisation gouvernementale n'est en mesure de protéger les capacités commerciales à l'extérieur de leur réseau, de les monitorer, de les défendre, d'empêcher l'exploitation des données et de réagir en cas de besoin.

**Service Partagé Canada et le ministère de la Défense**

Selon SPC, il n'existe pas d'approche universelle pour les services numériques du gouvernement du Canada, ce qui est un défi en soit. Dans un contexte de connectivité à distance pour le télétravail, il existe des solutions qui sont déployées dans d'autres ministères et qui auraient pu être déployées pour les FAC et ce, avant la pandémie. Il existe malheureusement certains contentieux liés à la sécurité (besoins supplémentaires et préoccupations) qui semblent ne pas être résolus ce qui explique les retards accumulés pour le MDN[30]. Il existe de plus des divergences d'opinions concernant les moyens d'authentifications et l'accessibilité entre le RÉD via IRPVD-D et des solutions tels que Office 365. Ainsi, les deux capacités sont gardées séparées

[27] Gouvernement du Canada, Centre Canadien de cybersécurité, Conseils de cybersécurité pour le télétravail (ITSAP.10.116), consulté le avril 2020, Lien
[28] Gouvernement du Canada, Ministère de la défense, site web consulté le 21 mai, Lien
[29] National Post, increase in teleworking bureaucrats makes Canadian Government more vulnerable to cyberthreats than ever, Christopher Nardi, 7 April 2020, consulté le 21 mai 2020, Lien

[30] Email from Command Information System Security Officer / Canadian Joint Operations Command, Subject: SSC and DWAN Remote connectivity, 14 May 2020

pour l'instant. Selon le site de SPC, cette capacité est temporaire et d'autres solutions sont à venir[31].

**Conclusion**

Au cours du présent essai, nous avons pu observer et soutenir que les FAC ne possèdent pas d'infrastructure de technologie de l'information, de communication, de commandement et de contrôle (dans le domaine non-classifié) leur permettant d'être efficaces au travail lorsque la vaste majorité de ses membres sont dispersés. Les moyens disponibles au moment où la pandémie a débutée sont basés sur un modèle de centralisation des lieux de travail axée sur les structures organisationnelles. Les plans de continuité des opérations sont basés sur l'activation de sites alternatifs centralisés et d'une quantité limitée d'équipement RÉD requérant l'authentification au moyen de certificats dits matériels (Technologie d'infrastructure à clé publique des FAC).

Il faudra donc repenser la méthodologie de travail du point de vue de l'expérience utilisateur puisqu'il est maintenant confirmé que l'hypothèse selon laquelle tous membres des FAC ont accès à un terminal RÉD, une carte PKI et l'infrastructure IRPVD-D s'est avérée fausse. Les mesures d'atténuation mises en place par SPC et SMA GI (augmentation de l'infrastructure IRPVD-D et déploiement d'une enclave d'office 365) ne règle en rien la problématique vécue pendant la pandémie. Le MDN tout comme le reste du gouvernement du Canada devra passer de

[31] Gouvernement du Canada, Service Partagés Canada, Foire aux questions sur Services partagés Canada et la COVID-19, consulté le 22 mai 2020, Lien

réseaux ministériels uniques à réseaux d'entreprise modernes. Ces réseaux devront être accessibles en tout temps, en tout lieu et par tous[32].

Les lacunes en connectivité engendrées par la pandémie ont mis à risque le MND et ses membres. La solution à ce problème sera une aventure coûteuse et de longue haleine qui nécessitera de repenser totalement l'expérience utilisateur, nos méthodes de travail et un changement de culture. Y sommes-nous prêts?


**Figure 2: Résumé des composantes de base requises dans le cadre d'une analyse d'une nouvelle solution RÉD pour les FAC**

[32] Gouvernement du Canada, Service Partagés Canada, SPC 3.0 : Une approche d'entreprise, consulté le 22 mai 2020, Lien

**BIBLIOGRAPHIE**

Site web de Entrust, consulté le 12 mai 2020, Lien

Gouvernement du Canada, Ministère de la défense, site web consulté le 12 mai 2020, Lien

Gouvernement du Canada, Ministère de la défense, CÉMD, CANFORGEN NOVEL CORONAVIRUS (COVID-19) UPDATE / MISE A JOUR DU NOUVEAU CORONAVIRUS (COVID-19) CANFORGEN 039/20 SJS 017/20 031919Z MAR 20

Gouvernement du Canada, Ministère de la Défense, CJOC, CJOC FRAG O 003 – OP LASER 20-01, March 2020

Gouvernement du Canada, Ministère de la Défense, SMA GI, Degradation of Services – NCR Service Desk Services – NCR – 27 February 2020 / Dégradation des services – Services du centre d'aide de la RCN – RCN – 27 février 2020

Gouvernement du Canada, Service Partagé Canada, TDVPNI – Emergency Upgrade Options (Security), 4 March 2020

Gouvernement du Canada, Ministère de la Défense, CÉMD, CDS Frag O 001 to CDS TASKORD – Op LASER 20-10 Ph 3 Activation, 13 Mar 20

Gouvernement du Canada, SPC et SMA GI, Guide de sécurité du MDN et de FAC pour le télétravail pendant l'intervention de COVID-19, 22 avril 2020

Teleworking in the Context of the Covid-19 Crisis by Angel Belzunegui-Eraso and Amaya Erro-Garcés, Sustainability 2020, 1 May 2020.

Baruch, Y.; Nicholson, N. Home, Sweet Work: Requirements for Effective Home Working. J. Gen. Manag. 1997, 23, 15–30

Site web de Smartsheet, Information Management Strategies: From Punch Cards to Data Warehouses, and Looking to the Future with Big Data and AI, consulté le 13 mai 2020, Lien

Site web de Calian, Calian Wins $3 Million DND Contract For Information Technology Service Management Support Services, June 13, 2016, consulté le 13 mai, Lien

Varick D. Love / Lawrence R. Ness, Integrating ITSM into the Corporate Environment, Journal of Health Care Compliance, May–June 2016, consulté le 14 mai, Lien

Gouvernement du Canada, Email, Update from the Deputy Minister Regarding Flexible Work Arrangements and Leave / Mise à jour de la sous-ministre concernant les modalités de travail flexibles et les congés, 16 mars 2020

Site web de ImproveIT, Getting started with Telework, consulté le 14 mai, Lien

Minister of Defence of UK, Chiefs of Staff, Joint doctrine publication 6-00 Communication and Information Systems Support to Joint Operations, 3rd Edition, January 2008, Lien

Gouvernement du Canada, Ministère de la Défense, VCDS, Frago 002 to VCDS OP Order – OP LASER PH 3 ACTIVATION, 1st April 2020

NATO, Directive on the protection of communication and information system (CIS) handling non-classified NATO information, 6 November 2019

The Star, Web conferencing platforms at risk of being lure for phishing emails: consultant, David PaddonThe Canadian Press, March 27, 2020, consulté le 21 mai, Lien

Gouvernement du Canada, Ministère de la Défense, site web consulté le 21 mai, Lien

National Post, increase in teleworking bureaucrats makes Canadian Government more vulnerable to cyberthreats than ever, Christopher Nardi, 7 April 2020, consulté le 21 mai 2020, Lien

Gouvernement du Canada, Centre Canadien de cybersécurité, Conseils de cybersécurité pour le télétravail (ITSAP.10.116), consulté le 22 mai 2020, Lien

Email from Command Information System Security Officer / Canadian Joint Operations Command, Subject: SSC and DWAN Remote connectivity, 14 May 2020

Gouvernement du Canada, Service Partagés Canada, Foire aux questions sur Services partagés Canada et la COVID-19, consulté le 22 mai 2020, Lien

Gouvernement du Canada, Service Partagés Canada, SPC 3.0 : Une approche d'entreprise, consulté le 22 mai 2020, Lien