CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la défense nationale

NDDN • NUMÉRO 065 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 25 octobre 2017

Président

M. Stephen Fuhr

Comité permanent de la défense nationale

Le mercredi 25 octobre 2017

● (1530)

[*Traduction*]

Le président (M. Stephen Fuhr (Kelowna—Lake Country, Lib.)): Je vous souhaite la bienvenue à notre dernière réunion sur la crise en Ukraine et je souhaite également la bienvenue aux trois témoins avec lesquels nous discuterons de cet enjeu aujourd'hui. Nous avons Alan Bell, président de Globe Risk International, et Stuart Wright, dirigeant principal de la sécurité de l'information chez Aegis Technologies, qui témoigne à titre personnel, et nous attendons encore l'arrivée de Viktor Siromakha. Nous l'inscrirons comme dernier intervenant à prendre la parole en vue de pouvoir commencer la réunion.

Merci à tous. Je crois comprendre que vous avez été informés que vous avez 10 minutes pour faire votre exposé. Je vous saurais vraiment gré de bien vouloir respecter le plus possible cette limite, parce que cela me permettra de donner aux membres du Comité l'occasion de poser des questions.

Monsieur Wright, vous avez la parole.

M. Stuart Wright (responsable de la cybersécurité, Aegis Technologies, à titre personnel): Premièrement, j'aimerais vous remercier de m'avoir demandé de témoigner ici à Ottawa pour informer ces éminents députés.

Je m'appelle Stuart Wright, et je témoigne aujourd'hui à titre personnel.

J'ai travaillé dans le domaine de la réglementation, de l'énergie, y compris le pétrole, le gaz naturel et le transport, la distribution et la production d'électricité, et de la vérification relative aux systèmes d'information et j'ai occupé divers postes de direction durant de nombreuses années. Je possède une bonne expertise et j'ai une perspective unique en ce qui concerne la cybersécurité en Amérique du Nord.

Je suis ici aujourd'hui pour vulgariser les événements qui se sont déroulés en Ukraine et en Europe de l'Est relativement à la cybersécurité. J'espère que mon témoignage vous aidera dans votre évaluation des mesures appropriées et des prochaines étapes pour soutenir nos alliés de l'OTAN et renforcer la capacité militaire du Canada en vue d'intervenir face à un nouveau type de guerre.

Cette semaine, des cyberattaques utilisant le maliciel Bad Rabbit ont frappé mardi la Russie et d'autres pays; elles ont touché l'agence de presse Interfax et ont retardé des vols à l'aéroport d'Odessa en Ukraine. Le rançongiciel Bad Rabbit est un type de virus qui verrouille les ordinateurs infectés et qui demande aux victimes de verser une rançon pour recouvrer l'accès à leurs appareils. Même si aucune panne majeure n'a été rapportée, plusieurs gouvernements ont émis des avertissements concernant l'attaque, qui fait suite aux campagnes de mai et de juin où un maliciel similaire a été utilisé et a entraîné des pertes de plusieurs milliards de dollars, selon certains économistes. Cette nouvelle série d'attaques est préoccupante, parce que les attaquants ont rapidement infecté les infrastructures essentielles, y compris des exploitants de services de transport, ce qui laisse entendre que c'était une attaque bien coordonnée.

Certaines entreprises de cybersécurité ont indiqué que Bad Rabbit a semblé se propager par le biais d'un mécanisme similaire à celui employé en juin par le virus NotPetya qui a perturbé les activités de nombreux organismes gouvernementaux et entreprises en Ukraine. Le maliciel s'est ensuite propagé par le biais de réseaux de multinationales qui ont des activités ou des fournisseurs en Europe de l'Est. Selon les premiers rapports au sujet de Bad Rabbit, plus de la moitié des victimes se trouvaient en Russie; viennent ensuite l'Ukraine, la Bulgarie, la Turquie et le Japon.

J'aimerais maintenant parler de la cyberattaque de 2015 en Ukraine, comme vous me l'avez demandé. Le 23 décembre 2015, des cyberforces inconnues ont réussi pour la première fois à perturber un réseau électrique, ce qui a causé d'importantes pannes d'électricité qui ont touché plus de 225 000 clients en Ukraine. Les conséquences de cette cyberattaque ont été ressenties dans plusieurs régions du pays qui sont restées sans électricité durant plusieurs heures. Le maliciel BlackEnergy a contribué à rendre possible cette attaque.

En décembre 2016, pratiquement un an plus tard jour pour jour, il y a eu une autre panne d'électricité qui était de moins grande envergure et qui a seulement duré une heure. Une seule région a été touchée, mais l'attaque a été menée grâce à un maliciel plus évolué, soit Industroyer, qui est soupçonné d'être à l'origine de cette panne.

Ces cyberincidents ont touché des exploitants de l'industrie de l'électricité, mais les tactiques utilisées lors de ces attaques auraient facilement pu déjouer n'importe quel exploitant, tous secteurs confondus, dans n'importe quelle région de n'importe quel pays. Ce qui importe ici, c'est que les cybermenaces ne sont plus seulement le problème des administrateurs de réseaux informatiques et des ingénieurs en TI; cela doit être au coeur de nos préoccupations si nous voulons exploiter des infrastructures essentielles de manière sécuritaire, efficace et résiliente.

J'aimerais maintenant parler du contexte mondial. Les cyberattaques dans le monde sont maintenant menées de manière concertée. Ce sont des efforts orchestrés en vue d'exploiter les vulnérabilités des personnes, des systèmes et des processus. Ces attaques ont des répercussions à long terme et sont souvent menées par des professionnels en vue d'utiliser l'infrastructure réseau d'un organisme contre lui-même de manière hautement ciblée.

Dans la définition traditionnelle d'une guerre, les infrastructures essentielles étaient une cible inopinée valable, parce que cela empêche l'ennemi de les utiliser, les rendant ainsi inutiles. Sécurité publique Canada définit les infrastructures essentielles comme « l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sécurité ou le bien-être économique des Canadiens ainsi que le bon fonctionnement du gouvernement ». La perturbation des services d'un fournisseur d'infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes et pourrait considérablement ébranler la confiance du grand public. Autrement dit, les infrastructures essentielles sont une cible facile et de choix.

Par le passé, les infrastructures essentielles étaient faciles à défendre, étant donné que seules les ressources aériennes, terrestres et maritimes d'un ennemi pouvaient les atteindre. Le déploiement de telles ressources pouvait laisser entrevoir du mouvement, et nous pouvions intervenir en ayant recours à des capacités de défense conventionnelles, même si la cible exacte est inconnue. C'était particulièrement pertinent à l'époque où les guerres étaient livrées entre des États, comme les campagnes de bombardement que nous avons connues lors de la Seconde Guerre mondiale et les conflits politiques et militaires de la fin du XX^{e} siècle.

Cependant, dans notre époque géopolitique moderne, il y a maintenant d'autres ressources dans le cyberespace qui ont une portée pratiquement planétaire et qui requièrent peu de déplacement ou aucun déplacement. En fait, la nature de la guerre et des conflits a évolué. Ces ressources cybernétiques peuvent maintenant être rapidement déployées et ne sont jamais physiquement exposées à l'ennemi. Elles permettent de cibler des infrastructures essentielles à l'intérieur des frontières de l'État ou de mener des attaques efficaces contre des cibles par le biais de mandataires en utilisant des techniques, des tactiques et des procédures.

Le ministère de la Défense nationale, ses partenaires de l'OTAN et ses alliés stratégiques en Europe, en Asie et au sud de la frontière doivent revoir les doctrines militaires nécessaires pour orienter efficacement nos stratégies de cyberguerre. Cela inclut nos capacités et les éléments fondamentaux en matière de formation, de renseignement et de soutien pour veiller à la sécurité et à la stabilité de nos alliés et de nos partenaires régionaux.

● (1535)

Les mêmes techniques, tactiques et procédures sont ce qui sépare le cybercriminel moyen des acteurs malveillants expérimentés, et ces menaces persistantes avancées sont en fait une série de processus furtifs de piratage informatique qui sont menés de façon continue par une personne ou un groupe de personnes pour cibler une entité précise.

Une menace persistante avancée vise des organismes privés, des États ou les deux. Des menaces persistantes avancées peuvent prendre pour cible des infrastructures essentielles ou des actifs d'un État comme les institutions financières; les systèmes énergétiques; les transports automatisés; la gestion de l'eau potable et des eaux usées; les systèmes de communication et les systèmes pour premiers répondants, comme nous en avons été témoins au cours de la dernière semaine, et bien entendu nos capacités, nos réseaux et nos éléments essentiels de défense.

Aucune industrie verticale ou aucun secteur n'est à l'abri, et nous assistons maintenant à l'évolution d'une guerre hybride. Pour vous mettre l'expression en contexte, nous pouvons parler d'une guerre hybride pour décrire à titre officieux la complexité et la dynamique en constante évolution du champ de bataille, ce qui inclut le recours à la cyberguerre avant de passer à une action militaire de plus grande envergure.

Je vais maintenant discuter des attaques qui ont eu lieu au cours des dernières années et qui ont ciblé le réseau électrique d'Ukraine en 2015 et en 2016 ainsi que les attaques dans les pays baltes en 2015.

De manière chronologique, nous examinerons tout d'abord le maliciel qui a servi à comprendre les outils qui ont été utilisés pour perpétrer ces attaques. Deuxièmement, nous regarderons le déroulement des attaques et la façon dont ces attaques ont été menées. Enfin, nous nous tournerons vers l'avenir, et je vous donnerai mon point de vue sur l'avenir de la cyberdéfense des infrastructures essentielles relativement à la guerre irrégulière ou à la « guerre hybride », expression qui a récemment été inventée, ainsi que les occasions qui s'offrent au ministère de la Défense nationale, à l'OTAN et au NORAD de renforcer notre capacité d'intervention face à ce nouveau type de menace.

Premièrement, en ce qui a trait au maliciel utilisé pour perpétrer ces attaques, lorsqu'il est question d'une cyberattaque d'envergure, il y a normalement une description sommaire du maliciel accompagnée d'une photo. Vous l'avez tous déjà vue. C'est comme dans *La Matrice*: un écran vert sur un fond noir ou un individu louche dont la face est voilée et qui vous demande de lui envoyer des bitcoins. La donne a maintenant évolué.

Vous voyez dans les reportages des descriptions techniques en vue de présenter une histoire accrocheuse pour stimuler l'intérêt des lecteurs. Cependant, cela ne fournit pas nécessairement une compréhension approfondie de la façon dont l'attaque a été perpétrée. En revanche, si nous adoptons une approche technique pour comprendre ces attaques en misant sur de solides explications, cela limite souvent l'audience. Cependant, cette situation restreint la capacité du travail de situer les attaques dans un contexte plus vaste ou mondial. Par conséquent, j'espère fournir au Comité une approche équilibrée et mitoyenne en vue de vous expliquer pourquoi et comment le maliciel fonctionne, sans trop entrer dans les détails d'ordre technique. Vous ennuyer avec de tels détails, c'est bien la dernière chose que je souhaite.

Le maliciel BlackEnergy, qui aurait été utilisé lors des attaques en Ukraine, est un cheval de Troie, soit un programme qui cache en fait ses mauvaises intentions. Il pénètre dans le système par le biais de l'envoi d'un fichier ou d'une campagne d'hameçonnage par courriel. Nous avons tous déjà reçu ces types de courriels, que nous appelions par le passé l'arnaque nigérienne par courriel, nous demandant de transférer de l'argent des pays africains pour débloquer des millions de dollars; cette arnaque repose sur l'urgence d'agir.

Dans les entreprises et les gouvernements, les cadres supérieurs reçoivent sans cesse des demandes de la part de leur équipe pour approuver ou autoriser des opérations financières internes — ayant trait aux services financiers généraux ou à l'approvisionnement — en vue de transférer de grosses sommes dans des banques en Asie, et ce, généralement lorsqu'ils sont sur le point de partir en vacances ou de s'en aller au chalet. Ce sont des campagnes ciblées. Nous appelons cela des campagnes de harponnage. Ces courriels ressemblent aux messages que les victimes ont l'habitude de recevoir quotidiennement dans le cadre de leur travail, au lieu de prendre une forme plus générique comme dans le cas d'une campagne d'hameçonnage, où les individus misent plutôt sur la quantité.

Une fois le maliciel téléchargé, il permet à l'attaquant de lancer une attaque par saturation et de télécharger des plugiciels personnalisés visant l'envoi de pourriels et le vol de renseignements. Autrement dit, lorsque BlackEnergy a infecté les systèmes en Ukraine, il a pu servir de porte d'entrée pour la prochaine étape de l'attaque, soit l'installation d'autres maliciels en vue de recueillir du renseignement et de faciliter les futures attaques.

Je tiens à vous expliquer qu'il y a plusieurs variantes de ces infections. Cela comprend BlackEnergy 2, qui est un outil plus précis utilisé pour inspecter des systèmes précis, et BlackEnergy 3, qui vise à fouiller un réseau à la recherche de systèmes précis ou alléchants, y compris ceux ayant trait au gouvernement, à l'armée et aux infrastructures à l'étranger. Ces variantes permettent de scruter un réseau et offrent un moyen pour propager l'infection.

La menace est présente. Après la première infection, le maliciel BlackEnergy installe l'utilitaire KillDisk sur le système. Cette partie de l'attaque rend inutilisables les systèmes au sein de l'infrastructure et permet à l'auteur malveillant de supprimer une composante centrale des systèmes infectés et ainsi nuire aux efforts de restauration. Lorsque l'utilitaire KillDisk est exécuté, il supprime ou écrase tous les principaux systèmes, y compris les enregistrements d'amorçage maître, ce qui arrête les systèmes et empêche leur redémarrage. Cela camoufle encore plus les activités de l'attaquant dans le système et masque la nature et l'origine réelles de l'auteur malveillant.

C'est fondamental lorsque vous analysez l'incident et que vous tentez de déterminer qui est l'auteur malveillant et en gros la personne que vous voulez pourchasser si vous optez pour une mesure d'intervention et de restauration.

● (1540)

BlackEnergy et KillDisk fonctionnent de concert, et c'était particulièrement vrai lors de l'attaque sur le réseau électrique en Ukraine en 2015. Les ennemis actuels et futurs sont susceptibles d'avoir davantage recours à un mélange d'approches conventionnelles et irrégulières par rapport aux conflits, ce que nous appelons une guerre hybride, comme je l'ai déjà mentionné, et ce sera peut-être un prélude aux attaques cinétiques.

Par ailleurs, une autre variante, soit Industroyer, aurait été le maliciel derrière l'attaque sur le réseau électrique ukrainien en 2016. Elle peut être fortement personnalisée avec des maliciels, et des chercheurs croient que ce maliciel cible des systèmes de contrôle industriel. Si nous examinons les rapports des dernières semaines, il devient vraiment de plus en plus envahissant. C'est un outil malveillant dans les mains d'un attaquant dévoué, bien financé et tenace. Ce n'est pas quelque chose qu'un pirate adolescent peut trouver sur le Web invisible et tout bonnement exécuter.

Le maliciel est capable de survivre dans des réseaux compromis et perturber directement les processus de travail essentiels dans ces installations. Il est extrêmement dangereux. Les dommages qu'il peut causer dépendent de la configuration des installations et peuvent varier d'un poste à l'autre, par exemple. Cela peut prendre la forme d'une simple panne locale, d'une défaillance en cascade ou même de dommages importants au matériel. Les faibles effets relatifs des récentes pannes contrastent grandement avec la complexité technique du présumé maliciel derrière Industroyer. Ces acteurs malveillants sont des institutions gouvernementales.

De l'opinion d'un grand nombre de chercheurs spécialisés dans le domaine de la sécurité, une possible explication est que c'était un essai à grande échelle. Les agents malveillants mettent à l'essai nos mesures de défense du périmètre, repoussent les limites et observent nos capacités d'intervention et de restauration. C'est une approche calculée et stratégique à l'égard de la guerre hybride.

Le milieu de la sécurité en Amérique du Nord a comparé Industroyer à la cyberarme Stuxnet — j'ai déjà travaillé chez Siemens — qui avait été utilisée pour viser le programme nucléaire iranien.

Je vais passer directement au déroulement des attaques. Je vois le président...

Je vous expliquerai rapidement comme se sont déroulées les attaques sur le réseau électrique et le contexte de chaque attaque.

Trois attaques ont été examinées: en Ukraine, dans les pays baltes et en Ukraine. Avant de traiter de chaque attaque, il est important de souligner le groupe auquel nous attribuons ces attaques.

Premièrement, les renseignements disponibles nous permettent seulement d'attribuer l'attaque en Ukraine à Sandworm, soit une menace persistante avancée que nous croyons être un groupe de pirates associé au gouvernement russe. Lors des attaques dans les pays baltes en 2015, des chercheurs ont affirmé avoir vu des preuves de la présence de Sandworm, mais ils n'étaient pas prêts à en fournir la preuve pour des raisons opérationnelles. C'est une partie du défi auquel nous sommes confrontés dans l'industrie en ce qui a trait aux méthodes d'intervention et de restauration. La confiance est essentielle pour mener à bien une intervention. Cependant, dans de nombreux cas, cela prend des mois, voire des années, pour déterminer tous les faits.

Enfin, pour ce qui est de l'attaque en Ukraine, l'utilisation d'Industroyer n'a pas encore officiellement été attribuée à un pays ou à un acteur. Par conséquent, aux fins de cette partie, les spécialistes du secteur privé s'entendent pour dire que l'attaque a été lancée par des Russes. Je répète que seuls le temps et une diligence raisonnable nous permettront de confirmer cette hypothèse.

Je vais passer les attaques, parce que je crois que nous avons passablement traité de la question; j'aimerais me concentrer sur les attitudes dominantes.

Le président: Je m'excuse énormément, mais je vais devoir vous arrêter là. J'espère que vous aurez l'occasion de traiter du reste de votre exposé lors des questions, mais je dois céder la parole à M. Bell.

M. Alan W. Bell (président, Globe Risk International inc.): Bonjour, mesdames, messieurs. Merci de m'avoir invité à témoigner aujourd'hui devant votre comité.

La Russie devient progressivement plus paranoïaque, étant donné qu'un grand nombre de pays de l'ancien bloc soviétique ont présenté des demandes pour devenir membres de l'Union européenne ou de l'OTAN. Cela agace la Russie, parce qu'elle doit conserver un avantage stratégique sur les pays de l'ancien bloc soviétique le long de ses vastes frontières. Elle aura besoin de ce champ de bataille pour manoeuvrer en cas de menace ou d'attaque éventuelle de l'OTAN. Compte tenu de son passé, la Russie n'est pas prête à être envahie de nouveau.

Lorsque la Russie a illégalement envahi la Crimée, elle a eu recours à une stratégie militaire associée à la guerre hybride qui allie de manière simultanée la guerre conventionnelle, la guerre irrégulière et la cyberguerre pour arriver à ses fins. En menant des opérations cinétiques et en misant sur d'autres activités subversives, les Russes ont tenté d'éviter l'attribution et la rétribution.

En pratique, le concept russe d'un conflit non linéaire illustre bien une stratégie typique d'une guerre hybride. Une guerre non linéaire est livrée lorsqu'un État emploie des forces militaires inhabituelles, conventionnelles et irrégulières de concert avec des attaques psychologiques, économiques, politiques et cybernétiques. Une guerre hybride peut se décrire comme l'utilisation d'une dynamique complexe et flexible du champ de bataille, ce qui à son tour nécessite une capacité d'intervention hautement adaptable, bien préparée et résiliente. Malheureusement, ni l'armée ukrainienne ni l'OTAN n'avait une résilience suffisante pour intervenir ainsi lorsque cela s'est produit.

La confusion et le chaos s'ensuivent lorsque l'information est utilisée comme arme pour exacerber la perception d'insécurité au sein d'une population et dresser des groupes culturels, sociaux et politiques les uns contre les autres et qu'il y a de nombreux responsables probables. Si nous utilisons le conflit ukrainien comme exemple, les tactiques hybrides russes ont grandement été utilisées lors de l'annexion de la Crimée. La guerre civile qui a suivi dans l'Est de l'Ukraine a carrément pris de court l'Occident, en particulier les États-Unis et le Royaume-Uni qui étaient incapables de préparer une quelconque réponse.

L'inaction de l'OTAN peut au moins être partiellement attribuée à son organisation militaire rigide actuelle. Plus important encore, les experts militaires et du renseignement russes ont réussi à déterminer avec précision et à exploiter les cadres juridiques internationaux régissant le recours à la force contre un autre État souverain.

La stratégie militaire de l'OTAN doit par-dessus tout mettre l'accent sur une pensée non linéaire lors du processus de modélisation de conflits. L'armée canadienne, même si elle est consciente que d'autres ont recours à la guerre hybride, n'est pas formée pour adopter une pensée non linéaire lors de son processus de planification et de modélisation de conflits. Pour l'instant, il n'y a eu aucune intervention concrète de la part de l'Occident ou de l'OTAN par rapport à l'agression russe en Crimée ou en Ukraine, si nous faisons abstraction de l'aide politique et économique offerte.

Si nous ne refondons pas le cadre juridique qui définit un acte d'agression, d'autres démocraties libérales peuvent courir un risque. Il semble de plus en plus évident que le principal moyen d'assurer le maintien de la primauté du droit est de revoir notre interprétation traditionnelle des conflits. L'Occident doit élaborer un cadre sur la dissuasion stratégique pour contrer l'utilisation comme armes de l'information, de l'argent et d'autres formes subversives d'agression. Une politique uniforme ne sera plus une mesure efficace de dissuasion à l'avenir.

Dès le début de l'engagement russe dans la guerre hybride en Crimée, les gens se sont énormément appliqués à garder un certain niveau de démenti plausible. Le drapeau russe a été hissé par des habitants de la Crimée et non des militaires russes. Les forces russes n'arboraient aucun insigne ou marque pouvant les identifier. Des cyberattaques ont été lancées contre des installations et des systèmes liés aux infrastructures essentielles en Ukraine et ont été structurées de manière à tenter de camoufler l'implication russe.

Il est évidemment généralement entendu que la Russie était responsable de la violation de la souveraineté de l'Ukraine. Cependant, la confusion qu'ont entraînée les campagnes de désinformation, les cyberattaques, les forces spéciales russes sans insigne et les événements qui ont suivi dans l'Est de l'Ukraine a fait en sorte que l'Occident a continué de rester là sans intervenir, ce qui a permis aux Russes de consolider et de normaliser l'annexion de la Crimée par la Fédération de Russie.

Les concepts de la guerre hybride ne sont pas enseignés aux officiers du ministère de la Défense nationale, ce qui signifie que le ministère de la Défense nationale n'est pas en mesure de tenir compte des signes manifestes d'une guerre hybride lors de la planification d'opérations militaires futures. Pourquoi?

● (1545)

C'est parce que nous n'adoptons pas une approche pangouvernementale et que nous n'examinons pas complètement ces concepts d'un point de vue psychologique, éducatif, économique, militaire, financier, politique, légal et cybernétique, ainsi que sur le plan du renseignement et de la sécurité des communications. À ma connaissance, aucun pays membre de l'OTAN, à l'exception des États-Unis, ne prévoit des processus tels que la planification relative aux méthodes de guerre hybrides et aux conflits linéaires.

Comment pourrons-nous à l'avenir nous préparer et nous entraîner à combattre les mesures de guerre hybrides prises activement par les Russes, comme celles qu'ils infligent actuellement à l'échelle mondiale, si nous ne comprenons pas comment ces mesures fonctionnent? Ce changement exige maintenant que les États-Unis et leurs alliés souscrivent à une nouvelle interprétation légale, psychologique et stratégique de la guerre et du recours à la force, en particulier par la Russie.

En ce qui concerne les options en matière d'aide internationale canadienne et de mission de maintien de la paix de l'ONU en Ukraine, de nombreuses questions doivent être posées avant de s'engager dans une voie ou une autre. Par exemple, où et comment la paix serait-elle maintenue, et comment y arriver? La Russie souhaite participer à toute mission de maintien de la paix future. Toutefois, il est impossible que la Russie y participe, parce qu'elle est l'agresseur dans ce conflit.

À quoi ressemblerait une mission de maintien de la paix en Ukraine de l'Est? Quelles sont les règles d'engagement de l'opération Unifier dans l'éventualité d'une attaque par des forces hostiles? Des plans ont-ils été élaborés afin de gérer les acteurs russes implantés dans le gouvernement et l'armée de ce pays?

Le droit de veto de la Russie au Conseil de sécurité l'emporterait sur toute ambition canado-ukrainienne en matière de maintien de la paix.

Le gouvernement actuel pourrait trouver attrayante, en surface, l'idée de contribuer à une intervention menée par les Nations unies en Ukraine ou dans les districts sécessionnistes de l'Est qui sont en difficulté, étant donné que cette mesure cadrerait avec son mantra « le Canada est de retour » et lui permettrait, en même temps, d'honorer l'engagement qu'il a pris de fournir 600 soldats et 150 agents de police pour les opérations de soutien au maintien de la paix que l'ONU mène à l'étranger. Les gens parlent de la possibilité de confier à l'ONU une mission de maintien de la paix en Ukraine depuis 2015 et, jusqu'à maintenant, rien ne s'est produit.

En ce qui a trait à nos options, la première étant de déployer des Casques bleus de l'ONU en Ukraine, la Russie pourrait approuver ou non une telle mission. Les Russes pourraient exiger d'y participer, et j'ignore comment cela serait accompli. La mission de maintien de la paix pourrait être dirigée par le Canada. Cependant, la Russie pourrait utiliser son droit de veto pour s'y opposer, étant donné que le Canada pourrait être considéré comme trop proche des États-Unis.

Le temps requis pour discuter d'une force de maintien de la paix de l'ONU, puis l'organiser et la déployer pourrait être considérable et osciller entre deux et trois ans. Pour l'instant, le Canada a convenu qu'une mission future pourrait aider, tout en indiquant qu'il n'avait pas encore choisi l'endroit où il allait affecter les FAC à un rôle de maintien de la paix.

En ce qui concerne la deuxième option, que faut-il faire au chapitre de la formation pour offrir aux militaires ukrainiens des cours de formation sur toutes les opérations militaires hybrides? Il ne s'agit pas seulement d'une formation de base, mais plutôt d'une formation plus complète et dynamique. La solution consiste à pourvoir en personnel un collège de commandement capable de donner des cours de formation sur toutes les opérations militaires hybrides aux officiers militaires supérieurs et subalternes de l'Ukraine. Il faut aussi que nous formions le gouvernement ukrainien ainsi que les militaires dans le domaine de la cybersécurité et de l'évaluation des menaces liées aux systèmes.

En outre, un certain nombre de questions doivent toujours être posées. Quelles sont les règles d'engagement des Forces armées canadiennes et leur capacité sur place d'extirper au besoin ces 200 soldats canadiens? S'ils sont attaqués, entourés et forcés de se rendre, comment le MDN planifiera-t-il de répondre à la prochaine vague offensive de la Russie en Ukraine? Les FAC ont-elles élaboré des plans d'évacuation adéquats pour répondre à tous les scénarios possibles, et ces plans ont-ils été mis à l'épreuve? Le Canada est-il prêt à faire face à une escalade de combats, et quelles seraient les conséquences pour les équipes de formation militaire qui se trouvent en Ukraine en ce moment?

Le reste de mon exposé reproduit essentiellement ce que mon collègue a présenté. Par conséquent, je n'irai pas jusque-là. Je vais vous fournir un compte rendu complet et détaillé de mon exposé, au cas où quelqu'un aurait besoin de le lire plus tard.

Merci beaucoup.

● (1550)

Le président: D'accord. Merci beaucoup.

Puisque c'est la première fois que vous comparaissez devant notre comité, je vous précise que, si vous êtes en train de répondre à une question, mon signal signifie habituellement qu'il vous reste 30 secondes avant que je donne la parole au prochain intervenant. Je fais ce signal afin que tous puissent bénéficier de leur temps de parole.

Monsieur Wright, je m'excuse de vous avoir interrompu. Vous êtes la personne la plus qualifiée que notre comité ait entendue au sujet de la cybersécurité. Par conséquent, j'espère que les séries de questions nous permettront de découvrir ce que vous alliez dire, parce que nous savons que cet aspect joue un rôle important dans les événements qui surviennent en Ukraine.

Cela dit, je vais céder la parole à M. Spengemann.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci beaucoup, monsieur le président.

Messieurs, je vous remercie d'être parmi nous pour nous faire part de votre expertise.

Monsieur le président, je pourrais peut-être vous demander de laisser M. Wright finir son exposé, brièvement, en une minute ou deux, peut-être en faisant une simple liste de points. Je crois que ce qu'il était en train de dire est important.

M. Stuart Wright: Je m'excuse. Ma femme me dit toujours que je suis bavard, donc je vais vous présenter mon appel à l'action, ma conclusion.

Premièrement, je recommande de revoir et d'adapter la doctrine officielle du ministère de la Défense nationale afin de prescrire plus en détail comment le ministère et ses partenaires stratégiques, dont l'OTAN, peuvent intégrer les tactiques militaires de guerre, y compris en matière de cybersécurité.

Deuxièmement, il faudrait créer et adopter un manuel sur l'adaptation aux contre-mesures, puis établir un mécanisme afin que seuls nos partenaires de confiance puissent connaître nos outils d'intervention et de rétablissement, ce qui comprendrait la création d'un centre conjoint, tel que mentionné par mon collègue.

Troisièmement, il faudrait adopter des lignes directrices, un code de pratique ou un cadre afin d'améliorer les mesures d'intervention et de rétablissement, parce qu'il est fort probable que nous serons touchés, compte tenu du nombre d'attaques toujours en hausse; nous devrons accroître notre résilience et notre souplesse.

Quatrièmement, il faut adopter des mesures, des outils, des techniques et prévoir des ressources à l'appui des efforts susmentionnés.

Pour terminer, il faut continuellement tester et adapter nos mesures d'intervention et veiller au maintien constant de capacités opérationnelles au Canada comme à l'étranger.

● (1555)

M. Sven Spengemann: Merci infiniment.

Monsieur Wright, pour placer tout cela dans un contexte plus général, qui tient compte de tous les problèmes auxquels est confronté le gouvernement dans la région du Donbass, pouvez-vous nous donner une idée de l'ampleur du problème des logiciels malveillants et des cyberattaques? Y a-t-il des filets de sécurité non informatiques, des formes d'immunisation, outre les contre-attaques et les mécanismes de cyberdéfense, que le gouvernement actuel de l'Ukraine pourrait mettre en place pour s'immuniser ou se protéger?

M. Stuart Wright: À la lumière des incidents récents survenus aux États-Unis, des attaques d'Equifax ou d'autres incidents comme la cyberattaque contre Dyn, qui ont paralysé toute la sécurité Internet de la côte Est, on voit que les meilleures méthodes de l'industrie sont utilisées en Amérique du Nord. Nous avons tout intérêt de mettre à profit ces outils, ces connaissances et ces apprentissages et à les appliquer dans des pays éloignés comme l'Ukraine.

La stratégie de défense et de mesure de la profondeur que le pays a adoptée pour protéger son infrastructure essentielle est bonne. Il faut désormais penser en termes d'intervention et de rétablissement. Nous savons que nous serons frappés. Nous savons à quel point les attaques peuvent être complexes. Cela n'ira qu'en augmentant. Nous devons pouvoir travailler avec l'Ukraine et lui fournir des renseignements sur le niveau actuel de menace, puis intervenir de manière appropriée, avec les bonnes équipes tactiques.

M. Sven Spengemann: Les deux attaques que vous avez décrites, survenues en 2015 et en 2016, sont-elles les plus graves, les plus étendues et les plus complexes auxquelles l'OTAN a été confrontée sur le terrain?

M. Stuart Wright: À ce jour. Encore une fois, ce sont les attaques qui ont été déclarées en Ukraine et en Europe de l'Est. D'après ce que nous comprenons, ce sont celles qui ont été les plus répandues. Elles ont réussi à perturber les activités et à paralyser le réseau, si bien qu'il a fallu déployer beaucoup d'efforts pour rétablir le courant et l'infrastructure critique.

Nous constatons qu'ils testent le périmètre ici. Ils sont en train de déterminer comment nous réagissons. Ils ne voient pas ces attaques comme une façon de paralyser le réseau plus encore. Ils sont en train de tester notre vitesse d'intervention, de déterminer qui nous faisons intervenir et quels sont nos mesures et nos mécanismes. Il faut commencer à analyser la situation sous l'angle stratégique. Ils sont en train de tester le périmètre. Nous n'avons pas encore été frappés de plein fouet.

M. Sven Spengemann: Merci beaucoup, monsieur Wright.

Laissons un peu de côté les cyberattaques. Je suis certain que mes collègues auront d'autres questions à vous poser à ce sujet.

M. Stuart Wright: C'est certain.

M. Sven Spengemann: Monsieur Bell, très brièvement, pouvez-vous nous présenter un peu ce que fait Globe Risk International?

M. Alan W. Bell: Nous sommes consultants en sécurité internationale, et nous menons la plupart de nos projets dans des pays hostiles.

M. Sven Spengemann: Géographiquement, où déployez-vous votre expertise?

M. Alan W. Bell: J'ai passé 23 ans au sein des Forces spéciales britanniques. J'ai ensuite immigré au Canada, où j'ai ma propre entreprise depuis 21 ans maintenant.

M. Sven Spengemann: Merci beaucoup. Je vais vous poser quelques questions.

Monsieur Siromakha, je vous souhaite la bienvenue au Comité. N'hésitez pas à intervenir pour répondre aux questions vous aussi.

Colonel Viktor Siromakha (attaché de la défense, de la marine et de l'aviation, Ambassade de l'Ukraine): Merci infiniment.

M. Sven Spengemann: Monsieur Bell, vous avez parlé d'une mission de maintien de la paix. Croyez-vous qu'il y ait une façon, politiquement, d'organiser une mission de maintien de la paix dirigée par l'ONU dans la région du Donbass sans l'accord, l'appui ni l'approbation de la Russie?

M. Alan W. Bell: Je pense que ce sera difficile sans le consentement de la Russie, parce que la Russie a un droit de veto à l'ONU et qu'elle peut vraiment y dicter ce qu'elle veut. Elle pourrait se tailler une place de force au sein de cette mission pour s'attribuer le rôle qu'elle souhaite, et je ne vois pas trop comment l'ONU pourrait l'en empêcher.

M. Sven Spengemann: Croyez-vous qu'il serait politiquement possible d'établir une telle mission avec la participation des Russes?

M. Alan W. Bell: Oui. Ce sera difficile, parce que nous ne connaissons pas les intentions des Russes. Ils se sont arrêtés dans la région du Donbass. À cette heure-ci, la semaine prochaine, ils pourraient se trouver ailleurs. Nous ne savons pas ce qu'ils feront. Le fait que l'OTAN n'ait rien fait pour les arrêter et qu'elle ne leur ait pas demandé de rendre des comptes poussera probablement les Russes à oser être de plus en plus audacieux dans leurs actions. Les autres pays de l'ancien bloc soviétique voisins de la Russie craignent d'être les prochaines cibles. Ce pourrait être la première de nombreuses incursions dans ces pays.

M. Sven Spengemann: Le Comité a recueilli le témoignage de l'ambassadeur Waschuk, qui a laissé entendre que le prix allait monter pour Poutine, s'il veut conserver sa mainmise sur la région du Donbass ou à tout le moins l'occuper. Êtes-vous d'accord avec cela?

M. Alan W. Bell: Oui.

M. Sven Spengemann: Quels seraient les principaux facteurs pour lesquels ce prix va augmenter?

M. Alan W. Bell: Jour après jour, nous (et par nous, j'entends l'Occident et l'OTAN, je ne regrouperai que ces deux-là) ne faisons rien mis à part sur le plan politique, si bien que personne ici n'en saura probablement rien, et ils seront de plus en plus téméraires. Ce n'est qu'un début. Ils en ont le pouvoir. Le but de l'armée russe est de mener la guerre sur les terres qui bordent les frontières russes; elle est prête à faire la guerre. Bien sûr, aucun des autres pays de l'ancien bloc soviétique n'est en mesure de se défendre de ce genre d'attaque.

● (1600)

M. Sven Spengemann: Serait-il futé de se demander si M. Poutine a un plan de sortie de la région du Donbass ou seriez-vous porté à croire qu'il ne sait même pas comment il en sortira à ce stade-ci?

M. Alan W. Bell: Je pense qu'il tâte le terrain. La seule chose qui pourrait changer, d'après moi, c'est qu'il pourrait perdre le pouvoir au profit d'une autre personne avec qui il serait un peu plus facile de négocier. Cela ne semble toutefois pas se dessiner à courte échéance. Donc moins nous en ferons pour lui mettre des bâtons dans les roues, plus il voudra probablement intensifier ses attaques.

M. Sven Spengemann: Merci, monsieur Bell.

Monsieur Siromakha, j'aimerais vous demander de répondre à la même question, sachant que je n'ai presque plus de temps et donc, que mes collègues poursuivront probablement avec vous. Comment voyez-vous la sortie de Poutine du Donbass? Y en a-t-il une qui se profile? Qu'est-ce qui nous attend, d'après vous?

Col Viktor Siromakha: Je pense que le rêve de M. Poutine est de créer quelque chose qui ressemblerait à l'Union soviétique. Pour cet homme assez âgé et expérimenté, ce serait probablement l'oeuvre de sa vie. Il essaie probablement de terminer son tour de piste à titre de président de la Russie par un très grand coup, afin de créer quelque chose de très gros et de très fort.

M. Sven Spengemann: Monsieur le président, je pense que c'est tout le temps que j'avais. Merci.

Le président: Merci.

Colonel, je vous remercie d'être parmi nous. J'aimerais vous inviter à vous joindre à la conversation, officiellement. Je vais vous donner 10 minutes pour présenter un exposé, après quoi je relancerai la période de questions avec M. Hoback.

Colonel, la parole est à vous.

Col Viktor Siromakha: Merci infiniment, monsieur.

Honorables président du Comité et députés, mesdames et messieurs, je vous remercie de me fournir l'occasion de présenter aujourd'hui la compréhension ukrainienne du conflit qui fait rage dans l'Est de l'Ukraine.

Quelque chose a-t-il changé dans les faits et gestes de la Russie au cours des trois dernières années de guerre? Rien du tout. Permettez-moi de vous confirmer que ce conflit fait encore des morts tous les jours. La journée d'hier a été un autre jour sombre pour l'Ukraine. Nous avons perdu quatre soldats ukrainiens, tués au combat. Quatre autres soldats ont été blessés. Pensez-y un peu: quatre femmes se sont réveillées veuves, des enfants ont perdu leur père, des mères ont perdu leur fils. L'Ukraine aspire à la paix, comme toutes les personnes ici présentes, j'en suis certain, mais aujourd'hui, nous sommes toujours contraints de chercher des solutions à l'agression russe.

Le but de l'agression russe est de détruire la démocratie, les libertés libérales et les droits de la personne en Ukraine. Parfois les Russes frappent avec leurs tanks; parfois ils le font à coup de fausses nouvelles, de tactiques de guerre hybrides comprenant notamment des cyberattaques, comme hier, où ils ont attaqué l'aéroport ukrainien d'Odessa et le métro de Kiev. C'est un exemple éloquent des cyberoutils qu'ils utilisent.

La Russie viole constamment et de manière flagrante son propre engagement, comme Moscou continue de faire la sourde oreille devant nos demandes insistantes et celle de la communauté internationale afin qu'elle respecte à nouveau le sol international, mais la Russie continue de prétendre que cela n'a rien à voir avec la situation. Moscou continue de faire fi de ses engagements en vertu de l'Accord de Minsk. Ses forces militaires sont toujours présentes sur le territoire de l'Ukraine, en Crimée comme au Donbass.

Permettez-moi de vous exposer un peu plus en détail la situation dans l'Est de l'Ukraine. Les zones touchées par le conflit au Donbass souffrent de pertes énormes. Plus de 10 000 personnes ont été tuées à ce jour, plus de 20 000 personnes ont été blessées et 1,5 million de personnes ont été déplacées. Des ponts, des routes, des maisons et d'autres éléments d'infrastructure ont été détruits. D'immenses terrains sont désormais criblés de mines antipersonnelles et antichars, ainsi que de pièges explosifs. Beaucoup d'usines ont été cambriolées, et l'équipement unique qu'elles possédaient a été transporté illégalement vers la Russie. Du matériel militaire, des armes, des munitions, du carburant et des rations sont toujours acheminés à des entités illégales créées par la Russie. La sécurité demeure très précaire.

Les forces séparatistes russes combinées continuent d'ignorer systématiquement l'Accord de Minsk en utilisant abondamment des armes prohibées. La vaste majorité des provocations armées ont lieu dans le noir, lorsque l'OSCE et la Croix-Rouge ont terminé leurs missions quotidiennes. Les observateurs de secours n'arrivent pas à jouir de l'accès illimité voulu aux zones non contrôlées par le gouvernement ukrainien, si bien qu'ils ne peuvent pas vraiment observer si l'Accord de Minsk est respecté, notamment à proximité du village de Telmanove, il y a deux jours, pas moins de deux jours.

En revanche, l'Ukraine a prouvé à maintes reprises qu'elle est prête à régler pacifiquement une situation créée artificiellement par la Russie. En 2017, l'Ukraine a initié à trois reprises de longs cessez-le-feu: à Pâques, pendant les récoltes et pendant la rentrée scolaire. Les troupes d'occupation russes et leurs mandataires les ont violés presque immédiatement chaque fois. Depuis le début de 2017, on compte plus de 13 000 violations du régime de cessez-le-feu. Il y a quelques semaines, le Parlement ukrainien a adopté une loi afin d'établir les conditions préalables à un règlement pacifique dans certaines parties des régions de Donetsk et de Lougansk. Il compte sur la Russie pour enfin commencer à respecter ses engagements en matière de sécurité découlant de l'Accord de Minsk. Nous nous attendons aussi à ce que ces mesures permettent le déploiement d'une mission de maintien de la paix de l'ONU au Donbass.

C'est notre président qui a proposé cette mission de maintien de la paix au printemps 2015 au Conseil de sécurité de l'ONU. Les délégations ukrainiennes à l'ONU demandent sans relâche l'envoi d'une mission d'évaluation du Conseil de sécurité de l'ONU en Ukraine pour examiner la situation sur le terrain. Malheureusement, toutes ces propositions se butent à une farouche opposition de la délégation russe à New York, qui prétend que ce genre de mission ira à l'encontre de l'Accord de Minsk.

● (1605)

L'Ukraine est prête à s'atteler à un travail constructif sous l'égide d'une mission pleine et entière de maintien de la paix de l'ONU. Cependant, le projet proposé par la Russie ne peut pas servir de fondement à la discussion sur l'évaluation préalable au Conseil de sécurité.

Les principaux éléments de la position ukrainienne sont les suivants.

Toute mission future de l'ONU devra être déployée sur toute l'étendue du territoire temporairement occupé, y compris dans la partie incontrôlée de la frontière nationale entre l'Ukraine et la Russie. Le déploiement d'une mission de l'ONU devrait mener immédiatement à un cessez-le-feu permanent, de même qu'au retrait complet de toutes les troupes, formations et militaires étrangers armés, ainsi que de leurs armes et de leur équipement, du territoire de l'Ukraine.

Toute mission de l'ONU doit respecter les principes directeurs de la mise en oeuvre d'opérations de maintien de la paix de l'ONU, qui excluent la participation de représentants du pays agresseur et d'autres parties au conflit. Par conséquent, l'Ukraine rejette l'idée d'une coordination des paramètres futurs d'une mission de l'ONU avec les séparatistes pro-russes. Une future mission de l'ONU ne devrait en aucun cas nuire au travail de l'OSCE ni aux autres organisations internationales présentes au Donbass en les empêchant d'accomplir leur mandat ou en restreignant leur liberté de mouvement.

Mesdames et messieurs, permettez-moi encore une fois de répondre à ma propre question. Y a-t-il quelque chose qui a changé au cours des trois dernières années, depuis l'éclatement de la guerre en Ukraine? Oui, quelque chose a changé. La coalition internationale à l'appui de l'Ukraine et la primauté du droit international se sont renforcées. Je suis très heureux de souligner que le Canada est l'un de nos principaux partenaires et amis à l'appui de la souveraineté et de l'intégrité territoriale de l'Ukraine.

Cette année, nous avons célébré le 25e anniversaire de l'établissement des liens diplomatiques entre le Canada et l'Ukraine. L'Ukraine est résolument déterminée à approfondir encore davantage cette relation bilatérale. Le Canada et l'Ukraine continuent de collaborer à la formation et à la défense militaires.

En avril dernier, le Canada et l'Ukraine ont signé un accord de coopération de défense, qui témoigne de l'engagement inébranlable du Canada envers l'Ukraine et le peuple ukrainien. Depuis le début de l'opération UNIFER, les Forces armées canadiennes ont offert plus de 160 formations à 5 800 soldats ukrainiens. Cette année, pour la sixième fois, un contingent d'environ 30 membres des Forces armées canadiennes déployés dans le cadre de l'opération UNIFER ont marché dans le cadre de la parade du jour de l'indépendance de l'Ukraine.

Nous sommes reconnaissants au gouvernement canadien de prolonger le mandat de l'opération UNIFER jusqu'en mars 2019. Nous attendons impatiemment une décision positive du gouvernement canadien concernant l'ajout de l'Ukraine à la liste des pays désignés pour ce qui est des armes automatiques. C'est une initiative cruciale. J'insiste: c'est une initiative cruciale pour l'Ukraine. L'Ukraine a besoin d'avoir accès à des armes létales défensives à l'aube de sa quatrième année de combat dans une guerre très réelle et brutale.

L'Ukraine apprécie énormément l'appui politique et l'assistance pratique essentielle du gouvernement et de la population du Canada aux forces armées de l'Ukraine. Je suis très reconnaissant envers les membres de cette assemblée de protéger l'Ukraine contre l'agression russe depuis le tout début. Le peuple ukrainien se rappellera toujours cette main tendue par nos amis pendant ce moment extrêmement difficile de notre histoire.

Je vous remercie de votre attention, de votre appui et de votre confiance.

Gloire à l'Ukraine! Gloire au Canada!

● (1610)

Le président: Nous vous offrons nos plus sincères condoléances pour la mort de vos soldats, hier, dans la bataille contre la Russie.

Col Viktor Siromakha: Merci beaucoup.

Le président: Monsieur Hoback.

M. Randy Hoback (Prince Albert, PCC): Merci, monsieur le président.

Je remercie les trois témoins parmi nous aujourd'hui pour cette excellente discussion.

La cybersécurité, les fausses nouvelles, la cyberguerre hybride: tous ces phénomènes semblent présents en Ukraine, qui semble être un front de choix. On dirait que toutes ces nouvelles armes sont créées ou testées là-bas, voire même carrément utilisées. Nous l'avons vu hier soir, comme vous l'avez dit.

Comment les cyberattaques redéfinissent-elles la guerre? En quoi changent-elles la stratégie que devra adopter le Canada pour se préparer à sa propre protection? De même, comment pouvons-nous aider le peuple ukrainien, un peu comme les Américains et les Britanniques leur offrent de l'aide cybertechnologique, une cyberassistance?

Monsieur Bell, je commencerai par vous, après quoi je m'adresserai à M. Wright.

M. Alan W. Bell: La guerre se livre à peu près de la même façon depuis des années. C'est une nouvelle ramification de la guerre tangible, qui diffère de ce que nous avons l'habitude de prévoir et de ce que nos dirigeants ont l'habitude de gérer depuis longtemps. Ces incursions dans différents pays, il y en a au Canada, mais cela ne signifie pas que nous serons envahis. Cependant, en Ukraine et en Crimée, il y a eu des attaques préconçues qui ont mené à l'annexion de la Crimée, puis à l'occupation d'une partie de l'Ukraine.

Nous ne savions pas, ou nous ne comprenions pas à l'époque que c'était le résultat de cyberattaques. Bien sûr, les autres pays de cette partie du monde vont commencer à s'inquiéter s'ils sont la cible de cyberattaques répétées contre les infrastructures essentielles. Ils craindront que la Russie ne s'apprête à envahir leur territoire.

C'est ce qui les inquiète. Cela devrait nous inquiéter aussi, parce que nous devons lutter contre ce genre d'attaque nous aussi, comme la plupart des autres pays occidentaux. Tant que nous ne maîtriserons pas vraiment la cyberguerre — et je pense que mon collègue voudra vous parler de l'informatique quantique dans quelques instants, qui pourrait être une pierre d'achoppement importante, mais je ne peux pas vous en parler moi-même —, je pense que nous nous demanderons ce que cette surabondance de cyberactivité signifie. Signifie-t-elle que les attaquants ne nous aiment pas ou est-ce un signe précurseur d'une autre attaque?

M. Randy Hoback: Dans ce cas-ci, c'était un signe précurseur d'une attaque sur le terrain.

En Amérique du Nord, ce peut être le signe précurseur d'une élection ou d'autres activités qui viendraient perturber les médias, perturber les déplacements des Canadiens.

Monsieur Wright, quels liens voyez-vous entre toutes ces choses? Que pourrions-nous faire en Ukraine pour nous aider à nous préparer à ce qui pourrait se passer au Canada? Prenons l'exemple des attaques survenues hier. Si nous étions là, quelles leçons pourrions-nous retenir pour le Canada? Parce que nous ne sommes pas là-bas, donc nous n'apprenons pas de ces expériences.

M. Stuart Wright: Dès le départ, le renseignement est menacé. Nous saurions ce que faisait l'auteur de la menace sur le terrain, comment les attaques ont été orchestrées, quels outils et mécanismes ont été utilisés pour les mener, quelle infrastructure essentielle était visée et la raison pour laquelle elle a été ciblée. J'entends parler de victimes. C'est comme s'il s'agissait d'efforts concertés, menés à un moment stratégiquement choisi de sorte qu'il pourrait y avoir eu intensification des conflits en même temps.

Pour revenir à la question de savoir ce que nous pouvons faire à l'échelle nationale et à l'étranger, il faut d'abord améliorer les cybercapacités, tant en Ukraine qu'en Amérique du Nord. Puisqu'on s'attend à ce que des vulnérabilités soient exploitées dans les systèmes de contrôle industriels comme les systèmes SCADA, ce qui a perturbé les systèmes d'automatisation du transport, c'est sur quoi nous voulons axer nos efforts dans l'industrie, au gouvernement et dans les forces armées.

Des questions ont été soulevées par le groupe. Je dirais que les exercices, comme l'exercice Locked Shields, organisé par l'OTAN, constituent également un excellent moyen de réduire les répercussions. Il ne s'agit pas ici des vulnérabilités latentes repérées dans ces systèmes industriels, de sorte que nous devons commencer le travail de formation, de mobilisation et de ressourcement pour contrer les risques actuels. Par exemple, dans le cadre des exercices, des membres de l'OTAN ont défendu le réseau électrique en Estonie contre une cyberattaque.

Bien qu'elles soient essentielles, de telles mesures de défense doivent aller de pair avec la prise de mesures proactives, comme la mise à jour et le renforcement de la sécurité du système industriel. Autrement, ce ne sont que des moyens de contourner le problème pour des mesures de défense active. Ils continueront d'utiliser de nouveaux outils, de nouveaux maliciels. On doit commencer à renforcer ces systèmes. Il faut que des gens aident l'Ukraine sur le terrain, prennent les connaissances acquises et les utilisent en Amérique du Nord.

● (1615)

M. Randy Hoback: Une question s'impose alors. Au Canada, nous avons une conception conventionnelle des forces armées: armes et soldats. Nous faut-il redéfinir les forces armées et la guerre?

M. Stuart Wright: Dans le cadre de cette stratégie, nous devons redéfinir la guerre hybride. Nous savons que nous pouvons mener des opérations cinétiques. Nous avons les outils et les processus. Des experts en la matière pourraient m'en apprendre sur la façon de procéder à cet égard. Il faut comprendre que comme prélude à ces activités, la cyberguerre est le premier mécanisme permettant de perturber les communications, les mesures liées à l'énergie, ce qui cause le chaos dans les systèmes et a une incidence sur la capacité de répondre par des moyens cinétiques. Si l'on s'engage dans cette voie, il faut commencer à accroître les ressources, à donner de la formation et à fournir des outils, des processus et des mesures supplémentaires pour appuyer les troupes dans ces activités, ici comme ailleurs dans le monde.

M. Randy Hoback: D'accord. Dans ce cas, monsieur Bell, on n'a pas nécessairement besoin de gens qui peuvent faire 100 pompes. On a besoin de gens comme Sheldon Cooper dans l'émission *The Big Bang Theory*. Comment attirer ce genre de personnes?

M. Alan W. Bell: Nous devons redéfinir l'espace de combat, et voilà pourquoi je parle d'avancées militaires.

J'aimerais dire, par ailleurs, que nous avons la responsabilité d'effectuer un vaste audit de l'un des systèmes d'approvisionnement en eau de la province. Tous nos systèmes SCADA n'étaient protégés d'aucune façon. J'ai demandé aux gens responsables de ce système d'approvisionnement en eau ce qu'il se passerait s'il subissait une cyberattaque. Ils m'ont dit que les gens de la province n'auraient plus d'eau pendant une période d'au moins un à deux mois.

Imaginez les conséquences si cela devait se produire durant l'été et que nous ne pouvions plus acheminer de l'eau vers une province. Je ne parle pas ici d'une ville, mais bien d'une province. La province aurait été complètement vulnérable. On n'a pas encore trouvé de façon de le protéger.

M. Randy Hoback: Autrement dit, nous serions vulnérables, non seulement pour ce qui est des réseaux électriques...

M. Alan W. Bell: Nous sommes vulnérables présentement, aujourd'hui.

M. Randy Hoback: ..., mais aussi pour ce qui est des systèmes d'approvisionnement en eau et toutes sortes d'autres secteurs auxquels nous ne pensons probablement pas.

M. Alan W. Bell: Oui. Je ne parlerai même pas de nos centrales nucléaires.

M. Randy Hoback: En Saskatchewan, le maliciel qui a été utilisé hier pourrait, en fait, être utilisé pour attaquer le réseau électrique de la province, par exemple, n'est-ce pas?

Comment pouvons-nous nous défendre contre cela?

Le président: Il vous reste environ 20 secondes, et vous pouvez donc répondre.

M. Alan W. Bell: Voulez-vous répondre à la question?

M. Stuart Wright: Oui.

Nous devons élaborer un cadre, mettre en commun les connaissances, définir une démarche commune et commencer la formation dès maintenant, car la menace est de plus en plus grande. Elle évolue de jour en jour et de nouveaux outils apparaissent. Si nous n'élaborons pas de cadre commun pour protéger toutes les infrastructures essentielles, alors nous serons essentiellement dans le noir.

M. Randy Hoback: Merci, messieurs.

Le président: Bienvenue, madame Hardcastle. La parole est à vous.

Mme Cheryl Hardcastle (Windsor—Tecumseh, NPD): Merci, monsieur le président. Je suis ravie d'être ici.

Messieurs, tout ce que vous avez dit m'intrigue beaucoup.

Monsieur Wright, je reviens à vous. D'après ce que vous avez dit, le Canada et les prochaines étapes... Êtes-vous d'avis que, pour que nous puissions renforcer nos systèmes, qu'il s'agisse de l'approvisionnement en eau ou du réseau électrique d'une province ou d'une municipalité, concernant le cadre dont vous parliez, l'élaboration d'une stratégie, il incombe à un organisme national, peut-être au ministère de la Défense, d'approuver ou d'examiner ces nouveaux réseaux d'infrastructure?

D'après ce que j'entends et ce que je comprends de mes lectures sur le sujet, nous n'en sommes plus à l'utilisation de la métaphore du pare-feu. C'est presque comme s'il nous fallait utiliser une métaphore qui ressemble à la façon dont nous construisons des immeubles dans des zones à haut risque sismique. Nous devons avoir des structures autonomes.

Comment établir une stratégie maîtresse? Je voulais seulement en savoir plus. Je pense que vous n'avez pas pu en dire davantage. Par conséquent, durant le temps qu'il me reste, je vais vous laisser répondre.

M. Stuart Wright: Il y a un certain nombre de mesures que nous pouvons prendre. Le cadre... Encore une fois, je dois être très prudent. Je parle en tant qu'individu.

Il appartient au Parlement d'envisager la création d'un modèle fédéré quant à l'adoption d'un cadre non seulement pour le ministère de la Défense, mais pour tous les fournisseurs d'infrastructures essentielles du pays, qu'il s'agisse des secteurs de l'automatisation du transport, de la gestion des eaux usées ou des services financiers. Il existe des précédents: en Australie, en Italie et dans d'autres pays. Je sais que le Royaume-Uni et l'Allemagne ont examiné la question.

Je conseille de prendre les éléments centraux que nous avons vus, comme le NIST et le programme C2M2 du département de l'Énergie, et les spécifications militaires, et d'intégrer deux éléments supplémentaires. Le premier, c'est la sécurité dès la conception; pour chaque élément et mécanisme mis en place, on intègre cela dans la conception dans le cadre de la construction de notre infrastructure et de l'adoption des mesures. Le deuxième, et on tient compte du fait que nous vivons dans une société démocratique, c'est le respect de la vie privée dès l'étape de la conception. Je pense à Ann Cavoukian ici. Nous devrions épouser ces principes très rapidement. Il ne s'agirait pas seulement du secteur de l'énergie, mais de tous nos secteurs.

Il nous faut examiner la question de façon globale. Nous devons travailler avec nos partenaires, d'ici, de l'Amérique du Nord et d'ailleurs, pour agir collectivement en tant que secteur. Ensemble, nous sommes plus forts. Si nous agissons chacun de notre côté, nous sommes faibles. Nous devons agir dans un cadre fédéré et regarder au-delà de nos frontières. Il nous faut collaborer avec nos partenaires de l'étranger, l'OTAN et nos homologues en Ukraine pour essentiellement mettre au point un mécanisme de sorte que nous tenions le même langage, agissions dans le même laps de temps et ayons les mêmes types de ressources et de formation. Ainsi, si nous devons déployer des ressources dans un théâtre d'opérations, nous aurons les ressources voulues pour ce faire, tant du côté de l'industrie que de la défense.

Je ne parlerai pas de l'informatique quantique maintenant, car je ne veux pas terroriser qui que ce soit.

● (1620)

Mme Cheryl Hardcastle: Il me reste un peu de temps

Vous avez donné un exemple un peu plus tôt. Vous avez été coupé, en quelque sorte. Voulez-vous revenir un peu sur certains des exemples qui vous ont incité à nous dire qu'il nous fallait adopter un plan fédéral qui dépasse nos frontières?

M. Stuart Wright: Il s'agissait de l'attaque dans les pays baltes. À peu près au même moment, il y a eu l'attaque contre l'Ukraine en 2015. Dans l'un des trois États baltes — qui sont l'Estonie, la Lettonie et la Lithuanie —, le réseau électrique a été la cible d'une attaque, mais n'a pas été perturbé. On n'a pas annoncé publiquement quel pays avait été ciblé. Dans l'attaque contre les États baltes, la méthodologie est similaire à celle qui a été utilisée contre l'Ukraine.

Ce que nous constatons, c'est qu'ils utilisent la même stratégie pour déstabiliser différents pays, mais nous devons intervenir non seulement individuellement, mais collectivement: utiliser un modèle fédéré, un cadre fédéré fondé sur les pratiques de l'industrie. Je sais que quant à la standardisation, Google, Apple, le département de la Défense et le département de la Sécurité intérieure s'appuient sur le NIST comme cadre solide. Nous avons eu beaucoup de discussions à cet égard. D'autre part, je peux vous parler de ce que nous faisons ici, en Ontario.

En général, cette attaque a échoué, mais elle a révélé une chose: la présence d'acteurs dans le réseau électrique des pays baltes. Ils sont peut-être déjà dans les systèmes de réseau électrique, et ils ont peut-être déjà déployé le maliciel. Ce que nous devons faire, c'est prendre les mesures qui s'imposent pour confirmer que ces systèmes n'ont pas déjà été compromis.

Pour que nous puissions le faire, nous devons avoir les ressources et la formation voulues et commencer à renforcer les systèmes. Si nous voulons reproduire cela — que ce soit en Estonie, en Ukraine, ou ici Canada —, nous devons adopter un langage commun. Ce cadre serait l'élément fondamental requis. Ce que je recommande au Comité, c'est de commencer à examiner la question et à adopter une mesure en ce sens.

Mme Cheryl Hardcastle: Merci.

Le président: Monsieur Robillard.

M. Yves Robillard (Marc-Aurèle-Fortin, Lib.): Merci, monsieur le président.

[*Français*]

Bonjour, messieurs.

Merci de vos témoignages aujourd'hui.

Monsieur Bell, je vais citer votre biographie.

[*Traduction*]

M. Bell a formé des équipes de protection rapprochée pour deux rois et deux présidents, et il a participé à des opérations de lutte contre le terrorisme et à de la formation sur le contre-terrorisme partout dans le monde.

M. Alan W. Bell: Oui. C'est vrai.

[*Français*]

M. Yves Robillard: En vous basant sur votre expertise, que pouvez-vous nous dire sur les risques liés à la sécurité auxquels font face les dirigeants actuels du gouvernement ukrainien?

● (1625)

[*Traduction*]

M. Alan W. Bell: Le principal risque, c'est que la Russie aille plus loin. Autrement dit, ce que craignent l'Ukraine ainsi que les autres pays qui faisaient partie de l'Union soviétique, c'est que la Russie reprenne d'autres régions dans ces pays afin d'accroître son espace de bataille opérationnel si l'OTAN décide d'intervenir.

Il est très peu probable que l'OTAN passe à l'attaque, évidemment, compte tenu de l'état actuel des choses, mais les membres de l'OTAN ont convenu — je ne me souviens pas à combien d'années cela remonte — qu'ils n'accroîtraient pas la taille de l'OTAN en y intégrant d'autres pays européens, mais en fait, l'organisation compte maintenant 29 pays membres.

Évidemment, comme je l'ai dit dans ma déclaration préliminaire, la Russie devient progressivement très paranoïaque. Elle est non seulement préoccupée par l'Europe, mais également par la Turquie. C'est un autre enjeu, car la Turquie a indiqué que bien qu'elle soit membre de l'OTAN, elle veut essayer de devenir la leader du monde musulman, et ces deux idées ne sont pas compatibles.

De plus, la flotte en mer Noire... Si l'OTAN décide d'empêcher la flotte de passer par le Bosphore et des Dardanelles, cette flotte ne peut plus opérer en eau chaude. Le seul port qu'elle a maintenant, c'est celui de Tartous, en Syrie. Voilà pourquoi elle intervient en Syrie.

[*Français*]

M. Yves Robillard: Y a-t-il une privatisation des forces de sécurité qui prennent part au conflit ukrainien? Observez-vous une tendance quelconque à cet égard?

Plus largement, à quel point le secteur privé est-il investi dans le conflit ukrainien et ses zones les plus dangereuses?

[*Traduction*]

M. Alan W. Bell: De nombreuses sociétés militaires privées y prennent part, surtout des sociétés américaines. Elles aident les Ukrainiens sur le plan de différentes formations et la façon de mener des opérations, surtout dans les zones urbaines où bon nombre de ces conflits ont lieu.

Pour ce qui est du nombre de compagnies et de leurs forces, nous n'avons pas cette information en ce moment, mais elles commencent à bouger. Voilà pourquoi des sociétés militaires privées ont été créées pour aller aider ces pays lorsqu'ils n'avaient pas beaucoup d'aide de l'étranger.

[*Français*]

M. Yves Robillard: De ce que vous savez et pouvez observer, quel est le statut de la frontière entre l'Ukraine et la Russie? Est-elle poreuse? Si oui, comment l'est-elle? Quelle est l'ampleur des risques liés à la sécurité dans cette zone?

[*Traduction*]

M. Alan W. Bell: L'Ukraine fait face à une armée très rapide, mobile, équipée et très bien formée. La Russie ne s'est pas rendue plus loin que dans le Donbass, à ce moment-ci, mais qui sait ce qui se produira?

Les cyberattaques s'intensifient de plus en plus, et il y a une ou deux raisons. Soit la Russie essaie de s'assurer de réussir son coup la première fois, soit elle veut voir ce qui se passera, quelle sera la réaction. La réaction de l'Occident, et surtout de l'OTAN, est négligeable à ce jour, ce qui l'a encouragée à aller plus loin. Par conséquent, jusqu'à ce qu'une force de maintien de la paix soit mise en place, l'Ukraine continuera de craindre une invasion complète ou une autre annexion, comme celle de la Crimée.

[*Français*]

M. Yves Robillard: Quelle est votre opinion sur les tactiques des groupes séparatistes prorusses adoptées contre les forces armées ukrainiennes dans la région du Donbass? En quoi le soutien offert par la Russie aux groupes séparatistes du Donbass a-t-il changé depuis l'éclatement du conflit? Quel type d'aide la Russie leur a-t-elle fourni?

[*Traduction*]

M. Alan W. Bell: La Russie les aide sur tous les plans. Une bonne partie des pro-russes font partie, en fait, des forces spéciales russes. Dans les médias, on les appelle les hommes verts. Ils sont partout. Il y a une énorme capacité de forces spéciales en Russie, qui traverse maintenant la frontière à divers moments pour aider et former les séparatistes qui sont en Ukraine et, en fait, mener des opérations en leur nom. C'est une situation très difficile pour le gouvernement ukrainien et particulièrement pour les forces ukrainiennes, pour la simple et bonne raison qu'ils ne savent pas qui sont ces gens puisqu'ils parlent tous la même langue. Si un soldat ne porte pas son uniforme de membres des forces spéciales, il peut s'agir de n'importe qui.

Le président: Nous passons maintenant à des interventions de cinq minutes.

C'est Mme Young qui posera les premières questions.

Mme Kate Young (London-Ouest, Lib.): Merci beaucoup.

Messieurs, je vous remercie beaucoup de votre présence.

Je veux revenir un moment sur le fait que la Russie repousse les limites et observe nos capacités d'intervention. J'essaie de comprendre ce que l'Occident doit faire ou ce que nous devons faire pour qu'elle recule. Que faut-il faire exactement? La collaboration, c'est bien beau, mais que devons-nous faire pour montrer à la Russie qu'elle ne peut pas continuer à mener de telles cyberattaques?

● (1630)

M. Alan W. Bell: Nous devons être engagés. Le pays attaqué est l'Ukraine. Il faut montrer un engagement de l'extérieur, montrer que nous sommes prêts à protéger l'Ukraine et que nous voulons passer à une autre étape avec elle. Si nous ne le faisons pas, la Russie commencera à s'intéresser aux pays Baltes, ce qui accentuera le problème. La Russie tente de gagner du temps, mais il y a un pays sur son chemin. Elle doit prendre pied dans ce pays ou l'annexer.

C'est ce qui inquiète tous les autres pays. Tous les gens de l'ouest de l'Ukraine pensent la même chose. Tous ces pays ont eu leurs propres réunions en plus de réunions collectives et ils disent tous la même chose: « Nous sommes inquiets; nous ne savons pas quoi faire. » Ils ne sauront pas à quoi s'attendre jusqu'à ce que l'OTAN, l'Occident ou les États-Unis prennent des décisions.

Le problème aussi, c'est que le leader du monde libre, le président Trump, s'intéresse à d'autres parties du monde et ne s'intéresse pas particulièrement à l'Europe en ce moment. On s'inquiète de cela. S'il y avait un autre président à la Maison-Blanche, on ne serait peut-être pas aussi inquiet, mais à l'heure actuelle, on se demande ce qui se passera au cours des prochaines semaines et des prochains mois.

Mme Kate Young: Allez-y, monsieur Wright.

M. Stuart Wright: Je suis d'accord avec Alan. Il est mieux placé que moi pour parler du volet géopolitique.

Ce qui m'inquiète, c'est l'aliénation des Russes. Je sais qu'une partie des points de friction dans les pays Baltes et en Ukraine a trait à la transition du réseau BRELL vers le réseau européen. On crée des périmètres entre ces deux régions. Il y a une grande incertitude quant à la source de ces attaques, à leurs auteurs.

Soyons clairs: nous sommes en présence d'un acteur hostile qui mène une guerre ouverte par des moyens directs et indirects. Le défi sur le plan cybernétique a trait à la façon de prouver que c'est bel et bien la Russie qui attaque et qui détruit le réseau. La Russie a des forces militaires qui travaillent de façon parallèle. Ce serait une drôle de coïncidence si ce n'était pas le cas.

À mon avis, il faut établir des mécanismes qui nous permettront de le vérifier. Il faut toutefois avoir les ressources et la volonté pour le faire. Les États-Unis se centrent sur d'autres régions, sur les pratiques commerciales et autres. Encore une fois, si la situation perdure et que l'OTAN souhaite adopter une approche plus mesurée, elle devra — en plus d'avoir les niveaux de force appropriés — tenir compte du fait que la cybernétique fait partie de cette guerre hybride et avoir des ressources formées pour aider au déploiement, à l'intervention et au rétablissement des systèmes industriels, entre autres.

Mme Kate Young: Colonel, vouliez-vous ajouter quelque chose?

Col Viktor Siromakha: Oui. J'aimerais ajouter qu'au début de 2014, lorsque la Russie a annexé la Crimée illégalement, ce n'était que la première étape des développements relatifs à la situation militaire. La Russie voulait un corridor de transport terrestre vers la Crimée par l'entremise du territoire ukrainien. C'est pourquoi en juillet-août 2014, la Russie a fait tout ce qu'elle pouvait pour gagner le contrôle de Mariupol, au sud. Les frictions étaient grandes entre les forces prorusses et la force régulière de l'Ukraine, le ministre de l'Intérieur et les services spéciaux de sécurité. Nous avons réussi à protéger Mariupol contre ses attaques. Néanmoins, la Russie utilise même des LRM pour détruire certains objets de Mariupol.

Autant que je me souvienne, certains des pires scénarios envisagés par les experts britanniques étaient la prise de contrôle du sud-est de l'Ukraine — y compris Odessa et un corridor direct vers la Transnistrie — ou la prise de contrôle de la rive gauche de l'Ukraine par la Russie. Vous savez probablement que le territoire de l'Ukraine est divisé en deux par notre principal fleuve, le Dniepr. Le pire des pires scénarios envisagés était la prise de contrôle de 70 % du territoire ukrainien par la Russie, ce qui ne laisserait que quelques régions ukrainiennes dans l'Ouest, comme Lviv, Ternopil et Rivne. Selon ce que je comprends, la Russie n'a pas réussi à prendre le contrôle, alors elle utilise les chars d'assaut et les hybrides pour atteindre son objectif.

● (1635)

Mme Kate Young: Merci beaucoup.

Le président: Monsieur Yurdiga, vous avez la parole.

M. David Yurdiga (Fort McMurray—Cold Lake, PCC): Merci, monsieur le président.

Ma première question s'adresse à M. Wright.

Nous nous préoccupons de la cybersécurité. Nos systèmes ont tous été la cible de maliciels. Je suppose que tous les systèmes de l'Ukraine ont été compromis dans une certaine mesure. De façon réaliste, combien de temps faudrait-il pour mettre à niveau les systèmes et veiller à ce qu'ils ne soient pas compromis? Il est difficile de répondre à cette question parce que nous ne savons pas ce qu'il y a à faire. J'aimerais connaître votre opinion à ce sujet.

M. Stuart Wright: C'est une question d'une très grande portée; une question importante. Nous avons de la difficulté à y répondre en raison des problèmes de notre infrastructure critique et aussi parce qu'il faut une gestion efficace des biens. Il faut d'abord savoir quels sont les biens à mettre à jour. Ensuite, il faut savoir s'ils sont vulnérables. Enfin, il faut savoir s'il y a des correctifs et dans l'affirmative, comment on les mettra à jour.

Pour nos ordinateurs personnels et les ordinateurs portatifs de nos bureaux, les correctifs sont là. Il y a un mécanisme et un écosystème en place qui appuient tout cela. On doit parfois mettre les systèmes SCADA hors ligne pour les renforcer; il n'y a donc pas de mesure réelle à prendre à cet égard. Comment pourrons-nous faire si l'on ne peut pas dresser l'inventaire de nos biens afin de trouver le fabricant qui a les correctifs nécessaires pour régler le problème? Il serait très difficile à l'heure actuelle d'évaluer le temps qu'il faudrait pour renforcer ou mettre à jour les systèmes afin d'en éliminer les vulnérabilités.

Ce qui devrait nous préoccuper, ce sont les vulnérabilités inconnues. Il faut savoir ce que l'on fera si les systèmes cessent de fonctionner. Quelles mesures prendra-t-on à ce moment-là? Quelles sont les mesures d'intervention et de rétablissement? Ensuite, lorsque les systèmes seront rétablis, il faudra les renforcer. Il faut user d'une autre tactique. Il faut prendre des mesures préventives et prévoir des mesures d'intervention. Nous en sommes déjà à l'étape de l'intervention. Comment peut-on aborder la question alors que nous sommes en situation de conflit?

Comment peut-on rétablir le réseau électrique et demander aux ingénieurs de sécuriser le système alors que les obus tombent et qu'il y a des victimes? C'est une évaluation très difficile à faire.

M. David Yurdiga: Est-il juste de dire qu'on élabore un plan à cet égard? Bien sûr, la tâche est importante. On parle d'années et non de mois...

M. Stuart Wright: Je suis d'accord, oui.

M. David Yurdiga: ... donc nous sommes toujours en situation de risque. Toutes les nations le sont, en fait. L'Ukraine est la zone d'essai. Croyez-vous que la Russie lancera des cyberattaques contre ses voisins?

M. Stuart Wright: Voilà ce qui pose problème. Encore une fois, c'est une question de responsabilité. Nous savons que pour certains intérêts... Alan a parlé de la Turquie et nous avons aussi parlé de l'Ukraine et de l'Europe de l'Est. Nous savons qu'il est fort probable que la Russie soit un joueur actif dans ces théâtres d'opérations. Ce qui nous préoccupe, ce sont les attaques de tiers.

Nous avons vu des attaques dans d'autres pays, comme l'Inde. Je crois qu'on a récemment ciblé les auteurs des attaques en Thaïlande; les attaques contre Sony sont un autre exemple. Nous avons aussi entendu parler d'attaques en Afrique. Est-ce que ces États-nations sont en guerre et utilisent des mécanismes cybernétiques pour attaquer les autres États-nations ou est-ce qu'ils sont utilisés à titre de tierces parties? Comment peut-on analyser la situation? Comment peut-on retrouver l'auteur de la menace? Voilà le défi. Il n'y a rien de clair.

Si vous m'aviez demandé si nous avons été attaqués par les Russes, je vous aurais répondu que nous avons certains indices qui viennent de l'Europe de l'Est ou de l'Estonie à cet égard. Il peut s'agir d'une cybergang ou d'une tierce partie. Il peut s'agir d'autres auteurs de menaces provenant d'autres régions. Ce peut être la Chine ou des gens en Amérique latine. Nous n'avons pas de mécanisme cohérent pour déterminer l'origine de ces menaces ou pour pouvoir les retrouver. Il faut qu'on puisse le faire. Il faut obtenir des renseignements utilisables.

M. David Yurdiga: Je crois que l'enjeu pour tous, c'est le coût. Est-ce qu'on investit suffisamment d'argent? Bien sûr, c'est une préoccupation pour tous les intervenants. Croyez-vous que les gouvernements investissent suffisamment pour sécuriser nos systèmes?

M. Stuart Wright: Je dois faire très attention ici. À quel gouvernement faites-vous référence?

M. David Yurdiga: Bien sûr, étant donné toutes les parties au conflit... Le Canada, par exemple...

M. Stuart Wright: Le gouvernement fédéral...?

M. David Yurdiga: Oui et aussi tous les autres intervenants. Bien sûr, nous nous préoccupons de l'Ukraine. Est-ce qu'on donne suffisamment d'argent à l'Ukraine pour qu'elle stabilise ses systèmes?

● (1640)

M. Stuart Wright: Le président m'indique qu'il ne me reste que 30 secondes. Je serai très bref.

Pour qu'il y ait plus de mesures, il faut des ressources supplémentaires, ce qui signifie un investissement supplémentaire. Il faut augmenter le nombre des ressources et embaucher des spécialistes du domaine ou les former. Il faut en faire plus et investir davantage dans ces efforts.

Le président: Monsieur Fisher, vous avez la parole.

M. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Merci, monsieur le président.

Merci, messieurs, de votre présence ici aujourd'hui, de votre expertise et de votre témoignage.

Comme nous arrivons à la fin de notre étude et que vous êtes le dernier groupe de témoins que nous recevons, de nombreuses questions ont déjà été posées, mais je m'intéresse beaucoup à la cybernétique, comme tous mes collègues.

Monsieur Wright, vous parlez de ce nouveau type de guerre. Vous avez parlé du maliciel Bad Rabbit, de KillDisk et de BlackEnergy. On jurerait qu'il s'agit de boissons énergétiques.

M. Stuart Wright: Il y a un marketing derrière cela. L'auditoire est captif. C'est assez ingénieux, en fait.

M. Darren Fisher: Est-ce que certaines de ces cyberattaques remontent directement à la Russie?

On émet une hypothèse, ce que je comprends. Je crois que nous savons exactement ce qui se passe, mais la Russie n'admet même pas qu'elle a déployé des soldats dans ce qu'elle appelle une zone de guerre civile. Est-ce qu'on a pu retracer certaines attaques, trouver leurs auteurs et les accuser plutôt que d'émettre des hypothèses?

M. Stuart Wright: Je vais faire attention, puisque la réunion ne se tient pas à huis clos. Il me faut certaines cotes de sécurité pour discuter ouvertement de cette question.

Je dirai ceci: si vous regardez le rapport d'analyse conjoint du département de la sécurité intérieure des États-Unis et du FBI du 27 décembre, qui présente certains renseignements précis sur la participation de la Russie au processus électoral de nos voisins du Sud dont on a parlé plus tôt, vous trouverez des preuves directes de la capacité, de la sophistication et de l'omniprésence de la cybermenace russe.

En ce qui a trait à une solution hybride dans les autres administrations, nous pourrions réévaluer la question, mais nous avons une indication claire de la responsabilité de la Russie dans au moins deux ou trois cas, notamment Sandworm et les pannes qui ont frappé l'Ukraine en 2014 et 2016.

Une fois de plus, nous sommes préoccupés. Je crois que l'Estonie n'a pas voulu établir la responsabilité à cet égard. On ne transmet pas l'information, ce qui est dommage. Il est difficile de tirer des conclusions.

M. Darren Fisher: Étant donné les événements récents, la fermeture des stations de métro et des aéroports, nous... On émet des hypothèses, mais...

M. Stuart Wright: C'est arrivé mardi. Nous en avons entendu parler, je suppose... On a publié les avis mardi soir, alors que j'étais dans l'avion.

Je le répète, il faut être sur le terrain pour mener des enquêtes, mais selon les premiers indices, lorsqu'il y a un conflit d'une telle ampleur et qu'on élimine la capacité de transporter les troupes, qu'on démolit les réseaux d'électricité, qu'on perturbe les lignes aériennes... Je dirais qu'il s'agit d'une drôle de coïncidence.

M. Darren Fisher: Merci.

Colonel, nous vous remercions de votre présence ici aujourd'hui.

Dans votre déclaration préliminaire, vous avez parlé de l'héritage de Poutine. Rebâtir l'ancienne Union soviétique est... Je ne sais pas si vous avez parlé d'une pièce de résistance, mais c'est son héritage, ce qu'il veut laisser derrière lui. De nombreuses personnes suggèrent que les attaques de la Russie émanent de l'intérêt de l'Ukraine à l'égard de l'OTAN ou, inversement, de l'intérêt de l'OTAN pour l'Ukraine. On comprend que la Russie veut s'approprier cette zone tampon entre elle et la région européenne.

À votre avis, est-ce qu'il s'agit des deux? C'est peut-être le cas. Je ne veux pas parler à votre place. J'ai toujours cru que c'était son héritage, mais de nombreux témoins ont dit que c'était autre chose. Vous pourriez peut-être nous dire ce que vous pensez...

Col Viktor Siromakha: Oui, bien sûr. Je peux vous donner mon avis.

Selon moi, la Russie est comme une belle-mère. Lorsqu'elle voit que l'Ukraine se rallie à l'Union européenne, à l'OTAN, la Russie se fâche. M. Poutine se fâche aussi.

À mon avis, le meilleur exemple de cela, c'est lorsque l'Ukraine a tenu un championnat de soccer en 2012, à Kharkiv, à Donetsk, à Kiev, à Dnipropetrovsk, et à Lviv, et a connu un énorme succès. Nous avons organisé une compétition incroyable en collaboration avec la Pologne. Dans le stade, tout était jaune et bleu; on ne voyait pas les couleurs de la Russie. C'est le stade central de Donetsk. C'est le meilleur exemple de notre réussite. Nous nous sommes déplacés vers Donetsk. Des trains à grande vitesse font la navette entre Kiev et Donetsk en quatre heures.

La Russie a vu ce qui se passait et a décidé d'agir. Elle a entrepris cette guerre politique contre l'Ukraine et a compromis notre transition vers l'Union européenne.

● (1645)

M. Darren Fisher: Je vais céder le reste de mon temps de parole à M. Gerretsen.

Le président: S'il vous restait du temps, je suis certain qu'il vous en serait reconnaissant. Malheureusement, votre temps est écoulé.

Monsieur Bezan, vous avez la parole.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Monsieur le président, je vais céder mon temps de parole à Mme Gallant.

Le président: Madame Gallant.

Mme Cheryl Gallant (Renfrew—Nipissing—Pembroke, PCC): Merci, monsieur le président.

Pendant des années, ils ont refusé de reconnaître qu'ils devraient accorder de l'attention à la cybernétique, et même aujourd'hui, ils ne veulent pas coordonner les efforts des pays membres. Ils affirment: « La politique a son propre système, et d'autres parties de l'Europe aussi. Ce sont des gens différents. » Les raisons sont nombreuses pour ne pas coordonner les efforts. Ils fournissent de l'aide par l'intermédiaire du centre de coordination des réactions.

À votre avis, l'OTAN devrait-elle avoir un groupe ou un centre qui fournirait de l'information en cas d'attaque, ou le fait-elle déjà d'une façon quelconque?

M. Alan W. Bell: À mon avis, une des grandes difficultés... Dans une section intitulée « La réaction du Canada à la guerre hybride », j'ai parlé de l'ensemble du pays. J'ai demandé pourquoi nous ne procédions pas de la sorte. J'ai employé le terme « pangouvernemental ». Je pense que tout le monde qui a pris la parole ce soir a demandé: « À qui revient la responsabilité, au MDN? Au gouvernement? À quelqu'un d'autre? D'où viennent les fonds? »

Si nous adoptions une approche pangouvernementale, nous obtiendrions peut-être des résultats, parce qu'à l'heure actuelle, chacun travaille en vase clos, ce qui ne fonctionnera pas dans le cas des questions cybernétiques. Cette méthode est efficace dans nombre d'autres situations. Nous savons que notre façon de lutter contre le terrorisme et de cloisonner les organisations qui sont censées communiquer entre elles fonctionne parfois; d'autres fois, elle échoue parce qu'il n'y a pas de communication.

Il en est de même pour l'OTAN. Tous les pays d'Europe ont le droit de se joindre à l'OTAN si leur gouvernement décide de le faire. C'est la même chose pour l'Union européenne. Aujourd'hui, les anciens pays baltes affirment qu'ils auront plus de succès s'ils font partie de l'Union européenne, sur les plans financier, économique et autres. En outre, en devenant membre de l'OTAN, les pays se joignent à un groupe qui, je le répète, compte aujourd'hui 29 membres. S'il arrive quelque chose, si la Russie tente quoi que ce soit, 29 pays réagiront. Malheureusement, nous n'avons pas réagi. Je ne dis pas que nous devrions envahir la Russie en raison de ce qui est arrivé en Ukraine et en Crimée, mais nous n'avons pas été assez forts pour lui dire de reculer. Il y a 29 pays, et la plupart sont limitrophes de la Russie.

Ainsi, il ne se fait pas taper sur les doigts. Il continuera, une action à la fois, jusqu'à ce que l'OTAN déclare: « Assez! » Quand dirons-nous que c'est assez? Quand l'OTAN dira-t-elle que c'est assez? Sera-ce l'année prochaine, dans un an, dans deux ans?

La Russie avance. Elle s'améliore dans le domaine de la cybernétique et dans tout le reste. Elle a une armée permanente énorme qui est formée pour se battre en Europe et nulle part ailleurs. Qu'arrivera-t-il si nous ne faisons rien pour l'arrêter?

Mme Cheryl Gallant: En réalité, la cyberguerre neutralise l'article 5 en raison de l'absence d'attribution. On affirme qu'il n'y aura pas de coordination des efforts parce que les pays individuels n'ont même pas adopté leur propre cyberdoctrine. Durant l'examen de la défense, on nous a dit que nous avions une approche pangouvernementale, mais lorsque nous avons posé une question concernant la création d'un cybercommandement canadien comme celui des États-Unis, on nous a répondu: « Ce n'est pas nécessaire. Toutes les personnes dont nous avons besoin sont à Ottawa. Il suffit de les appeler ou de les faire venir en taxi. »

M. Alan W. Bell: En 2016, l'OTAN a déclaré que la perpétration d'une cyberattaque contre un État membre entraînera l'activation de l'article 5. La Crimée et l'Ukraine ne sont pas visées par cette déclaration. S'il avait attaqué un pays membre de l'OTAN, aurions-nous activé l'article 5? Nous l'ignorons parce qu'il ne l'a pas fait, et il ne l'a pas fait parce qu'il n'est pas idiot. Voilà où nous en sommes.

Si, dans un an, il attaque un pays membre de l'OTAN, qu'arrivera-t-il? Je ne crois même pas que nous soyons allés si loin dans nos plans. J'ignore ce que fait l'OTAN, évidemment, parce que je ne suis qu'un individu ordinaire, mais il n'a pas attaqué un pays membre de l'OTAN et l'article 5 n'a donc pas été activé.

● (1650)

Mme Cheryl Gallant: S'il y avait une cyberattaque, par exemple...

En fait, il y a eu une réunion des parlementaires de l'OTAN en mai, lorsque l'aéroport Heathrow a été frappé par une panne des services de TI. Nous nous demandons toujours si c'est réellement ce qui est arrivé ou si, pour une raison quelconque, on ne voulait pas semer la panique en avouant qu'il s'agissait d'une cyberattaque.

M. Alan W. Bell: Prenez l'exemple des 12 derniers mois de l'administration Trump. Les Américains cherchent encore la réponse, et ils ont les ressources et les fonds nécessaires pour trouver les coupables. Ils sont maintenant d'avis que c'est la Russie qui a compromis les élections et ils en ont la preuve. Nous n'avons pas de preuve dans le cas de l'Ukraine simplement parce que nous n'avons pas eu assez de temps, car trop peu d'experts des questions cybernétiques sont en train d'examiner tous les événements.

Une des choses que le Canada ne fournit pas à l'Ukraine, ce sont des experts des questions cybernétiques. Nous ne faisons rien sur ce plan, mais nous le devrions, car nous devons découvrir ce que les gens ont appris afin que nous en tirions nos propres conclusions. Puisque nous ne sommes pas là, nous dépendons de ce que les autres nous disent.

Mme Cheryl Gallant: Vous avez répondu à la question...

Le président: Je suis désolé, votre temps est écoulé.

Je donne la parole à M. Mark Gerretsen.

M. Mark Gerretsen (Kingston et les Îles, Lib.): Merci, monsieur le président.

Monsieur Bell, vous avez parlé tout à l'heure de la présence de la Russie dans le Donbass, la région qu'elle occupe actuellement. Vous avez dit que nous ignorions si la Russie passerait à la prochaine étape. Quelle est la prochaine étape?

M. Alan W. Bell: La prochaine étape, c'est aller de l'avant et lancer une cyberattaque pour une raison quelconque, et puis continuer à avancer ou encore attaquer un autre pays qui ne fait pas partie de l'OTAN.

M. Mark Gerretsen: Selon un témoin qui a participé à notre dernière séance, un ancien diplomate ayant travaillé en Russie et en Ukraine, la Russie aurait envahi la région qu'elle occupe actuellement parce qu'elle aurait pratiquement — je paraphrase — été invitée par les Ukrainiens de la région, qui appuyaient la Russie et qui voulaient sa protection.

Approuvez-vous cette affirmation?

M. Alan W. Bell: Non, parce que je ne le sais pas. Toutefois, pourquoi est-ce que les membres des forces spéciales russes ont enlevé leurs uniformes et pourquoi est-ce que ce sont des citoyens de la Crimée qui ont hissé le drapeau de la Russie en Crimée?

M. Mark Gerretsen: En effet.

M. Alan W. Bell: Les a-t-on forcés? A-t-on préparé le coup? Nous ignorons qui étaient ces gens.

M. Mark Gerretsen: Vous rejetez donc cette notion.

M. Alan W. Bell: Non, je ne la rejette pas. Je ne sais tout simplement pas.

M. Mark Gerretsen: Vous ne savez pas. D'accord.

Vous avez dit que la réaction des alliés ou de l'OTAN était négligeable. Sur quoi fondez-vous cette affirmation?

M. Alan W. Bell: Ils n'ont rien fait. Ils ont juste pris des mesures diplomatiques et d'autres...

M. Mark Gerretsen: Et la réaction... Vous parlez de participer activement au conflit.

M. Alan W. Bell: Non, certainement pas.

M. Mark Gerretsen: Dans ce cas, nous avons 200 soldats sur le terrain qui aident à former les soldats ukrainiens. N'est-ce pas là une réaction?

M. Alan W. Bell: Oui, c'est une réaction, mais étant donné que leur adversaire est la Russie, qui a une équipe très mécanisée et hautement qualifiée, la présence de 200 personnes qui enseignent des tactiques militaires de base, des soins médicaux, des techniques d'identification des EEI et tout le reste ne changera pas grand-chose.

M. Mark Gerretsen: Que considérez-vous comme une réaction non négligeable?

M. Alan W. Bell: Peut-être qu'on le fait, je ne sais pas. Je ne suis pas dans le secret de ce que les gouvernements font aux autres gouvernements. De quoi les gouvernements du Canada et des États-Unis parlent-ils avec la Russie? Quels moyens utilisent-ils?

Il n'y a rien de visible; les Ukrainiens ne voient aucune action. Certains pays envoient des équipes de formation: les États-Unis, le Royaume-Uni et le Canada. Nous contribuons tous un peu à cela.

M. Mark Gerretsen: Le témoin que j'ai déjà mentionné a aussi déclaré — je paraphrase encore une fois — que nous devrions laisser l'Ukraine régler ses problèmes elle-même. Après tout, ce sont des soldats ukrainiens qui se trouvent au front. Appuyez-vous cette affirmation?

M. Alan W. Bell: Non. Plus d'un million et demi d'Ukrainiens habitent ici, ce qui représente un million et demi de votes.

● (1655)

M. Mark Gerretsen: D'accord. La question a peut-être déjà été posée, mais l'entreprise dont vous êtes le président, Globe Risk International inc., effectue-t-elle des travaux dans la région du Donbass en ce moment?

M. Alan W. Bell: Non.

M. Mark Gerretsen: À votre connaissance, y a-t-il des entreprises ou des intérêts canadiens dans la région?

M. Alan W. Bell: Non.

M. Mark Gerretsen: Non, d'accord.

Pour revenir à l'aide militaire, avez-vous des recommandations précises concernant ce que le Canada devrait faire de plus sur le plan militaire?

M. Alan W. Bell: Nous devons fournir aux soldats un entraînement exhaustif pour les préparer à la guerre, et non seulement de l'instruction de base.

M. Mark Gerretsen: Qu'entendez-vous par « entraînement exhaustif »?

M. Alan W. Bell: Nous devons leur transmettre l'ensemble de nos compétences. J'ai déjà évoqué le sujet lorsque je parlais de ce qui est nécessaire; cela comprend les forces spéciales, les aspects diplomatiques, juridiques, économiques et tout le reste. C'est la dernière chose. Nous devons tout faire. Soit nous ne faisons rien, soit nous agissons de manière à changer les choses. En travaillant dans d'autres pays — certainement pas en Europe —, j'ai appris qu'à moins que vous arriviez et que vous commenciez à prendre des mesures que le pays reconnaît, les gens vont penser que vous ne faites pratiquement rien. Ce n'est que symbolique. Vous aidez en déployant des efforts symboliques.

M. Mark Gerretsen: Est-ce que j'ai...

Le président: Vous tombez juste à point, à la seconde près. Merci de me faciliter la tâche.

La dernière intervenante officielle est Mme Hardcastle. Vous avez trois minutes.

Mme Cheryl Hardcastle: Merci. Comme je suis la dernière à intervenir avant la conclusion, je vais poursuivre sur le même sujet.

Le besoin d'élargir notre conception d'un soldat et du combat a beaucoup été soulevé. Vous parlez de diplomatie, de discussions entre personnes réelles. Je me demande à quoi ressembleraient ces relations interpersonnelles parce que vous avez dit plus tôt que nous devions affermir nos relations bilatérales. Parlez-vous de mesures tangibles et traditionnelles?

Par exemple, nous avons mentionné la possibilité de lever la restriction relative aux visas temporaires pour les Ukrainiens qui visitent le Canada. Parlez-vous de mesures de ce genre ou d'actions plus subtiles qui comprennent des choses que je ne vois pas?

M. Alan W. Bell: Jusqu'à maintenant, la contribution militaire canadienne a été de former 5 000 personnes, ce qui est suffisant, mais que leur avons-nous appris? L'instruction que nous leur fournissons sera-t-elle utile si la Russie décide d'envahir une autre région du territoire ukrainien?

Nous devons nous pencher sur... Je parle d'exhaustivité. Il n'y a pas seulement l'aspect militaire, il y a aussi la participation du gouvernement et de toutes les parties. Il se passe beaucoup de choses dont nous ne sommes pas au courant, et c'est ainsi. Le gouvernement ukrainien doit avoir une liste de ce qu'il aimerait que nous lui fournissions, et si nous ne lui donnons pas ce dont il croit avoir besoin, il se tournera vers quelqu'un d'autre, comme les États-Unis. Notre gouvernement doit décider ce qu'il veut faire.

Nous avons offert un soutien symbolique. Des Canadiens sont sur le terrain en ce moment, ils travaillent fort et tout cela, mais il y a beaucoup d'autres éléments à considérer: la politique, l'économie et tout le reste. Si nous voulons protéger le pays contre l'annexion par une force hostile, nous devons faire un peu plus qu'envoyer 200 soldats à 18 milles de la frontière de la Pologne pour offrir de l'instruction de base. C'est tout ce que nous faisons, en réalité: nous nous contentons de leur offrir de l'instruction de base.

La raison pour laquelle je crois que nous devons agir de la sorte, c'est que j'ai participé à des efforts en Afrique et au Moyen-Orient, et je sais quelles seront les conséquences si nous employons seulement des demi-mesures. J'ai aussi été envoyé en Afghanistan, dans la province de Kandahar, pour effectuer du travail au nom du gouvernement canadien. Je suis arrivé rempli de promesses, mais une fois le projet à moitié terminé, il est devenu non viable sur le plan politique, et on m'a donc empêché d'accomplir le reste de ce que nous devions faire.

Ce projet avait une valeur de 65 millions de dollars; c'était un des plus grands projets du Canada en Afghanistan avant que nous nous retirions, et pendant que nous étions là, il fonctionnait. Tout fonctionnait et nous atteignions nos objectifs, mais en cours de route, divers intervenants se sont ingérés dans ce que nous devrions faire et ce que nous ne devrions pas faire. Nous avions un plan, mais ce plan changeait selon la personne responsable; la bureaucratie nous compliquait donc la tâche. C'est là un autre problème que nous devons régler, sinon nous ne faisons que tourner en rond.

● (1700)

Mme Cheryl Hardcastle: Me reste-t-il du temps?

Le président: Vous aurez l'occasion d'intervenir à nouveau, mais pour l'instant, votre temps de parole est écoulé.

Mme Cheryl Hardcastle: D'accord.

Le président: Il nous reste du temps, et comme vous pouvez le deviner, je vais répartir le temps équitablement entre tous. Les libéraux, les conservateurs et les néo-démocrates auront droit à cinq minutes chacun.

Avant de poursuivre, j'aimerais souligner, très brièvement, que les nombreux témoignages que j'ai entendus ici et même durant notre visite en Ukraine rendaient compte d'une grande reconnaissance envers le soutien offert par le Canada. D'après moi, ce soutien est certainement plus que symbolique. Pouvons-nous en faire davantage? Nous allons discuter de ce que nous pouvons faire de plus et, bien sûr, nous allons présenter des recommandations au gouvernement du Canada, mais à mon avis, nos actions sont très appréciées et elles changent les choses. C'est ma perception des témoignages que nous avons recueillis auprès des Ukrainiens depuis le début de notre étude.

Cela étant dit, je donne la parole à M. Gerretsen.

M. Mark Gerretsen: Merci beaucoup. Je reviens à M. Bell. Vous avez abordé précédemment la question de la formation aux échelons inférieurs, si je puis m'exprimer ainsi. Est-ce que vous recommandez que l'on offre également de la formation et de l'aide aux échelons supérieurs de la hiérarchie militaire?

M. Alan W. Bell: Si nous ne formons pas nos propres officiers quant à la façon de composer avec la guerre hybride, on peut en conclure que c'est sans doute la même chose pour les Ukrainiens. Peut-être devrions-nous commencer par leur haut commandement pour ensuite redescendre vers le bas de la hiérarchie...

M. Mark Gerretsen: Je vous prie de m'excuser, mais j'ai vraiment peu de temps. À ce sujet, bon nombre des problèmes découlent du fait que la structure militaire ukrainienne est un héritage de l'ex-Union soviétique.

M. Alan W. Bell: Oui.

M. Mark Gerretsen: L'un des grands défis sera selon moi de trouver la façon d'apporter les réformes nécessaires. Le commandant de la base que nous avons visitée là-bas était en poste depuis 13 ans. Personne n'a été commandant de la base située dans ma circonscription pendant plus de deux ans. Au bout d'un certain temps, on commence à vouloir se bâtir un empire; c'est simplement la nature humaine.

Comment peut-on s'attaquer à un problème semblable?

M. Alan W. Bell: Il faut que le temps fasse son oeuvre.

Lorsqu'un pays a fait partie du bloc soviétique pendant autant d'années, il en a intégré la doctrine, les procédures militaires et tout le reste. Si ce pays décide tout à coup...

M. Mark Gerretsen: L'Ukraine ne fait plus partie de l'Union soviétique depuis...

M. Alan W. Bell: Depuis 15 ans.

M. Mark Gerretsen: Tout à fait. Regardez ce qui se passe dans les autres pays qui ont obtenu leur indépendance en même temps que l'Ukraine. Pourquoi les Ukrainiens n'ont-ils pas pu en faire autant... Je ne veux pas que l'on traite des raisons pour lesquelles les enjeux ne sont pas nécessairement les mêmes, mais pouvez-vous me dire combien de temps il va leur falloir?

M. Alan W. Bell: Si ces anciens pays du bloc soviétique doivent s'intégrer à l'OTAN et à l'Occident de façon permanente, il faudra complètement revoir leur entraînement et leur équipement de telle sorte qu'ils puissent agir comme membres à part entière de l'OTAN, et non comme des États indépendants ou comme des membres indépendants du regroupement des pays baltes. Cela va prendre un certain temps et tous les pays concernés devront apporter l'aide nécessaire.

Je reviens à la situation de l'Ukraine. Les Ukrainiens s'adressent au gouvernement du Canada pour demander ceci et cela en expliquant pourquoi. Nous pouvons répondre oui pour certaines choses et non pour d'autres. Mais c'est le gouvernement ukrainien qui demande de l'aide et nous devrions acquiescer à cette requête dans sa totalité ou alors pas du tout.

M. Mark Gerretsen: Merci.

Monsieur Spengemann.

M. Sven Spengemann: Merci beaucoup pour le temps que vous m'accordez.

Monsieur Bell, je vous ramène à la discussion de tout à l'heure concernant une possible mission de maintien de la paix des Nations unies. Avez-vous pu observer des éléments qui indiqueraient que Poutine est à la recherche d'une porte de sortie politique ou qu'il est intéressé à entamer un dialogue?

M. Alan W. Bell: Je ne suis pas un spécialiste de la politique. Je parle seulement d'expérience. Je ne veux pas aborder les choses sous un angle politique parce que je dis simplement... Je sais très bien ce que vous pensez et je vois vos regards qui disent: « Oh, mon Dieu! »

Je peux seulement vous dire ce que je pense de la situation. Je ne prétends aucunement avoir raison. Je suis sans doute l'un des très rares Canadiens à avoir combattu les Russes. Je l'ai fait pendant neuf mois au côté des moudjahidines à la fin des années 1980. Je sais comment ils sont. Je sais à quoi il faut s'attendre lorsqu'on les affronte et je connais leurs façons de procéder.

Ils ne pouvaient pas avoir recours à la cybermenace à l'époque, mais ils gardaient les femmes et les enfants afghans dans la crainte de représailles, car tous les hommes avaient joint les moudjahidines. J'ai pu constater ce que les Russes étaient capables de faire dans ces pays-là sans disposer de moyens cybernétiques. C'est donc effectivement l'impression que j'ai, à la lumière des expériences vécues lorsque j'étais plus jeune.

M. Sven Spengemann: Comment M. Poutine perçoit-il le Canada selon vous? Est-il hors de question que nous puissions assumer un rôle moins partial dans ce conflit?

M. Alan W. Bell: Nous avons un gouvernement. Nous avons un premier ministre. La diplomatie est bien sûr la voie à privilégier. Tout dépend si Poutine, qui a ses propres objectifs, est prêt à écouter notre premier ministre, ou le président américain, ou qui que ce soit d'autre. Pour le moment, il a des visées qui lui sont propres. Il semble s'en ficher et, malheureusement, sa contrepartie à la Maison-Blanche est un certain M. Trump.

● (1705)

M. Sven Spengemann: Colonel Siromakha, pourriez-vous nous dire brièvement ce que vous en pensez? À quel point l'Union européenne forme-t-elle un tout homogène relativement à ce conflit touchant l'Ukraine et aux mesures qui doivent être prises pour y mettre fin?

Col Viktor Siromakha: L'Ukraine attend que les pays de l'Union européenne arrivent à se concerter. La situation en Europe est actuellement plutôt complexe. Nous voyons ce qui se passe en Espagne et en Italie. Il y a eu aussi le cas du Monténégro il y a quelques mois à peine. Ce sont tous des pays membres de l'Union européenne.

M. Sven Spengemann: Avez-vous l'impression que l'Europe parle d'une seule voix dans le dossier de l'Ukraine?

Col Viktor Siromakha: L'Europe a sa propre opinion, et nous voudrions bien qu'elle l'exprime de façon plus sentie.

M. Sven Spengemann: Merci pour cette réponse.

Merci beaucoup, monsieur le président.

Le président: Monsieur Bezan.

M. James Bezan: Merci, monsieur le président.

Je veux remercier nos témoins de leur présence aujourd'hui.

Colonel Siromakha, si l'on considère également tous les soldats qui ont perdu la vie dans ce conflit, je pense que l'Ukraine a droit à toute la gratitude du Canada et de l'OTAN dans son ensemble pour avoir tenu le fort contre l'une des machines militaires les plus puissantes du monde contemporain. Comme l'indiquait M. Bell, l'OTAN a été prise au dépourvu et vos efforts lui ont permis d'avoir le temps de mieux se préparer et de renforcer ses positions avancées.

Le moment est venu pour nous d'en faire davantage pour l'Ukraine, je suis tout à fait d'accord avec vous. Vous avez mentionné différentes choses que le Canada pourrait faire pour votre pays. Le président Poroshenko a aussi parlé des images RADARSAT. Est-ce que ces images figurent également sur votre liste, en ce sens que vous souhaiteriez voir le Canada fournir à nouveau ce genre de renseignement?

Col Viktor Siromakha: Oui. Cela nous procurerait une meilleure vue d'ensemble de la situation. Nous avons vraiment besoin de cette information pour mieux comprendre ce qui se passe sur le territoire temporairement non contrôlé de l'Ukraine et le long de la frontière temporairement non contrôlée entre ce pays et la Russie. Sur cette frontière longue de quelque 400 kilomètres, on retrouve trois passages officiels. Pouvez-vous vous imaginer le nombre de passages non officiels que les Russes peuvent utiliser pour faire entrer des munitions, du carburant, des soldats ou quoi que ce soit d'autre?

Encore là, les images satellites pourraient nous être très utiles pour savoir exactement à quoi nous en tenir.

M. James Bezan: Il y a des militaires canadiens, américains et britanniques qui forment les soldats ukrainiens, mais l'inverse peut également être vrai. Lors de notre séjour en Ukraine, nos militaires cantonnés à la base de Yavoriv nous ont dit qu'ils tiraient aussi des enseignements de l'expérience des militaires ukrainiens qui ont eu à combattre directement les troupes russes. Ne pourrait-on pas tirer davantage profit de ces possibilités d'échanges de telle sorte que les officiers ukrainiens puissent former ceux du Canada et des autres pays membres de l'OTAN à l'égard de la guerre hybride que la Russie mène contre l'Ukraine?

Col Viktor Siromakha: Oui, certainement. C'est une excellente occasion de mettre en commun cette expérience pratique du combat dans un contexte moderne. Nous parlons maintenant de cybermenace et de guerre hybride, mais il y a aussi la réalité bien concrète des soldats qui doivent survivre dans de telles conditions.

Voici d'ailleurs un excellent exemple de l'astuce des soldats ukrainiens lorsqu'il s'agit de trouver de l'eau quand on est coincé dans un aéroport pendant des jours et des semaines. Ils ont ainsi déniché dans les systèmes de chauffage installés pour l'hiver une eau meilleure que celle qu'ils boivent habituellement. Ce fut toute une découverte pour nos partenaires canadiens qui entraînaient nos soldats dans la région de Yavoriv. Ce sont des aptitudes militaires tout à fait élémentaires, mais elles permettent néanmoins de sauver des vies.

M. James Bezan: Merci. J'ai quelques brèves questions pour nos autres témoins.

Monsieur le président, nous devrions inviter à nouveau M. Wright, surtout dans la poursuite de notre étude au sujet de l'OTAN. Il pourrait peut-être comparaître à huis clos avec les mesures de sécurité appropriées de telle sorte que nous puissions discuter plus à fond des actions qui doivent être entreprises. Vous parlez de cyberdéfense, de cyberguerre et de mesures préventives. Votre allusion aux mesures préventives nous indique-t-elle qu'il y a un volet offensif à cette cyberguerre?

M. Stuart Wright: C'est une autre question à laquelle il m'est difficile de vous répondre. Elle est fondée sur l'hypothèse que nous ne disposons pas déjà d'une capacité d'attaque. Je ne peux pas traiter de cet aspect. Je peux toutefois vous dire que le gouvernement actuel et ceux qui l'ont précédé ont pris des mesures appropriées dans ces différents domaines.

● (1710)

M. James Bezan: Merci.

Monsieur Bell, j'ai beaucoup aimé vos observations, notamment quant au fait que l'OTAN a été prise au dépourvu et que nous n'en avons pas fait suffisamment. Je sais que tout cela est en grande partie hypothétique, mais qu'est-ce que l'OTAN devrait faire de plus à l'avenir, non seulement pour aider l'Ukraine, mais aussi pour se préparer en prévision des prochaines manoeuvres de Vladimir Poutine.

Je sais que certains s'entêtent à croire qu'il essaie de réinventer l'Union soviétique. Je crois qu'il est impérialiste; il se voit comme un tsar. Il est capitaliste; il ne veut pas retourner à l'époque du communisme. Je voudrais savoir ce que l'OTAN devrait faire selon vous.

M. Alan W. Bell: Nous devons appuyer l'Ukraine, car il nous faut tenir notre bout dans ce dossier. Je ne parle pas seulement du Canada...

M. James Bezan: L'OTAN dans son ensemble...

M. Alan W. Bell: ... l'OTAN et tous les autres pays. Si nous n'intervenons pas, une autre attaque semblable sera sans doute lancée pour tenter de parvenir aux mêmes fins. Nous devons nous montrer fermes pour que les Russes comprennent bien que nous réagirons s'ils tentent encore le coup. Il n'est pas question de déclencher une guerre. Je ne crois pas que c'est ce qui va arriver, et il est bien certain que je ne le recommande pas. En fin de compte, nous devons montrer que nous allons apporter à l'Ukraine toute l'aide dont elle a besoin. Nous devons donc considérer très sérieusement toutes les requêtes que l'Ukraine nous adresse. Si nous négligeons de le faire, comme je l'indiquais, et si personne d'autre le fait à notre place, l'Ukraine sera pour ainsi dire abandonnée à elle-même.

Si nous permettons que l'Ukraine s'effondre totalement, qu'est-ce que la suite nous réserve? Le problème va seulement s'amplifier. Nous devons tenir notre bout dès maintenant.

Le président: Madame Hardcastle, vous aviez une autre question?

Mme Cheryl Hardcastle: Merci.

Colonel, j'aimerais que vous nous aidiez à mieux comprendre votre vision et vos points de vue. Vous savez que nos dispositions actuelles de financement pour la formation arrivent à échéance. Nous voudrions comprendre à quel point la formation est importante à vos yeux et à quel niveau il conviendrait de la bonifier, conformément aux observations formulées par nos autres témoins aujourd'hui. Lorsque vous aurez répondu, peut-être que M. Wright pourrait en faire autant.

Col Viktor Siromakha: Il va de soi que la formation actuellement offerte par le Canada à l'Ukraine dans le cadre de l'opération Unifier est très importante. En avril 2017, lors des négociations tenues à l'occasion de la visite au Canada de notre ministre de la Défense, Stepan Poltorak, il a été convenu de hausser le niveau visé par la formation, en passant par exemple du niveau tactique offert dans le cadre de l'opération Unifier, à celui d'opération qui se situe au centre de notre hiérarchie.

Je dois bien sûr souligner le rôle important joué par le Canada en Ukraine, parce que Mme Sinclair, conseillère stratégique au sein du Conseil consultatif sur la réforme de la défense, accomplit un travail formidable. Elle est directement responsable de la mise en oeuvre des réformes touchant la direction des forces conjointes de défense. C'est exactement le genre de soutien dont il est question.

J'ai 38 ans et je suis un officier de la nouvelle génération. Il est bien certain que nous avons en Ukraine de formidables officiers, généraux et amiraux qui ont l'expérience des combats. Reste quand même que c'est une génération qui doit céder graduellement sa place, jour après jour, semaine après semaine. Il faut espérer que dans 5 ou 10 ans d'ici, nous verrons émerger une toute nouvelle génération d'Ukrainiens possédant une vaste expertise, y compris l'expérience des combats et une formation linguistique appropriée. Dans un tel scénario, l'approche envisagée serait très intéressante pour nous. Si le Canada a la possibilité de fournir un financement additionnel à l'Ukraine, il nous serait d'une très grande utilité pour la formation et la professionnalisation de nos officiers. Ce serait un véritable investissement dans l'avenir des forces armées ukrainiennes. C'est une condition à remplir afin d'assurer la paix à long terme en Ukraine comme dans l'ensemble de la région de l'Europe de l'Est.

Mme Cheryl Hardcastle: Très bien.

M. Stuart Wright: Je suis d'accord avec Viktor. Pour ce qui est de la formation, la prochaine génération de spécialistes et d'experts en cybersécurité sort actuellement des universités. Il faut leur donner la possibilité d'être formés sur le terrain avec de véritables stratégies. Je vous recommanderais, si je puis me le permettre, de chercher à vous inspirer des succès remportés dans le développement des forces israéliennes de défense. Les soldats israéliens font leur service militaire obligatoire. Ils sont formés par l'unité responsable du renseignement sur les transmissions ainsi que par les spécialistes en cryptographie et en cyberexamen. Ils peuvent travailler au sein de l'industrie une fois leur diplôme obtenu, ce qui leur permet de perfectionner leurs compétences en vue de pouvoir les exploiter à l'échelle planétaire.

Je pense que nous pourrions adopter un modèle semblable au Canada. Il s'agit essentiellement d'harmoniser les efforts déployés auprès des diplômés universitaires en étroite collaboration avec l'industrie, le gouvernement et le ministère de la Défense nationale. Nous ne devons pas seulement leur transmettre ces compétences, mais aussi leur donner l'occasion de les perfectionner. Nous devons nous comparer à ce qui se fait ailleurs dans le monde dans le contexte des menaces qui pèsent sur nous.

Selon le rapport APT1 produit par Mandiant il y a plusieurs années, les Chinois pouvaient compter sur 130 000 spécialistes en cybersécurité. Je dirais qu'il y en a en Amérique du Nord, et peut-être au sein du G7 dans son ensemble, quelque part entre 20 000 et 25 000 dans le secteur privé seulement. Les estimations sont à peu près du même ordre pour ce qui est des spécialistes en cybersécurité de la Russie.

Si vous regardez du côté de WikiLeaks et de ce qui s'est passé avec la CIA en matière de divulgation, avec Langley et son infrastructure, vous constaterez qu'il y a au moins six ou sept divisions différentes dotées de structures d'appui appropriées aux fins de la cybersécurité. Nous devons admettre que nous avons été surpassés et qu'il nous faut commencer à intervenir davantage en amont, au sein des universités, pour former la prochaine génération de spécialistes en cybersécurité.

● (1715)

Mme Cheryl Hardcastle: Merci.

Le président: Nous allons accorder deux minutes à Mme Romanado, après quoi nous terminerons avec quelqu'un de l'autre côté.

Madame Romanado.

Mme Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Merci beaucoup, monsieur le président.

Je tiens à remercier nos invités pour leur comparution et les excellents témoignages dont ils nous ont fait bénéficier.

Vous parliez de cybersécurité, monsieur Wright. Lors d'une visite en Israël, j'ai rencontré les dirigeants de l'entreprise qui s'occupe de la cybersécurité pour Hydro-Québec, dans ma propre province. C'est donc une entreprise étrangère qui assure la cybersécurité du réseau électrique de la province de Québec, ce qui témoigne bien du grand retard que nous avons accumulé en la matière.

On nous a dit aujourd'hui que nous nous contentions en quelque sorte de réagir, plutôt que de prendre l'initiative. Vous nous avez fait part du plan d'action que vous recommandez. Il consisterait notamment à réviser et adapter la doctrine officielle du ministère de la Défense nationale, à établir et fournir les lignes directrices et le cadre nécessaires, et à adopter les mesures appropriées, notamment en ce qui concerne les outils, les techniques et les personnes. Certains ont fait valoir qu'une approche pangouvernementale s'imposait à l'égard de cet enjeu. On nous a également dit que l'OTAN n'avait pas, d'une manière générale, récompensé les comportements répréhensibles, mais n'avait pas non plus remis les Russes à leur place après l'invasion de la Crimée.

Il faudra du temps pour faire tout cela. Nous savons aussi qu'il y a chaque jour des gens qui meurent en Ukraine. Quatre soldats ont été tués pas plus tard qu'hier. Comme nous devrons prendre ces mesures en parallèle, j'aimerais savoir ce que le Canada devrait faire à court, moyen et long terme pour contribuer à la recherche d'une solution.

Nous avons l'opération Unifier, mais nous devons travailler sur le terrain en même temps que nous formons les gens. Pouvez-vous nous en dire plus long sur vos suggestions à court et à moyen terme?

M. Stuart Wright: À court terme, il faut d'abord adopter un modèle fédéré, c'est-à-dire travailler en coopération avec nos partenaires stratégiques au sein des autres administrations, tant en Amérique du Nord qu'à l'échelle planétaire.

Deuxièmement, il faut commencer à mobiliser la prochaine génération de spécialistes de la cybersécurité dans le cadre d'une approche harmonisée avec le milieu de l'enseignement, l'industrie, le gouvernement et les forces militaires. Il faut commencer à former cette prochaine génération.

Troisièmement, il faut fournir du financement et un mécanisme de communication, soit via une tribune d'échange de renseignements ou une instance consultative, de telle sorte que chacun puisse avoir accès en temps utile aux données dont il a besoin. Il faut également trouver un moyen de le faire sans qu'il y ait de répercussions sur l'image de marque de nos entreprises ou de notre gouvernement.

M. Alan W. Bell: Les gouvernements doivent comprendre que l'Ukraine a bel et bien été attaquée. Il faut maintenant qu'ils se demandent comment ils vont réagir. Nous ne saurons pas à quoi nous en tenir tant que la réponse à cette question n'aura pas été trouvée, car c'est une décision qui relève des gouvernements.

Les Ukrainiens ont besoin d'aide actuellement parce qu'il y a des gens mal intentionnés qui cognent à leur porte. Ils nous demandent différentes choses. Nous devrions prêter une oreille attentive à leurs requêtes et faire tout en notre pouvoir pour y acquiescer. Dans le cas contraire, si les Russes décident d'aller de l'avant en se montrant encore plus téméraires, nous pourrions avoir à regretter d'avoir perdu un autre pays faute d'avoir fait le nécessaire. Si nous ne tenons pas notre bout maintenant, nous pourrions nous retrouver dans l'obligation de mener une guerre en Europe, car les Russes ne vont pas manquer de répéter l'exercice tant que nous ne réagirons pas.

● (1720)

Mme Sherry Romanado: Merci.

Col Viktor Siromakha: Il est un peu difficile d'ajouter quoi que ce soit de très concret aux réponses que mes collègues viennent de vous donner. Je vous dirais simplement que l'Ukraine a réussi à survivre à l'essai de collision auquel le pays a été soumis il y a trois ans. Depuis 2014, nous avons fait l'objet de plus de 7 000 cyberattaques, et nous comprenons mieux maintenant de quoi il en retourne. Nos structures de cybersécurité sont bien en place et assurent une défense efficace de nos infrastructures essentielles.

Les attaques d'hier montrent bien que nous sommes maintenant capables de nous défendre. Il serait très intéressant que nos partenaires puissent venir profiter de cette expérience pratique en Ukraine pour voir comment les choses se passent et quelles formes peuvent prendre les diverses attaques. Nous pourrions procéder à une analyse de la menace de manière à améliorer les mesures de protection dans d'autres pays également.

M. Stuart Wright: Sherry, puis-je faire un dernier commentaire? Vous avez posé une question sur les mesures à court, moyen et long terme.

Nous avons vu des développements absolus et je n'entrerai pas dans les détails. Toutefois, le Canada doit entrer dans l'ère de l'informatique quantique. Nous devons appuyer les ressources que nous avons dans les universités et commencer à investir de l'argent et des ressources mesurées pour soutenir ces efforts. C'est une technologie qui change complètement la donne dans le domaine cybernétique.

Mme Sherry Romanado: Merci.

Le président: M. Bezan a la parole pour la dernière question.

M. James Bezan: Merci, monsieur le président.

J'aimerais revenir à la discussion sur une mission de paix potentielle de l'ONU. Des témoins qui ont comparu devant notre comité nous ont dit que le Canada ne devrait pas faire partie d'une telle mission, car il est déjà beaucoup lié à l'Ukraine et à ses efforts, et qu'il n'est donc peut-être pas un intermédiaire impartial.

J'aimerais savoir si vous êtes d'accord avec cette affirmation ou si vous pensez que le Canada, en raison de sa réputation, pourrait tout de même diriger une mission de paix de l'ONU s'il en avait l'occasion.

M. Alan W. Bell: Non, c'est moi qui ai fait ce commentaire. Essentiellement, je voulais dire que la Russie s'opposerait probablement à ce que le Canada dirige une mission de l'ONU, car nous sommes très près des États-Unis.

M. James Bezan: Vous n'êtes cependant pas le seul à nous avoir dit cela. D'autres témoins nous ont dit qu'il n'y avait absolument aucune chance que cela se produise.

M. Alan W. Bell: Je crois que la direction d'une mission de l'ONU représenterait une bonne occasion pour le Canada, car cela démontrerait notre volonté d'agir et de reconnaître la situation.

Je crois donc que le Canada devrait participer à une telle mission. Je pense que c'est une mission intégrale. C'est probablement l'une des missions les plus importantes auxquelles nous pouvons participer en ce moment. De nombreuses autres missions sont en cours — et nous connaissons tous ces missions —, mais elles ne produisent aucun résultat.

M. James Bezan: Colonel, pourriez-vous également nous donner votre avis sur la question?

Col Viktor Siromakha: Oui, bien sûr. Une future mission de paix marquerait un tournant dans l'histoire de l'Europe moderne. Si le Canada et ses partenaires de l'OTAN pouvaient tous jouer un rôle essentiel dans cette future mission, cela permettrait de régler la situation, car dans le pire des scénarios, l'avancée des Russes vers l'ouest compromettra la situation dans l'ensemble de la région.

À l'exception de l'Europe de l'Est, nous observons des confrontations d'intérêts dans de nombreuses régions du monde. Il vaut mieux arrêter les choses maintenant que faire face aux conséquences des intentions de la Russie plus tard.

M. James Bezan: Monsieur Bell, vous avez mentionné à quelques reprises qu'il y avait d'autres exemples que nous pouvions utiliser pour orienter la façon dont nous gérons la guerre en Ukraine. À quoi faites-vous référence? Parlez-vous de ce que les partenaires de la coalition ont fait en Afghanistan ou en Irak ou avez-vous autre chose en tête, par exemple le renforcement de notre capacité et notre participation à un conflit?

M. Alan W. Bell: La guerre en Afghanistan était complètement différente. Les Afghans n'avaient pas les capacités de la Russie, mais ils ont tout de même repoussé les Russes à l'extérieur de leur pays ou ils les ont forcés à s'en aller; il faut croire qu'ils savaient ce qu'ils faisaient.

Ce que je dis, c'est qu'au lieu de leur offrir un entraînement militaire de base, nous devons leur offrir un entraînement complet. Ils doivent obtenir un entraînement qui touche à tout. Comme je l'ai dit, il faut couvrir tous les éléments, non seulement sur le plan militaire, mais également sur le plan gouvernemental, économique, financier, juridique, etc.

Si nous décidons d'adopter une approche pangouvernementale à cet égard, nous devrions nous attendre à ce que l'Ukraine fasse la même chose. De cette façon, nous travaillerons de concert, au lieu de nous concentrer sur ce que nous croyons approprié.

M. James Bezan: Ma dernière question s'adresse aux trois témoins. Lorsque vous comparaissez devant notre comité, il se peut que dans le feu de l'action, vous oubliiez d'ajouter quelque chose. Aimeriez-vous formuler un dernier commentaire avant la fin de la réunion?

● (1725)

M. Alan W. Bell: J'ai été chanceux, car je ne savais pas vraiment quoi dire et je ne connaissais pas l'orientation du Comité. J'ai tenté de me représenter l'ensemble du problème et je me suis dit que la guerre hybride devait faire partie de ces discussions, car c'est la menace principale. J'ai donc consacré la plus grande partie de mon temps à ce sujet.

J'ai également perdu mon temps sur le domaine cybernétique, car je ne suis pas un expert dans ce domaine et je ne savais pas que nous avions un expert sur place. Si un groupe prévoit parler de certains points précis, il faudrait que les gens qui comparaissent ou qui sont invités à comparaître le sachent, afin qu'ils puissent parler des sujets que vous voulez entendre, au lieu d'improviser.

M. James Bezan: Monsieur Wright, avez-vous des recommandations?

M. Stuart Wright: J'aimerais partir en formulant un dernier commentaire. Le Canada ne doit jamais relâcher sa vigilance. La cybersécurité doit être intégrée au fonctionnement quotidien de la société.

M. James Bezan: Colonel.

Col Viktor Siromakha: J'aimerais ajouter que le Canada joue maintenant un rôle essentiel et qu'il s'est pleinement engagé à l'égard de l'Ukraine. J'aimerais que l'année 2018 soit encore plus réussie grâce à la présidence du Canada au G7.

Le président: Le Canada, le gouvernement du Canada et les membres de notre comité tiennent à ce que l'Ukraine prospère. Les membres de notre comité ont maintenant l'occasion et le devoir de formuler des recommandations substantielles au gouvernement sur les points à améliorer et sur les mesures supplémentaires qui peuvent être prises. C'est ce que nous ferons.

Je vous remercie d'avoir pris le temps de comparaître devant le Comité aujourd'hui.

La séance est levée.