

Introduction aux notions de base sur la cybersécurité du gouvernement du Canada : un premier aperçu

ALEXANDRA GREEN ET MATTHEW KELLETT

Alex Green a été la toute première officière responsable de l'Équipe de cybergdéfense de la Flotte dans les Forces maritimes du Pacifique [FMAR (P)], de 2018 à 2020. Elle prépare actuellement un doctorat en études de la guerre au Collège militaire royal du Canada, où elle se spécialise en cyberterrorisme. En 2024, elle a reçu le prix Franklin-Pinch pour ses recherches sur la mise au point d'applications personnalisées à des fins terroristes.

Matthew Kellett, Ph.D. est conseiller spécial au Commandement des cyberopérations des Forces armées canadiennes. Il a déjà été programmeur de logiciels dans le secteur commercial et scientifique de la défense. Il est titulaire d'un doctorat en informatique théorique, plus précisément sur la conception et l'analyse d'algorithmes répartis. Il aime les échecs, la course à pied et le curling, et il a déjà été président du Ottawa Curling Club.

Les Forces armées canadiennes (FAC) et le ministère de la Défense nationale (MDN) s'empresent de répondre à la demande en matière de capacités de cybersécurité. Les FAC ont créé le groupe professionnel des opérateurs de cyberopérations en 2017,¹ et l'École d'électronique et des communications des Forces canadiennes (EEFC) a annoncé la première promotion de diplômés en 2021.² Trois ans plus tard, en septembre 2024, les FAC ont officiellement établi le Commandement des cyberopérations des Forces armées canadiennes (COMCYBERFAC). Ce commandement est la seule autorité reconnue du MDN et des FAC pour les cyberopérations, qui englobent le renseignement électromagnétique et la guerre électronique interarmées. La création du COMCYBERFAC est importante, car elle permet de regrouper en une seule chaîne de commandement unifiée et transparente plusieurs efforts pandomaines, visant à tirer parti des capacités de cyberopérations, créant ainsi un « guichet unique » pour l'expertise en cyberopérations.

Au cours des sept années qui ont mené à la mise sur pied du Commandement des cyberopérations, les FAC ont créé un nouveau groupe professionnel et diplômé leur première cohorte d'opérateurs de cyberopérations. Les FAC investissent dans les capacités de cyberopérations. La dotation représentait autrefois un défi, mais le nombre d'opérateurs qualifiés est en croissance. Malgré cette croissance, un rapport de 2020 du directeur général – Évaluation, intitulé *Évaluation des cyberforces*, a conclu que les « cyberforces comptent un nombre suffisant de postes; toutefois, la dotation de ces postes pose problème », et a fait état de difficultés liées à l'embauche et au maintien en poste de civils, ainsi qu'à l'arrimage des besoins en matière de capacités de cyberopérations avec l'approche conventionnelle du perfectionnement professionnel militaire. Le rapport faisait état plus particulièrement de la frustration liée aux situations de « cyberpersonnel qui compte le plus d'expérience, et qui travaille pour du personnel qui possède peu d'expérience du cyberdomaine ». La création du Commandement devrait grandement contribuer à résoudre ces problèmes.

La situation s'améliore à mesure que le groupe professionnel de cyberopérateur arrive à maturité et que l'Unité d'instruction sur le cyberespace forme des opérateurs. Même si cette capacité se développe rapidement, les connaissances de base en cybersécurité dans le reste du MDN et des FAC n'ont pas suivi le même rythme. Les membres de l'Équipe de la Défense sont souvent affectés à des postes nécessitant des connaissances en cyberopérations sans avoir de solides antécédents en la matière. Bon nombre de ces militaires ne sont pas nés à l'ère du numérique. Cela se comprend, puisque l'âge moyen des militaires des FAC est de 36 ans³ et que le *World Wide Web* est accessible au grand public depuis 30 ans; l'effectif moyen des FAC n'est donc pas né dans un monde où l'Internet était déjà présent. La plupart des personnes en poste à la haute direction des FAC ont plus de 30 ans; il est donc raisonnable de supposer que beaucoup de personnes ne sont pas nées dans un univers entièrement connecté à l'Internet et médiatisé par celui-ci. Elles représentent une génération de militaires des FAC qui doivent composer avec le cyberdomaine dans leurs tâches militaires, mais pour qui l'Internet a d'abord été une

idée nouvelle apparue au début de leur carrière. À mesure que les FAC élargissent et priorisent les cyberopérations et les cybercapacités, de nombreux militaires doivent rapidement s'approprier et comprendre la terminologie du domaine.

Il va de soi qu'un grand nombre de membres de la communauté de défense canadienne connaissent bien les aspects techniques et non techniques de la cybersécurité. Ces personnes peuvent juger le présent article utile comme aide-mémoire. Cet article vise surtout à servir de texte d'initiation pour établir un niveau de connaissances de base chez les militaires et les civils qui viennent tout juste d'être affectés à un poste, où ils doivent se familiariser avec ces concepts.

En plus de présenter certaines notions de base dans un cadre militaire, le présent article traite des fausses idées courantes auxquelles ces nouveaux membres de l'équipe peuvent être confrontés. D'abord, nous présentons certains termes fréquemment utilisés. Même si les employés du gouvernement du Canada peuvent avoir accès aux notes de doctrine interarmées, à la Banque de terminologie de la Défense et à Termium, nous croyons que le fait de regrouper les notions dans un même article, avec des exemples, aidera les nouveaux membres à s'adapter plus rapidement. Nous présentons des termes tels que *cyberespace*, *cyberenvironnement*, *nuage*, *cyberdomaine* et l'emploi de « *cyber* » comme adjectif. Nous expliquons ensuite que le cyberespace est souvent considéré comme un bloc monolithique et nous exposons les nuances entre les différents types de technologies qui se rattachent au cyberespace. Compte tenu de ces nuances, nous établissons une distinction entre le cyberespace et l'environnement de l'information. Les deux sont souvent confondus, car les équipes de cyberopérations doivent souvent soutenir des effets d'information. Nous expliquons également la populaire analogie du château et la façon dont elle peut servir à comprendre la différence entre les cyberopérations et les opérations de réseau. L'article se termine par deux autres distinctions importantes : la première entre cybersécurité et cyberdéfense, et la seconde entre cyberévénement, cyberincident et cyberattaque. Après avoir lu le présent article, les lecteurs devraient posséder une base solide pour approfondir les concepts et participer à des discussions plus poussées.

Définitions et termes courants

D'abord, nous expliquons des termes courants avant d'aborder les différences nuancées entre les concepts. Tout membre de la communauté de la défense sait que les FAC et le MDN peuvent être perçus comme un véritable alphabet de sigles et de termes déroutants. Il est donc pertinent de traiter d'emblée certains termes normalisés que les lecteurs pourraient trouver dans leur travail. Pour les FAC et le MDN, l'*environnement des cyberopérations*, le *cyberenvironnement* ou, en abrégé, le *cyberespace*, est un environnement physique, tout comme la mer, la terre, l'air et l'espace. Une infrastructure matérielle sous-tend le monde virtuel et en est

indissociable. Chaque équipement avec lequel un utilisateur interagit est relié à un autre équipement matériel situé ailleurs, soit par des fils et des câbles de fibre optique, soit par des photons qui circulent dans l'air et l'espace. Le nuage n'est pas réellement un nuage; il s'agit généralement d'un immense entrepôt rempli d'équipements de réseautage et de serveurs informatiques qui exécutent des logiciels chargés de veiller à ce que les données continuent d'exister même après la défaillance inévitable du matériel sur lequel elles sont stockées. Ainsi, plutôt que d'être entreposées sur votre appareil physique, ces données sont sauvegardées sur un serveur ou un groupe de serveurs et sont accessibles par l'Internet ou par un autre grand réseau. C'est de là que vient notre premier mot à la mode, soit le terme *nuage*. Les ingénieurs de réseaux, informaticiens et autres spécialistes qui tracent des diagrammes de réseaux utilisent traditionnellement un symbole en forme de nuage comme substitut pour représenter l'infrastructure sous-jacente complexe qui échappe au contrôle de l'organisation. Lorsque des compagnies comme Amazon et Google ont commencé à offrir des ressources informatiques à distance, le *nuage* a été présenté comme un nouveau type de prestation de services, les entreprises interagissant avec ces services sans exercer de contrôle direct sur l'infrastructure.

Ensuite, le *cyberdomaine* correspond au cyberespace, ainsi qu'à tout ce qui l'entoure et le soutient, notamment les personnes, les processus et les infrastructures. Le gouvernement du Canada utilise ce terme pour désigner « toute l'infrastructure, toutes les entités, tous les utilisateurs et toutes les activités liées au cyberespace ou qui ont une incidence sur celui-ci ».⁴ Le cyberdomaine peut englober la vérification de l'identité d'un nouvel employé avant qu'on lui attribue des preuves d'identité pour accéder au réseau ministériel, la sécurité des locaux abritant les serveurs et l'équipement de réseautage, et même les personnes qui administrent le réseau; autant d'éléments essentiels au maintien du cyberespace, mais qui ne relèvent pas à proprement parler du cyberespace. Le Canada, l'OTAN et de nombreux alliés ont reconnu le cyberdomaine comme un domaine de guerre, au même titre que les domaines maritime, terrestre, aérien et spatial. Cette reconnaissance signifie que les FAC doivent être prêtes à mener des cyberopérations dans le cyberenvironnement (c'est-à-dire le cyberespace) et être capables de défendre leur part du cyberdomaine.⁵

Le terme *cyber* n'est donc qu'un adjectif, indiquant que l'élément qu'il qualifie est lié au cyberdomaine ou au cyberespace. Pensez, par exemple, à son emploi dans la cybersécurité, les cyberopérations et les cyberincidents. Le mot *cyber* est d'ailleurs utilisé à outrance. Dans un contexte militaire, les lecteurs entendront peut-être le terme *cyberplanification* beaucoup trop souvent. La *cyberplanification* n'est rien d'autre qu'une planification militaire appliquée au cyberdomaine; elle n'a rien de particulièrement *cyber* et devrait simplement être appelée par son nom, soit la planification. Par ailleurs, le terme *cyber* ne devrait pas être utilisé comme un nom ni comme un verbe, même si c'est souvent le cas

dans la langue courante. Ainsi, on ne devrait jamais écrire : « Ils devraient utiliser le cyber pour cela » ou « Nous devrions cyber ceci ». Dans la prochaine section, nous décomposerons le vaste concept de *cyberespace*, puis nous en établirons la distinction par rapport à l'environnement de l'information.

Décomposer le cyberespace : notions de TO, TP et IdO

Même s'il est courant de regrouper tous les éléments sous le terme de *technologie de l'information (TI)*, les FAC et le MDN doivent être plus précis au sujet des composantes du cyberespace s'ils veulent les gérer correctement. Au sein des FAC et du MDN, nous disons TI pour désigner l'infrastructure classique de bureautique et de réseautage, pour faire la distinction avec la technologie opérationnelle, qui sert à faire fonctionner les systèmes physiques, comme les pompes et les appareils de chauffage, et de la technologie de plateforme, qui correspond à la technologie opérationnelle, installée sur des plateformes militaires, comme les navires, les systèmes de commande des moteurs et les systèmes de guidage des missiles. Nous pouvons diviser le cyberespace en sous-catégories : technologie de l'information (TI), technologie opérationnelle (TO) et technologie de plateforme (TP). Il vaut également la peine de préciser où se situent les appareils de l'Internet des objets (IdO) dans ces différentes catégories. Si vous êtes nouveau dans le domaine, vous entendrez probablement ces termes employés pour désigner des biens du gouvernement. Nous avons simplifié les définitions ci-dessous pour rendre ces concepts plus accessibles.

Technologie opérationnelle (TO)

La technologie opérationnelle concerne l'ensemble des systèmes industriels cyberphysiques. Elle comprend les systèmes de contrôle industriel et les systèmes de contrôle et d'acquisition de données. À la maison, le thermostat qui commande votre fournaise est un exemple de TO. La TO assure l'interface entre le cyberespace et les systèmes physiques, comme les vannes, les registres et les ventilateurs, que l'on retrouve dans tout, des systèmes de chauffage, de ventilation et de climatisation jusqu'aux oléoducs servant au transport du carburant. Même s'il est souvent possible de mettre à jour le code informatique de ces systèmes, cela ne se produit généralement qu'à l'occasion de révisions majeures ou, dans le pire des cas, lors de leur remplacement. Parfois, il est difficile de mettre ces systèmes à jour, car ils soutiennent des systèmes essentiels. On ne voudrait certainement pas arrêter une usine de traitement de l'eau ou désactiver régulièrement les systèmes de sûreté d'une centrale nucléaire pour mettre à jour leurs logiciels.

Dans certains cas, les mises à jour sont difficiles, voire impossibles, parce que l'équipement est inaccessible. Par exemple, il peut être nécessaire de vider des sections de l'usine de

traitement de l'eau pour accéder à certains équipements, ou un organe de commande essentiel peut se trouver dans une zone radioactive d'une centrale nucléaire. Même si les systèmes de TO relient le cyberespace aux systèmes physiques, la bonne pratique consiste à les isoler sur leurs propres réseaux et à ne pas, par exemple, les brancher directement à l'Internet.

Technologie de plateforme (TP)

La technologie de plateforme désigne la technologie opérationnelle utilisée sur les plateformes militaires. Elle comprend le matériel et les logiciels qui se trouvent à bord des navires, des aéronefs, des véhicules et des systèmes d'armes. Comme pour votre voiture, les microprocesseurs et les fils servant à contrôler les fonctions d'un véhicule blindé sont tous des exemples de TP. La TP comprend souvent des processeurs ou des microprocesseurs spécialisés qui commandent les fonctions de la plateforme, comme un système de guidage de missile. Il est souvent presque impossible de remplacer ces microprocesseurs; toute vulnérabilité qu'elles présentent subsiste donc pendant toute la durée de vie de l'équipement.

Puisqu'il est difficile de mettre à jour ou de remplacer la TO et la TP, nous devons assurer leur sécurité et veiller à ce que les mises à jour n'introduisent pas de vulnérabilités. Cette protection s'inscrit dans un effort plus vaste appelé *cyberassurance de la mission (CAM)* que le gouvernement du Canada définit comme « processus consistant à protéger ou à assurer la résilience des ressources et des capacités essentielles à la mission, contre les cybermenaces ou cyberactions, dans tout environnement d'opérations ou toute condition opérationnelle ». ⁶ En termes simples, la CAM est la capacité de mener des cyberopérations militaires au moyen de capacités militaires qui reposent sur le cyberespace, lequel peut être contesté. Dans un contexte naval, par exemple, un navire devrait encore être en mesure d'utiliser ses réseaux et ses capacités techniques pour combattre, flotter ou se déplacer dans un cyberenvironnement contesté. La CAM peut aussi consister à assurer la sécurité de ces systèmes et de leurs chaînes d'approvisionnement, tant au cours de leur mise au point qu'une fois qu'ils sont déployés. Puisque les chaînes d'approvisionnement technologiques sont souvent de nature mondiale, il existe toujours un risque que les systèmes, les logiciels et les capacités techniques que les FAC acquièrent soient éventuellement exploités. Les commandants qui adhèrent aux principes de la CAM doivent prévoir des plans de rechange pour continuer à exécuter la mission, peu importe la cybermenace.

Internet des objets (IdO)

Les appareils de l'Internet des objets deviennent moins coûteux, plus pratiques et faciles à adapter, si bien qu'il ne soit pas surprenant qu'ils finissent par fournir certaines capacités essentielles dans le cadre d'une opération militaire. L'Internet des objets

comprend des éléments de TI et de TO de qualité grand public et d'entrée de gamme. Parmi les exemples d'IdO, mentionnons les ampoules intelligentes, les verrous intelligents et les appareils électroménagers intelligents, ainsi que les thermostats connectés, caméras, sonnettes et moniteurs pour bébé connectés à l'Internet. Ils offrent souvent des capacités utiles, comme la surveillance de votre propriété au moyen d'une caméra ou la commande automatique de lait par votre réfrigérateur lorsque vos réserves sont faibles. Les appareils de l'IdO sont souvent peu coûteux, dotés de processeurs à faible puissance et munis de mesures de sécurité minimales ou inexistantes, et ils peuvent être difficiles, voire impossibles à mettre à jour.

À mesure que les FAC sont confrontées à un environnement de menaces plus complexe et qu'elles doivent composer avec des processus d'approvisionnement difficiles, les appareils de l'IdO, qui étaient auparavant nouveaux et difficiles à intégrer, offrent maintenant des solutions simples. Cependant, ces appareils posent un *problème de complexité à faible coût*.⁷ Dans le passé, si les FAC voulaient acquérir une machine ou un dispositif spécialisé et complexe, elles devaient trouver un fournisseur spécialisé. Ce dispositif coûtait très cher, compte tenu des efforts et des ressources nécessaires à sa conception. Or, la situation est différente avec les appareils de l'IdO. Aujourd'hui, il est souvent moins coûteux de prendre un dispositif complexe et de le *faire passer* pour un dispositif simple que de fabriquer réellement un dispositif simple. Par défaut, en raison des économies d'échelle (il est moins coûteux de fabriquer des millions d'exemplaires d'un même produit que d'en fabriquer quelques exemplaires sur mesure), les fournisseurs sont encouragés à doter les appareils de l'IdO de toutes les fonctions possibles : Wi-Fi, stockage en nuage, apprentissage automatique, logiciels complexes, Bluetooth et microphones. Si une organisation (comme les FAC) veut utiliser ce dispositif pour une capacité opérationnelle sans la connectivité Wi-Fi, il est souvent plus simple et moins coûteux de désactiver cette fonction que de fabriquer une version sur mesure qui en est dépourvue. Néanmoins, cette fonction résiduelle demeure une vulnérabilité et, comme les appareils de l'IdO sont tristement célèbres pour la rareté des mises à jour de leur micrologiciel, cette vulnérabilité peut demeurer non corrigée et sujette à l'exploitation.

Ces caractéristiques font des appareils de l'IdO une cible idéale pour l'exploitation par des acteurs malveillants. Par exemple, le botnet Mirai a été observé pour la première fois en août 2016. Il a tiré parti de centaines de milliers d'appareils de l'IdO mal sécurisés, comme les moniteurs pour bébé et les caméras connectées à l'Internet, pour créer un réseau capable de submerger des cibles de paquets réseau dans le cadre d'attaques par déni de service distribué.⁸ Même si sa cible initiale était *Minecraft*, il a servi à de nombreuses autres attaques et son code source a fini par être publié dans un dépôt de code libre.⁹ Malgré les problèmes que ces appareils posent sur le plan de la sécurité, leur utilisation augmente en raison de leur commodité. Il ne serait pas surprenant qu'ils viennent un jour à fournir certaines

capacités essentielles dans le cadre d'une opération militaire. Si tel est le cas, nous devons être conscients des risques en cause, tout comme nous devrions l'être des risques liés à leur utilisation dans nos foyers.

Différence entre le cyberspace et l'environnement de l'information

Les lecteurs qui découvrent ce domaine pourraient employer indifféremment les termes *environnement de l'information* et *cyberspace*. Mais qu'est-ce que l'environnement de l'information? Le gouvernement du Canada le définit ainsi : « environnement comprenant l'information elle-même et les personnes, les organisations et les systèmes qui reçoivent, traitent et transmettent l'information, ainsi que les espaces cognitif, virtuel et physique dans lesquels cela se déroule ».¹⁰ Cependant, ce n'est pas la seule définition. Il en existe plusieurs autres, et la définition canadienne n'est pas universelle. Par exemple, selon le *Tallinn Manual*, une vaste étude universitaire (non contraignante) sur l'applicabilité du droit international à la cyberguerre et aux cyberopérations, l'environnement de l'information est « l'ensemble des personnes, des organisations et des systèmes qui recueillent, traitent et diffusent l'information, ou qui agissent sur cette base ».¹¹ Les deux définitions diffèrent, car la définition du *Tallinn Manual* met l'accent uniquement sur les acteurs et les systèmes, tandis que la définition du gouvernement du Canada englobe les acteurs, les systèmes et l'environnement dans lequel ils interagissent. À cet égard, la définition du gouvernement du Canada mentionne explicitement l'information comme partie intégrante du système, alors que la définition du *Tallinn Manual* ne mentionne pas l'information comme un objet en soi. Par ailleurs, même si la définition du gouvernement du Canada décrit explicitement l'environnement de l'information comme un environnement et insiste sur ce contexte, elle n'aborde pas le concept plus large d'*environnement*.

À la différence des environnements maritime, terrestre, aérien, spatial et cyberspatial, l'environnement de l'information n'est pas un environnement physique, même s'il interagit avec l'environnement physique à titre de support. Par exemple, si des troupes du pays A sont déployées dans un pays allié B pour dissuader une agression du pays C, et que le pays C ne souhaite pas encore recourir à une action militaire conventionnelle contre le pays B, il peut tirer parti de l'environnement de l'information. Le pays C pourrait créer des comptes sur les médias sociaux et des robots conversationnels pour diffuser de la désinformation sur les activités du pays A dans le pays B, en avançant que les troupes du pays A terrorisent la population locale, laissent des déchets un peu partout et commettent des crimes. Dans cet exemple, tous les commentaires laissés par les robots sur les médias sociaux sont des éléments de l'environnement de l'information. Le pays C utilise du matériel pour faire fonctionner ces robots (serveurs accueillant les réseaux de robots, stockage des données des utilisateurs, fichiers journaux et alimentation

permettant l'intégration aux applications de médias sociaux), et ce matériel fait partie du cyberspace. Une partie de ce contenu diffusé sur les médias sociaux peut se retrouver dans un journal, où ces allégations seront imprimées sur un support physique. Les citoyens du pays B consulteront ces messages au moyen d'appareils physiques, en passant par l'Internet. Ces appareils font eux aussi partie du cyberspace. Si les citoyens du pays B croient ces allégations et modifient leur opinion quant à l'accueil des troupes du pays A, l'environnement de l'information s'en trouve modifié.

Cet exemple illustre également la différence entre les opérations d'information et les cyberopérations, qui se distinguent par leurs objectifs et leur nature. Les opérations d'information portent principalement sur l'environnement de l'information et visent à modifier la façon dont la cible perçoit l'information. Les opérations d'information sont des « activités d'informations coordonnées dans ou par le biais de l'environnement d'information visant à produire des effets désirés sur la volonté, la compréhension et la capacité de personnes ».¹² Cette définition comporte quelques éléments essentiels : les actions ou opérations doivent être délibérées et synchronisées, viser à atteindre des résultats ou des effets précis, et cibler principalement des personnes. Supposons que Bob envoie un courriel à Alice pour lui présenter les points saillants de son projet, en vue de lui demander plus tard du financement. Ce courriel constitue une opération d'information, car Bob modifie positivement la perception qu'elle a du projet.

Alors que les opérations d'information visent à modifier la perception ou le comportement du sujet, les cyberopérations servent à modifier le support que constitue le cyberspace, en permettant des activités qui seraient normalement interdites, intentionnellement ou non, ou en empêchant des activités qui seraient normalement permises, intentionnellement ou non. Le cyberspace est au cœur des cyberopérations. Il est impossible de mener une cyberopération sans l'infrastructure du cyberspace. Les définitions usuelles mettent en évidence ce lien. Par exemple, le gouvernement du Canada définit une opération dans le cyberspace comme un « ensemble d'actions menées dans ou via le cyberspace dans le but de préserver la liberté de ses propres forces ou des forces amies dans le cyberspace ou de créer des effets permettant d'atteindre les objectifs militaires ».¹³ En termes plus simples, le *Tallinn Manual* décrit une cyberopération comme « l'emploi de cybercapacités ayant pour objectif principal d'atteindre des objectifs dans le cyberspace ou au moyen du cyberspace ».¹⁴ Quand on entend parler de *cyberopérations*, on pense souvent à des opérations spectaculaires du niveau de Stuxnet. Cependant, une cyberopération peut être aussi simple que l'application d'un correctif pour contrer délibérément un virus connu et, en définitive, modifier le cyberspace afin d'améliorer la santé du réseau.

Pourquoi les cyberopérations et les opérations d'information sont-elles souvent confondues, et comment sont-elles liées? D'abord, dans les deux cas, il s'agit de produire des effets, qu'ils portent sur la psyché humaine (opérations d'information) ou

sur des systèmes techniques (cyberopérations), et ces effets peuvent parfois se recouper. Certains peuvent présumer que les opérations d'information sont des cyberopérations, parce que des cyberopérations peuvent être menées en même temps que des opérations d'information. Comme nous l'avons mentionné, le cyberspace est un support que les gens utilisent pour accéder à l'environnement de l'information (par exemple, en se servant d'un ordinateur pour effectuer des recherches). Nous confondons souvent les câbles, les serveurs et les routeurs (les éléments matériels du cyberspace) avec l'environnement de l'information, parce que nous pouvons les utiliser pour communiquer de l'information. Ces deux concepts prêtent aussi à confusion parce qu'à une certaine époque, les opérations d'information et les cyberopérations étaient regroupées dans une seule et même catégorie. Enfin, la confusion est entretenue par le fait que les équipes désignées pour les cyberopérations se voient habituellement confier la tâche d'influer sur l'environnement de l'information : une cyberopération peut avoir des effets liés à l'information, et les opérations d'information peuvent tirer parti du cyberspace. Par exemple, si Alice hésite encore à financer le projet de Bob, celui-ci pourrait engager Ève pour lui envoyer un enregistreur de frappes (application cachée qui enregistre les touches du clavier et parfois l'écran) afin d'infecter l'ordinateur d'Alice et de recueillir des renseignements susceptibles de servir au chantage. Bob pourrait ensuite utiliser ces renseignements pour influencer sur la décision d'Alice. Il est toutefois possible de mener cette opération d'information entièrement en dehors du cyberspace. Par exemple, Bob pourrait agraffer sur le campus des affiches contenant de la désinformation au sujet des recherches d'Alice afin de susciter un climat défavorable.

Il existe donc des moyens d'influer sur le comportement ou les décisions d'un public cible sans recourir au cyberspace. Nous avons utilisé un exemple fictif pour illustrer la différence entre les opérations d'information et les cyberopérations, et la section suivante porte sur la métaphore bien connue du château, qui fait ressortir les distinctions entre les cyberopérations et les opérations de réseau. L'article distingue ensuite la cyberdéfense de la cybersécurité.

La métaphore du château : cyberopérations et opérations de réseau

Les débutants peuvent rencontrer la métaphore de la forteresse ou du château en tant qu'explication simplifiée de la façon dont un réseau ou un ordinateur est protégé. Dans cette métaphore, un défenseur peut protéger un bien derrière des couches de défense, comme les dirigeants de l'époque médiévale qui fortifiaient une structure au moyen d'un fossé et de murs d'enceinte épais, parfois arrondis pour empêcher l'ennemi de les escalader, et de murs intérieurs servant à diviser le château en différentes zones d'accès (basse cour, haute cour, donjon). Même si les couches de défense réduisent le risque d'intrusion, il demeure toujours

possible qu'une force ennemie tente de briser ces défenses. De même, le fait de creuser un fossé et d'ériger des murs d'enceinte ne signifie pas que le travail est terminé. Les défenseurs doivent évoluer au même rythme que leurs adversaires. Si les murs offrent une bonne protection contre les flèches et les frondes, rien ne garantit que ces murs et ce fossé résisteront suffisamment bien aux catapultes. Par ailleurs, le défenseur doit assurer l'entretien continu de ces défenses. Les murs doivent être réparés lorsqu'ils sont endommagés et surveillés pour repérer les ennemis et toute personne qui tenterait de les escalader.¹⁵

Les parallèles avec un réseau sont évidents. Les murs du château sont souvent assimilés à un pare-feu, qui laisse entrer certains éléments, mais pas d'autres, et qui assure un périmètre défensif. Les murs intérieurs du château ressemblent aussi au cloisonnement des réseaux, qui permet de segmenter les différentes parties du réseau en fonction des niveaux d'accès privilégiés. Ainsi, si un assaillant franchit les murs du château, il se peut qu'il soit incapable d'accéder à la basse-cour ou au donjon. L'exigence d'un mot de passe pourrait s'apparenter au levage de la herse. À l'instar d'un château, les défenses du réseau doivent être constamment mises à jour au fur et à mesure que les ennemis évoluent : les défenseurs du réseau doivent appliquer des correctifs, mettre à jour les listes de signatures de logiciels malveillants et ajuster la configuration de leurs listes de permissions et d'interdictions. Ce processus est sans fin.

La défense peut aussi devenir encore plus active. Si vous envoyez vos troupes au-delà des murs pour repérer la catapulte et la détruire, nous appellerons ces actions des *cyberopérations défensives—mesures d'intervention*, ce qui correspond simplement à une forme d'autodéfense dans le cyberdomaine afin d'assurer la *liberté d'action*.¹⁶ Si vous prenez pour cible les troupes adverses et détruisez leur château, ou si vous capturez leur drapeau et hissez le vôtre, dans le monde du cyberspace, nous parlerions alors de *cyberopérations offensives*, puisqu'il s'agit d'une opération visant à « projeter une puissance dans le cyberspace ou au moyen de celui-ci pour produire des effets à l'appui d'objectifs militaires ». ¹⁷ Dans un contexte de cybersécurité, cela pourrait consister, par exemple, à surcharger l'infrastructure de l'adversaire de trafic pour perturber sa capacité à mener des campagnes de désinformation.

La métaphore du château peut aussi servir à préciser les différences entre les cyberopérations et les opérations de réseau. Nous avons déjà abordé les cyberopérations, mais les opérations de réseau s'entendent des « activités entreprises pour approvisionner, sécuriser, configurer, exploiter, étendre, maintenir et soutenir un réseau ». ¹⁸ Dans le cadre de cette métaphore, il s'agit des activités générales nécessaires au maintien du château : veiller à l'entretien des murs d'enceinte, s'assurer que les ressources, comme la nourriture, l'eau et les armes sont disponibles, que les portes fonctionnent pour permettre les entrées et les sorties, et que des gardes sont présents pour surveiller les murs et l'entrée. Ces fonctions sont analogues à des éléments des opérations de

réseau : pare-feu, listes de contrôle d'accès, disponibilité de la bande passante et présence d'administrateurs réseau pour régler les problèmes. Si les murs du château tombent en ruine, il peut être difficile de savoir si cela est dû à l'action d'un assaillant ou au mauvais entretien des murs. Il en va de même pour les opérations de réseau. Si certains appareils ne sont plus connectés au réseau, cela peut être attribuable à un acteur malveillant qui les a pris pour cible ou au fait que le Centre d'opérations des réseaux n'a pas mis à jour le micrologiciel et qu'un correctif récent a provoqué la déconnexion de ces appareils. Si un réseau est mal entretenu, comme un château, il devient difficile de savoir rapidement si un problème est banal ou malveillant.

Cependant, la métaphore du château comporte des limites générales. Premièrement, elle établit une dangereuse dichotomie entre l'intérieur et l'extérieur. ¹⁹ Tous les réseaux ne sont pas aussi tranchés. Par exemple, de nombreux réseaux comportent des zones démilitarisées, où sont hébergés des biens accessibles à partir de l'Internet, mais qui ne peuvent pas communiquer directement avec les bases de données internes. La zone démilitarisée constitue donc un type de zone intermédiaire qui est protégée par le pare-feu, mais qui n'est pas entièrement interne. Deuxièmement, la métaphore du château suggère que toutes les menaces proviennent de l'extérieur. Tandis que les châteaux ne privilégiaient généralement pas les défenses internes, les réseaux modernes appliquent souvent un contrôle d'accès fondé sur les rôles pour limiter les privilèges, même une fois à l'intérieur du réseau. Toutefois, même avec ces contrôles, les menaces internes (Ortis, Snowden, Reality Winner, Manning, etc.) prouvent que toutes les menaces ne viennent pas de l'extérieur.²⁰

Cybersécurité et cyberdéfense : principales différences

Si vous travaillez depuis peu en cybersécurité au ministère de la Défense nationale, vous aurez peut-être remarqué que l'on emploie parfois indifféremment les termes cybersécurité et cyberdéfense, même s'il s'agit de notions tout à fait distinctes au sein du MDN. Dans l'appareil gouvernemental en général, le terme cybersécurité sert à décrire les processus visant à sécuriser la composante TI du cyberspace. Toutefois, au MDN, on distingue la cybersécurité de la cyberdéfense. Contrairement aux autres ministères, le MDN dispose de technologies de plateforme et doit protéger ces technologies contre l'ennemi dans des contextes opérationnels. La cybersécurité constitue la base nécessaire à toutes les activités de cyberdéfense, ce qui pourrait expliquer en partie pourquoi ces deux termes sont souvent confondus. La cybersécurité englobe les activités qui visent à assurer la santé et le stockage sécuritaire des biens, indépendamment de la présence d'un acteur hostile. La confidentialité, l'intégrité et la disponibilité sont au cœur de ces préoccupations. La confidentialité garantit que l'information demeure privée et accessible uniquement aux personnes autorisées à la consulter; l'intégrité

assure que l'information reste exacte et inchangée; et la disponibilité signifie que les utilisateurs peuvent accéder à l'information dont ils ont besoin, au moment voulu, sans retard ni difficulté.²¹

En pratique, la cybersécurité peut, par exemple, consister à exiger que les utilisateurs emploient des mots de passe pour accéder aux biens ou aux systèmes, à appliquer un contrôle d'accès fondé sur les rôles pour gérer l'accès et les privilèges (confidentialité), à utiliser des sommes de contrôle pour vérifier que le logiciel offert en téléchargement est bien la bonne version (intégrité), à exiger des signatures numériques (intégrité), à prévoir un plan de reprise après sinistre en cas de catastrophe naturelle ou d'urgence (disponibilité) ou à surveiller le rendement du système (disponibilité).

Alors, en quoi la cybersécurité diffère-t-elle de la cyberdéfense? Certes, les pratiques de cybersécurité peuvent contribuer à dissuader un acteur de menace d'accéder aux données, de les modifier ou d'en refuser l'accès. Cependant, la cyberdéfense s'en distingue, car, contrairement à la cybersécurité, elle suppose la présence d'un acteur hostile dans le cyberspace et comporte des efforts visant à détecter, à prévenir et à contrer les menaces dirigées contre le réseau. Une cybermenace ou un acteur de menace est au cœur de cette définition, alors que cette notion est absente de la définition de la cybersécurité.

Même si aucune analogie n'est parfaite (comme l'a montré la métaphore du château plus haut), la différence entre les deux concepts se prête bien à une analogie sur le hockey. La cybersécurité ressemble beaucoup au filet en dehors d'un match de hockey. Plus le cadre du filet est petit, plus il est difficile pour des éléments indésirables (y compris la rondelle) de pénétrer dans la zone de but. Il se peut que le filet reste sur la glace pendant les séances de patinage libre et que de jeunes enfants s'y aventurent par mégarde. On espère alors que le personnel d'entretien de la patinoire sera présent pour s'assurer que le filet demeure intact et qu'il reste en dehors de la zone accessible. Si un patineur trop enthousiaste fonce accidentellement dans le but et déchire le filet, le personnel d'entretien réparera la déchirure pour que le filet puisse remplir sa fonction. Ce même personnel pourra remplacer le cadre s'il se corrode, afin d'en préserver l'intégrité de la structure. Le personnel pourra ensuite retirer le filet de la glace pendant le patinage libre pour qu'il soit disponible pour les parties. Toutes ces pratiques se rapprochent de l'entretien courant en cybersécurité : veiller à ce que le trafic indésirable soit tenu à l'écart du réseau et, si le réseau est endommagé par inadvertance, le réparer et éventuellement l'isoler d'autres incidents susceptibles d'avoir une incidence sur sa disponibilité; il s'agit là de pratiques normales.

À l'inverse, la cyberdéfense s'apparente à un match de hockey. Le filet peut être considéré comme la composante de cybersécurité. Plus la cybersécurité est robuste, plus le « filet » est petit (et plus la surface d'attaque est réduite). Le filet peut être fait d'un meilleur matériau, équipé d'un système d'ouverture automatisé, remplacé et remis à neuf à chaque changement, etc. Tous ces

ajustements rendent plus difficile la réussite de l'équipe adverse. De la même façon, ils évoquent les pratiques de cybersécurité, où les propriétaires de réseaux peuvent ajuster les règles des pare-feu et appliquer régulièrement des correctifs pour réduire la surface d'attaque de leur réseau. Néanmoins, comme au hockey, peu importe la qualité de conception de votre filet (ou de vos pratiques de cybersécurité), si vous n'avez pas de gardien de but, l'adversaire pourra marquer des points facilement. La cyberdéfense revient à ajouter un gardien devant le filet. L'équipe locale place un gardien dans le but pour empêcher la rondelle d'y entrer. Plus l'équipement du gardien est imposant et plus ses réflexes sont rapides, plus il est difficile pour l'autre équipe de marquer. L'entraîneur peut aussi informer le gardien et les joueurs en défense sur les attaquants de l'autre équipe et sur les stratégies ou les jeux qu'ils privilégient. L'équipe locale peut ensuite utiliser ces renseignements pour empêcher l'autre équipe de marquer. De la même manière, en cyberdéfense, les défenseurs du réseau peuvent investir dans des outils de détection de signatures de logiciels malveillants (un nouvel équipement) pour empêcher un acteur de cybermenace de percer le réseau. Ils peuvent aussi recourir à l'analyse heuristique, à des systèmes de détection d'intrusion ou à la connaissance des techniques, tactiques et procédures pour repérer certains acteurs de menace, atténuer la menace ou améliorer les délais d'intervention. Dans cet exemple, l'équipe doit prendre des mesures défensives précises pour se protéger contre l'autre équipe. Cependant, contrairement à un match de hockey, la cyberdéfense et la cybersécurité sont des activités soutenues, menées en tout temps, qui ne prennent jamais vraiment fin. La différence entre les deux notions sera aussi utile pour la section suivante, qui présente le continuum des cyberévénements, des cyberincidents et des compromissions.

Distinguer les cyberévénements des cyberattaques : comprendre l'échelle des activités

Certaines activités ou anomalies dans le cyberspace sont parfois regroupées dans un même « panier » sous l'étiquette de *cyberattaque*. Toutefois, sur le plan technique, il existe des différences. Nous devons distinguer les types d'activités pour pouvoir ajuster l'ampleur des mesures d'intervention. Par exemple, si vous venez d'arriver dans une équipe et que vous recevez un courriel d'hameçonnage (auquel vous ne répondez pas) et que vous affirmez qu'il y a eu une cyberattaque, cette qualification est erronée et amplifie indûment l'incident. Le gouvernement canadien utilise les définitions énoncées dans le *Plan de gestion des événements de cybersécurité du gouvernement du Canada* pour distinguer les différents types d'activités.²² La principale différence entre les catégories tient au degré de gravité et au niveau de certitude quant à la compromission.

À l'extrémité la moins grave de l'échelle, on trouve l'événement de sécurité, c'est-à-dire tout événement qui *peut* avoir entraîné

une compromission.^{23,24} Parmi les exemples d'événements de sécurité, mentionnons un courriel d'hameçonnage ciblé sur lequel la cible n'a pas cliqué ou des requêtes inhabituelles bloquées par un pare-feu. Même si certains de ces événements peuvent être malveillants, il est essentiel de reconnaître qu'un événement n'est pas la même chose qu'une compromission. Si une organisation traite chaque événement comme une atteinte à la sécurité, elle sera submergée par le nombre d'alertes, ce qui mènera à une lassitude face aux alertes et étirera les ressources déjà limitées.

Un événement de sécurité peut devenir un *incident de sécurité* lorsqu'il y a atteinte à la sécurité et que le système est compromis.²⁵ Par exemple, si un acteur de cybermenace envoie un courriel de harponnage à un employé et que l'employé clique sur un lien malveillant incorporé au courriel ou ouvre une pièce jointe infectée et télécharge un logiciel malveillant, l'événement de sécurité (le courriel) devient un incident de sécurité (téléchargement réussi du logiciel malveillant). L'événement devient un incident dès que le réseau est compromis.

Conclusion

Nous avons rédigé le présent article à l'intention des personnes qui se joignent à la communauté de la cybersécurité du gouvernement du Canada, dans l'espoir de les aider à reconnaître les idées fausses courantes auxquelles elles pourraient être confrontées. Après avoir lu cet article, nous estimons que tous

les lecteurs devraient posséder les mêmes connaissances de base. Les lecteurs devraient comprendre que le cyberspace est un objet physique, aussi banal et peu enthousiasmant que cela puisse paraître à certains. Le cyberdomaine correspond au cyberspace et à tout ce qui l'entoure. Il s'agit également de l'un des cinq domaines reconnus de la guerre que les FAC s'emploient activement à opérationnaliser.

Cet article ne cherche-t-il qu'à couper les cheveux en quatre? Pourquoi consacrer un article entier à des définitions que l'on retrouve déjà dans un enchevêtrement de notes de doctrine interarmées, de documents politiques, d'annexes, de glossaires et de présentations? Pourquoi est-il important de dire *cyberopération* plutôt qu'*opération d'information* si la plupart des gens comprennent de toute façon ce que l'on veut dire? En réalité, les FAC et le MDN se trouvent dans une situation particulière. Contrairement aux États-Unis, à la Chine et à la Russie, les FAC et le MDN sont en train de bâtir les assises de cybercapacités militaires essentielles. À mesure que le COMCYBERFAC sera pleinement opérationnel et que plusieurs équipes interagiront avec cette capacité, il sera important que tous parlent le même langage et emploient les termes avec justesse, afin d'éviter la confusion et les malentendus. Nous espérons que les explications simplifiées présentées ici auront permis de mieux comprendre la façon dont le cyberdomaine est structuré, ses liens avec les autres domaines et les raisons pour lesquelles il est peut-être plus simple à appréhender que ne le croient certains.

Notes

- Gouvernement du Canada, « Cyberopérateur : Nouvel insigne de métier des Forces armées canadiennes », La Feuille d'érable, 11 janvier 2022, source originale : <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/defense/2022/01/cyberopérateur-nouvel-insigne-metier-forces-armees-canadiennes.html>.
- Gouvernement du Canada, « Félicitations aux premiers cyberopérateurs diplômés de l'EECF », La Feuille d'érable, 21 septembre 2021, source originale : <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/defense/2021/09/felicitations-premiers-cyberopérateurs-diplomés-eeccf.html>.
- Gouvernement du Canada, « Mars 2020 - Forces armées canadiennes 101 », Défense 101 - cahier de transition mars 2020, s.d., 2, source originale : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/transition-ministerielle/defense-101/2020/03/defense-101/fac-101.html>.
- Gouvernement du Canada, « Cyberopérateur : Nouvel insigne de métier des Forces armées canadiennes ».
- Statistique Canada, « Protéger nos foyers et nos droits : servir dans les Forces armées canadiennes », (Gouvernement du Canada, 13 juillet 2022), source originale : <https://www150.statcan.gc.ca/n1/daily-quotidien/220713/dq220713c-fra.htm>.
- Gouvernement du Canada, « Cyber Mission Assurance », dans Banque de terminologie de la défense, s.d., source originale : https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&srchtxt=cyber%20mission%20assurance&context2nd_wet=1&index=alt.
- Bruce Schneier, « Security and Cheap Complexity », Schneier on Security, blogue, 26 août 2022, source originale : <https://www.schneier.com/blog/archives/2022/08/security-and-cheap-complexity.html>.
- « Heightened DDoS Threat Posed by Mirai and Other Botnets », CISA, s.d., source originale : <https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets>.
- Scott J. Shackelford et Scott O. Bradner, « Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything », Hastings Law Journal 72, no 2 (2021), source originale : https://repository.uchastings.edu/cgi/viewcontent.cgi?article=3921&context=hastings_law_journal.
- Gouvernement du Canada, « Information Environment », dans Banque de terminologie de la défense, s.d., source originale : [dtb.terminology.mil.ca](https://www.dtb.terminology.mil.ca).
- « Glossary », dans Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 282.
- Gouvernement du Canada, « Information Operation », TERMIUM Plus, s.d.
- Gouvernement du Canada, « Cyber Operation », TERMIUM Plus, s.d.
- « Glossary », op.cit.
- Deborah A. Frincke et Matt Bishop, « Guarding the Castle Keep: Teaching with the Fortress Metaphor », IEEE Security & Privacy 2, no 3 (2004) : 69-72.
- Gouvernement du Canada, « Defensive Cyber Operation - Response Action », TERMIUM Plus, s.d.
- Gouvernement du Canada, « Offensive Cyber Operation », TERMIUM Plus, s.d.
- Gouvernement du Canada, « Network Operations », dans Banque de terminologie de la défense, s.d.
- Christian Leuprecht, David B. Skillicorn et Victoria E. Tait, « Beyond the Castle Model of Cyber-Risk and Cyber-Security », Government Information Quarterly 33, no 2 (s.d.) : 250-257.
- Christian Leuprecht et al., op.cit.
- National Institute of Standards and Technology, « NIST Special Publication 1800-26A », National Cybersecurity Center of Excellence, 2020, source originale : <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>.
- Gouvernement du Canada, « Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) », 2019, source originale : <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientations-politiques-matiere-cybersecurite/gestion-incidents-securite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html>.
- Gouvernement du Canada.
- National Institute of Standards and Technology, « Cadre pour l'amélioration de la cybersécurité des infrastructures critiques », NIST, s.d., source originale : <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018fr.pdf>.
- National Institute of Standards and Technology.