



Réponse du Sous-comité national des DPI sur la protection des renseignements (SNDPI) suite aux demandes du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) présentées à la réunion tenue en juillet 2017

Préparé au nom du SNDPI avec la contribution des membres du comité par
Martin Dinel, président du SNDPI et dirigeant principal de la sécurité de l'information (DPSI) de l'Alberta
Robert Samuel, vice-président du SNDPI et DPSI de la Nouvelle-Écosse
Gary Perkins, secrétaire du SNDPI et DPSI de la Colombie-Britannique
12 septembre 2017

INTRODUCTION

Une révision de l'ordre du jour de la réunion d'octobre a été effectuée suite à la mise à jour du SNDPI, lors de la réunion du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) tenue en juillet 2017. Une décision a été prise afin de réserver 60 minutes pour une mise à jour du SNDPI à l'ordre du jour de la réunion du 5 octobre 2017. Les membres du CDPISP ont déterminé plusieurs sujets d'intérêt et demandé si le SNDPI pouvait aider à fournir des renseignements pour une discussion durant cette réunion. Voici les sujets :

1. *Comment les administrations canadiennes fédérale, provinciales et territoriales (F/P/T) se préparent-elles aux élections en termes de cybersécurité?*
 - a. *Qu'est-ce que le géoblocage?*
2. *Comment le SNDPI peut-il aider à garder les dirigeants principaux de l'information (DPI) du pays mieux informés concernant les menaces pour la cybersécurité?*
 - a. *Est-ce qu'une habilitation fédérale de sécurité devrait être obtenue pour avoir accès à une information partagée sur la cybersécurité?*
3. *Comment le gouvernement peut-il aider à encourager les écoles afin d'inclure la cybersécurité dans leurs programmes scolaires?*
4. *Que font les administrations canadiennes F/P/T pour éduquer les ministres et les employés du gouvernement à propos de la cybersécurité?*

Le document suivant fournit des réponses résumées, qui seront revues plus en détail au cours de la réunion du CDPISP qui aura lieu le 5 octobre prochain.

Sous-comité national
des DPI sur la
protection des renseignements



Les administrations participantes comprenaient le gouvernement du Canada (GC), Terre-Neuve-et-Labrador (T.-N.-L.), Nouvelle-Écosse (N.-É.), Nouveau-Brunswick (N.-B.), Île-du-Prince-Édouard (Î.-P.-É.), Ontario (Ont.), Manitoba (Man.), Saskatchewan (Sask.), Alberta (Alb.), Colombie-Britannique (C.-B.), Yukon (Yn), Territoires du Nord-Ouest (T.N.-O.), ASIM Est (ME), ASIM Ouest (MW) et ASIM Prairies (MP).

Aucune réponse du Québec et du Nunavut (aucune représentation sur le SNDPI).



DEMANDE N° 1 : COMMENT LES ADMINISTRATIONS CANADIENNES F/P/T SE PRÉPARENT-ELLES AUX ÉLECTIONS EN TERMES DE CYBERSÉCURITÉ?

Seulement quatre répondants (Yn, T.N.-O., Î.-P.-É. et ME) ont rapporté ne pas avoir commencé à se préparer pour leurs prochaines élections. Cependant, il est probable qu'ils effectueront des travaux dans ce domaine ultérieurement.

Toutes les autres administrations (GC, T.-N.-L., N.-É., N.-B., Ont., Man., Sask., Alb., C.-B., MW et MP) ont commencé à se préparer en vue de leurs prochaines élections, y compris les activités suivantes :

- Les administrations ci-dessus ont partagé le rapport émis par le gouvernement fédéral intitulé « Les cyber-menaces envers le processus démocratique du Canada » et/ou un exposé connexe avec leurs directions générales afin de les sensibiliser aux attaques et aux risques concernant le processus démocratique du Canada.
- Toutes les équipes de cybersécurité des administrations ont revu le document du gouvernement fédéral et pris des mesures pour améliorer la cybersécurité avant et durant leur prochaine élection, y compris :
 - **Des évaluations de menaces de sécurité et de risques sont effectuées concernant la menace identifiée pour le processus d'élection dans chaque administration.** Les risques identifiés sont évalués du point de vue des probabilités et des impacts, priorisés par exposition aux risques, les atténuations sont déterminées, et les risques seront contrôlés et gérés par des processus de gestion des risques internes. (Tous)
 - **Mise en place du géoblocage.** Mise en place du contrôle de sécurité pour bloquer le trafic imprévu du réseau (principalement les services du réseau autres que la navigation Web ou le http sur le port 80 et les https sur le port 443) provenant de pays à l'extérieur du Canada. (En place ou mis en place : Alb., C.-B., N.-B., N.-É., MW, Ont.; planifié : NL, T.N.-O., Sask., Yn; non planifié : Man., MP, Î.-P.-É., ME)
 - **Augmentation de la surveillance des opérations de cybersécurité.** Des protocoles pour l'augmentation de la surveillance des opérations de cybersécurité seront suivis quelques semaines avant, pendant et après les élections, s'assurant ainsi que toute activité suspecte, soit enquêtée par le personnel et la direction de la cybersécurité. (Tous)
 - **L'équipe de réponse de la cybersécurité est en attente.** Le personnel de la cybersécurité sera en attente durant la période de surveillance, augmentée avec le personnel sur appel, prêt à répondre à toute activité ou incident de nature suspecte. (Toutes)
 - **Surveiller les flux de renseignements sur les menaces.** Toutes les administrations ont rapporté qu'elles surveillent déjà ou surveilleront les flux de renseignements sur les menaces avant et durant le processus électoral.

Quelques différences entre les administrations :

- Le Manitoba n'exploite pas actuellement le géoblocage. Le Manitoba a une politique restrictive de pare-feu qui permet seulement le trafic entrant basé sur les communications HTTP/HTTPS, peu importe la source géographique du trafic. Ceci est dû en partie à des défis inhérents à la mise en place du géoblocage basé sur la capacité technologique. Il existe une forte possibilité que le trafic Web légitime soit bloqué, lorsque le géoblocage est mis en place de façon globale.

Sous-comité national
des DPI sur la
protection des renseignements



- L'Ontario rencontre les partenaires fédéraux, provinciaux et municipaux pour développer une stratégie et des plans de réponse aux incidents concernant les incidents touchant la cybersécurité durant l'élection. La police provinciale de l'Ontario préside ces réunions.
- L'Île-du-Prince-Édouard commencera le travail de préparation concernant ce sujet, dès qu'un nouveau directeur des élections sera nommé.
- Le Nouveau-Brunswick ira aux urnes en 2018. Il y a des contrôles de sécurité stricts concernant le traitement électronique des renseignements électoraux, y compris la formation et les tests pour les responsables des élections. Il prévoit une formation et des tests en ligne pour l'élection de 2018.
- Durant la récente élection en Colombie-Britannique, l'accent n'a pas été mis sur les technologies. La prochaine fois, la technologie jouera cependant un plus grand rôle, alors que l'accent sera mis sur la résolution des vulnérabilités identifiées durant l'évaluation des risques qui a débuté, de même que sur l'exploitation de l'expérience de la plus récente élection. L'élément ayant contribué à l'excellent environnement de cybersécurité ayant prévalu au cours de la récente élection réside dans le contact d'Elections C.-B. qui s'est mis d'accord pour avoir un deuxième observateur de la situation, doté d'un esprit ouvert. Des impacts « indirects » furent également à considérer avec les médias, compte tenu de la parution d'articles sur des incidents ou de fausses informations concernant les procédures électorales. Même si ces questions ont été réglées ad hoc, il est devenu évident que le travail de préparation concernant les communications doit être entrepris avant les futures élections. Les recommandations du DPSI de la Colombie-Britannique suggèrent de commencer à planifier aussitôt que possible et d'offrir de l'aide aux personnes responsables des procédures électorales. Concernant le géoblocage, il faut garder à l'esprit qu'il est beaucoup plus facile d'examiner 4 ports plutôt que 65 535. Réduisez le nombre de ports de liste blanche au lieu de bloquer des ports spécifiques. Réduisez le nombre de pays ayant accès à votre environnement, cela améliore la sécurité et la performance. Il est aussi important de considérer les besoins des entreprises : tout ce qui n'est pas un port 80/443/25/53 et qui doit être ouvert à un pays étranger devrait être une exception et être examiné de près avec des contrôles supplémentaires en place, etc. Lors de la mise en œuvre du géoblocage, optez pour le périmètre ultrapériphérique de votre réseau, peut-être même chez le fournisseur de services.
- La Nouvelle-Écosse a mis en place 3 niveaux de géoblocage : la Nouvelle-Écosse seulement, le Canada seulement, et l'Amérique du Nord seulement. Il y a 5 applications/services dans le géoblocage de la Nouvelle-Écosse, 11 dans le géoblocage du Canada et 8 dans le géoblocage de l'Amérique du Nord. La plupart des géoblocages ont été demandés par les propriétaires, étant donné que les utilisateurs de leurs applications et services sont connus.
- Le géoblocage de l'Ontario est appliqué « ad hoc » selon l'identification du trafic malicieux au sein de chaque sous-réseau particulier. Durant les élections, il peut bloquer des régions géographiques particulières selon les rapports de renseignements.
- Le Nouveau-Brunswick utilise peu cette technologie en raison de la facilité de contrefaire les adresses IP. Cependant, nous appliquons des règles pour l'accès à distance qui nécessite 2FA et des captchas de certaines sources géographiques. Nous avons aussi proposé (aucune décision n'a été prise) des profils d'accès conditionnels pour Office365 qui tiennent compte de la localisation. En ce moment, nous cherchons seulement à séparer le trafic canadien et non canadien. Nous ne sommes pas arrivés au point d'identifier des pays ciblés comme étant à risques.

Sous-comité national
des DPI sur la
protection des renseignements



1.A : QU'EST-CE-QUE LE GÉOBLOCCAGE?

Le géoblocage est aussi appelé *filtre de géolocalisation*. Il sert à bloquer ou à filtrer le trafic du réseau selon sa source géographique. Par exemple, bloquer le trafic du réseau provenant de la Chine ou d'un autre pays.

Le géoblocage ne bloque normalement pas **tout** le trafic du réseau, mais plutôt le trafic spécifique basé sur les ports TCP ou UDP (services de réseau) utilisés. Par exemple, le trafic de navigation Internet (ports 80 pour http, et 443 pour https) est permis pour tous les pays, permettant ainsi aux usagers de ces pays de naviguer sur les sites Internet, mais d'autres ports comme File Transfer Protocol (port 20 pour FTP) utilisé pour partager des dossiers, ou Secure Shell (port 22 pour SSH) utilisé pour administrer des systèmes à distance peuvent être bloqués, puisque ces activités ne devraient pas provenir de ces pays.

POINT IMPORTANT CONCERNANT LE GÉOBLOCCAGE

Des pirates plus sophistiqués trouvent maintenant des façons d'éviter les règles de géoblocage en utilisant un serveur mandataire dans la localisation géographique des environnements ciblés ou en contrefaisant des adresses IP.

DEMANDE NO 2 : COMMENT LE SNDPI PEUT-IL AIDER À GARDER LES DPI DU PAYS MIEUX INFORMÉS CONCERNANT LES MENACES POUR LA CYBERSÉCURITÉ?

Le premier point de communication concernant la cybersécurité avec le DPI de toutes les administrations est, et devrait être, la personne responsable de la cybersécurité pour sa administration (nommé DPSI ou responsable de la sécurité des systèmes d'information). Le SNDPI, le Centre canadien de réponse aux incidents cybernétiques et d'autres moyens pour se connecter et discuter de cybersécurité sont accessibles et utilisés par les DPSI dans tout le pays. Les renseignements concernant la cybersécurité proviendront de la communication directe entre les DSI et les DPSI des administrations.

Il faut noter que les DPSI n'ont pas tous les mêmes capacités en termes de communications avec leurs DSI. Par exemple, certaines administrations recueillent et produisent des rapports d'opérations mensuels, trimestriels ou biannuels, et d'autres n'ont nullement la capacité de procéder ainsi. Le SNDPI travaille avec toutes les administrations pour déterminer quel serait l'ensemble des rapports de base, que devraient-ils contenir, et quelle serait leur fréquence de publication. Nous cherchons aussi à développer un rapport national ou un tableau de bord qui pourrait fournir un portrait national des menaces et de la protection pour la cybersécurité. C'est une priorité élevée pour le sous-comité cette année.

Le résumé suivant donne un aperçu des besoins et capacités de communication en cybersécurité à travers les diverses administrations :

Administration	Le DPSI est le DPI	Doit informer le DPI d'entreprise	Doit informer plusieurs DPI	Disponibilité des rapports d'opérations	Disponibilité des rapports de renseignements
Terre-Neuve-et-Labrador	Non	Régulièrement et ad hoc	Régulièrement et ad hoc	Tel que demandé	Tel que demandé
Nouvelle-Écosse	Non	Régulièrement et ad hoc	Ad hoc	Tel que demandé + semestriel	Tel que demandé + semestriel

Sous-comité national
des DPI sur la
protection des renseignements



Nouveau-Brunswick	Non	Hebdomadairement et ad hoc	Régulièrement et ad hoc	Trimestriellement + ad hoc	Trimestriellement + ad hoc
Île-du-Prince-Édouard	Non	Régulièrement et ad hoc	Non	Tel que demandé	Tel que demandé
Québec	S.O.	S.O.	S.O.	S.O.	S.O.
Ontario	Non	Régulièrement et ad hoc	Régulièrement et ad hoc	Tel que demandé	Tel que demandé
Manitoba	Non	Régulièrement et ad hoc	Non	Trimestriellement + ad hoc	Trimestriellement + ad hoc
Saskatchewan	Non	Hebdomadairement	Non	Tel que demandé	Tel que demandé
Alberta	Non	Mensuellement et ad hoc	Mensuellement et ad hoc	Mensuellement et ad hoc	Trimestriellement + ad hoc
Colombie-Britannique	Non	Régulièrement et ad hoc	Régulièrement et ad hoc	Tel que demandé	Tel que demandé
Yukon	Non	ad hoc	Non	Tel que demandé	Tel que demandé
Territoires du Nord-Ouest	Non	Régulièrement et ad hoc	Ad hoc	Tel que demandé	Tel que demandé
Nunavut	S.O.	S.O.	S.O.	S.O.	S.O.
Gouvernement du Canada	Non	Régulièrement et ad hoc	Régulièrement et ad hoc	Tel que demandé	Tel que demandé
ASIM de l'Est	Non	Ad hoc	S.O.	Trimestriellement + ad hoc	Trimestriellement + ad hoc
ASIM des Prairies	Non	Régulièrement et ad hoc	Non	Tel que demandé	Tel que demandé
ASIM de l'Ouest	Oui	DPI = DPSI	Non	Tel que demandé	Tel que demandé

2.A : DOIT-ON AVOIR OBTENU L'HABILITATION DE SÉCURITÉ FÉDÉRALE POUR AVOIR ACCÈS AUX INFORMATIONS DE CYBERSÉCURITÉ PARTAGÉES?

Toutes les provinces participantes ont convenu que l'habilitation de sécurité fédérale devrait être obtenue par les DPI et les membres de la direction qui sont responsables de la cybersécurité, afin de s'assurer que toutes les informations en matière de cybersécurité peuvent être partagées avec eux.

Situation actuelle :

- Les dirigeants qui ont l'habilitation (8) : GC, Man., Alb., Ont., T.N.-O., C.-B., T.-N. L., N.-B.
- Les dirigeants qui ont demandé l'habilitation (1) : Î.-P.-É.
- Les dirigeants sans habilitation, et dont l'habilitation n'est pas demandée (5) : Sask., Yn, MW, MP, ME
- Sans réponse (2) : Québec et Nunavut

Quelques différences gouvernementales :

Sous-comité national
des DPI sur la
protection des renseignements



- En Nouvelle-Écosse, le DPI, le DPSI et le DPSI adjoint du gouvernement ont tous reçu l'habilitation, mais n'ont pas de moyens de communication sécurisés en ce moment. Un vIPer a été installé dans un bureau régional provincial en 2016 pour la communication entre greffiers, mais n'a jamais été utilisé. Il est aussi possible d'exploiter les MDN CSNI installées dans les QG MARLANT et autres installations du MDN, ou continuer à chercher d'autres solutions de communication sécurisée.
- Le Nouveau-Brunswick mentionne que le DPI ne devrait pas nécessairement être le « premier informé » concernant les cybermenaces ou les cyberattaques. Il ne devrait pas non plus s'attendre à plonger dans « les mauvaises herbes », mais l'autorisation est nécessaire.
- La Colombie-Britannique et l'Alberta ont des pièces sécurisées ainsi que des solutions téléphoniques cryptées pour la communication, mais ne peuvent confirmer être parvenues à en faire une utilisation complète et en bénéficier complètement.
- Pour ce qui est du gouvernement fédéral, les employés de tous les niveaux reçoivent l'habilitation correspondant aux informations requises pour exercer leurs fonctions. Le DPI du GC a l'habilitation appropriée (en tant que condition d'emploi). L'octroi des habilitations du gouvernement fédéral aux DPI provinciaux, territoriaux ou municipaux faciliterait le partage d'informations dans la sphère de la cybersécurité et serait considéré comme un multiplicateur de force qui devrait être recherché.

Les processus de demandes d'habilitation varient en fonction du gouvernement. Certaines provinces utilisent également la GRC pour fournir des habilitations, tandis que d'autres transitent par le gouvernement fédéral. Le meilleur moyen est de vous renseigner auprès de votre DPSI pour connaître le processus d'obtention d'habilitation de sécurité fédérale. Notez que dans la plupart des cas, le processus peut prendre jusqu'à 8 mois pour obtenir la cote SECRET. La cote TRÈS SECRET peut prendre jusqu'à 12 mois.



DEMANDE #3 : COMMENT LE GOUVERNEMENT PEUT-IL AIDER À ENCOURAGER LES ÉCOLES AFIN D'INCLURE LA CYBERSÉCURITÉ DANS LEURS PROGRAMMES SCOLAIRES?

Après une analyse rapide, nous avons constaté que seulement 2 provinces (MP, N.-B.) étaient officiellement et activement impliquées dans de telles activités; bien que bon nombre de provinces (Alb., C.-B., Sask., MW, ME) soient quelque peu impliquées en raison de la participation personnelle ou volontaire de leur personnel de sécurité.

Les deux provinces qui sont actuellement officiellement impliquées sont :

- À Lethbridge, l'ASIM des Prairies travaille avec les écoles primaires et postsecondaires pour défendre un certain nombre d'initiatives. La sécurité est l'un d'entre elles. En réalité, c'est notre système scolaire qui a le pouvoir dans ce domaine.
- Nouveau-Brunswick – Dans le cadre de son programme CyberSmart, CyberNB se concentre sur l'élaboration de stratégies de perfectionnement de la main-d'œuvre à l'échelle nationale, à court et à long terme, conçues pour faire face à une pénurie mondiale de professionnels de la cybersécurité. À travers le système K-12, CyberNB travaille avec des partenaires en éducation pour identifier et modifier le programme d'études afin de s'assurer que le Nouveau-Brunswick ait des diplômés en alphabétisation numérique. En partenariat avec le milieu universitaire, le gouvernement et l'industrie, CyberNB identifie les principales tendances ainsi que les compétences qui sont nécessaires maintenant et dans le futur. Un succès récent fut en partenariat avec l'entreprise Blue Spurs basée au Canada pour l'introduction d'une trousse d'éducation IdO dans les écoles du Nouveau-Brunswick culminant avec Blue Spurs qui remporte le prix *AWS Global City on Cloud Innovation*. CyberNB encourage également les étudiants du premier cycle secondaire et du secondaire du Nouveau-Brunswick à participer au programme national Cyber Titan, qui offre des compétitions au Canada et aux États-Unis. En mai 2017, CyberNB a été l'hôte de CyberSmart 2017, le premier sommet au Canada conçu spécifiquement pour promouvoir la collaboration entre l'industrie, le milieu universitaire, le gouvernement et les jeunes, sur une stratégie nationale de développement de la main-d'œuvre pour la cybersécurité.

De plus, le programme public de sécurité du Canada, GetCyberSafe, ne fonctionne pas directement de concert avec les écoles. Par contre, le programme collabore avec des organisations qui sont en lien direct avec les écoles, spécifiquement lorsqu'il s'agit de contenu destiné aux parents et aux jeunes. GetCyberSafe travaille également avec le programme TELUS AVERTI (Utilisation sécuritaire d'Internet et des téléphones intelligents) (fournissant du contenu et des fiches d'informations GetCyberSafe), qui dispose d'un programme de conférenciers disponible pour les écoles et les conseils de parents afin de discuter de la sécurité sur Internet. GetCyberSafe a récemment rejoint des associations d'étudiants universitaires et plusieurs d'entre eux à travers le Canada ont inclus une carte postale GetCyberSafe sur l'importance des transactions financières sécurisées en ligne (achats et services bancaires) dans leurs costumes pour la semaine d'initiation. Cela a mené à la distribution de plus de 40 000 cartes postales bilingues.

Quelques différences gouvernementales :

- Alberta – Le bureau de sécurité d'information gouvernementale est présentement impliqué dans des discussions avec un collège et deux universités afin de créer un programme menant à un diplôme en cybersécurité, qui pourrait éventuellement mener à un programme de grade universitaire. L'opérateur du système de gestion de sécurité du gouvernement de l'Alberta, CGI, est aussi impliqué dans ces activités. Un accord du genre « Coop type » est l'objectif ultime, qui fournirait à la fois une expérience de travail aux

Sous-comité national
des DPI sur la
protection des renseignements



étudiants et des ressources aux promoteurs de programmes. Aucune attention particulière sur le K -12 n'est accordée en ce moment.

- Colombie-Britannique – Des programmes menant à un diplôme avec des spécialités en cybersécurité en Colombie-Britannique existent déjà, mais l'objectif du DPSI vise un programme de grade universitaire.
- Île-du-Prince-Édouard – Aucune incidence pour le moment, mais a suggéré que les écoles envisagent de mettre en place un programme pour accompagner l'introduction de la technologie sans fil et le programme AVEC dans nos écoles.
- ASIM de l'Est – Le DPSI participe à une discussion sur les mérites de la création d'un programme de maîtrise sur la cybersécurité (un programme INFOSEC/gestion de réseaux de 4 ans existe déjà).



DEMANDE #4 : QUE FONT LES GOUVERNEMENTS FPT POUR ÉDUIQUER LES MINISTRES ET LES EMPLOYÉS DU GOUVERNEMENT À PROPOS DE LA CYBERSÉCURITÉ?

Toutes les provinces participantes ont une forme de programme générique de sensibilisation et de formation sur la cybersécurité, y compris l'accès aux ressources en ligne et des présentations en classe. Le programme est offert à tous les employés du gouvernement. La plupart des gouvernements ont une politique selon laquelle tous les employés doivent compléter ce type de formation chaque année.

La liste des sujets habituellement abordés lors des programmes de formation inclut :

- Hameçonnage de courriels et Ingénierie sociale
- Standards de l'industrie des cartes de paiement
- Pratiques de sécurité générales lors de l'utilisation d'appareils
- Classification de sécurité de l'information/Gestion de l'information
- Télécopieur sur IP
- Pratique standard de l'administration des systèmes de sécurité
- Pratique standard de sécurité pour le développement de systèmes

Ces programmes de sensibilisation incluent souvent des lettres d'information ou une participation régulière dans les lettres d'information d'entreprises, ainsi qu'une attention portée sur le mois de la sensibilisation à la cybersécurité (en octobre de chaque année) à l'aide d'affiches et d'activités pertinentes.

Bien que toutes les provinces conviennent qu'un programme d'éducation pour les ministres est un *impératif* absolu, seules deux provinces (GC et C.-B.) ont actuellement accès à leurs ministres. Les ministres ont accès aux outils génériques mis à la disposition d'autres employés du gouvernement, mais les rapports de diverses provinces confirment qu'ils n'ont généralement pas accès à ce matériel et sont rarement interrogés sur la menace cybernétique.

Le DPSI de la C.-B. s'est affilié directement au caucus afin de fournir du matériel de sensibilisation.

Au gouvernement du Canada, les ministres sont mis au courant des enjeux de la cybersécurité par l'entremets de plusieurs moyens, tels que les déjeuners des sous-ministres, les cyber-rencontres des sous-ministres et lors des réunions de divers organes de décision exécutifs au besoin.

Exception faite de ce qui précède, plusieurs provinces « pourraient » avoir accès aux ministres avant de faire un compte rendu, mais ce n'est pas la norme et cela ne se produit que rarement pour ces provinces.

Il convient de noter que cette année, l'Ontario aura pour la toute première fois accès à la haute direction et mènera un exercice de guerre virtuelle (Cyber War Game) avec des participants de différents ministères.

C'est un fait que les ministres représentent tous d'excellentes cibles pour les acteurs de menaces malveillantes. Étant continuellement dans l'œil du public, un nombre important d'informations personnelles sont souvent révélées à propos d'eux sur les médias sociaux ainsi que dans les médias d'information. Il est essentiel que les ministres soient informés et sensibilisés aux cyber-menaces susceptibles d'avoir un impact sur eux et qu'ils apprennent à y répondre.

Sous-comité national
des DPI sur la
protection des renseignements



EN CONCLUSION

Si vous avez d'autres préoccupations ou questions, contactez l'un des membres du SNDPI :

- **Président du SNDPI** : Martin Dinel, DPSI de l'Alberta | Martin.Dinel@gov.ab.ca | Téléphone : 780 427-2429
- **Vice-président du SNDPI** : Robert Samuel, DPSI de la Nouvelle-Écosse | Robert.Samuel@novascotia.ca | Téléphone : 902 222-6685
- **Secrétaire du SNDPI** : Gary Perkins, DPSI de la Colombie-Britannique | Gary.Perkins@gov.bc.ca | Téléphone : 250 387-7590