

La cybersécurité et la puissance aérienne : préserver l'intervention humaine

KRISTEN CSENKEY ET ALEXIS RAPIN

Kristen Csenkey, Ph.D. est boursière postdoctorale du Conseil de recherches en sciences humaines (CRSH) au Brian Mulroney Institute of Government de l'Université Saint-Francis Xavier. Elle est également chercheuse associée au Canadian Maritime Security Network, au Centre for Military, Security and Strategic Studies de l'Université de Calgary ainsi qu'au Réseau de défense de la sécurité de l'Amérique du Nord et de l'Arctique (RDSNAA), entre autres. Kristen Csenkey a dirigé plusieurs projets financés par le ministère de la Défense nationale portant sur les répercussions des technologies quantiques, des systèmes aéronautiques connectés et des véhicules électriques cyberrésilients sur la défense et la sécurité. Elle dirige actuellement un projet financé par une subvention d'engagement partenarial du CRSH, consacré à la gouvernance responsable des technologies quantiques à l'échelle mondiale. Elle est titulaire d'un baccalauréat spécialisé en sciences (H.B.Sc.), d'une maîtrise ès arts (M.A.), d'une maîtrise en administration publique (M.A.P.) et d'un doctorat (Ph. D.).

Alexis Rapin est chercheur associé à la Chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'Université du Québec à Montréal (UQAM). Ses travaux de recherche portent sur la cybersécurité et sur les répercussions des technologies numériques sur la sécurité internationale. En 2023, il a témoigné devant le Comité permanent de la défense nationale de la Chambre des communes du Canada au sujet de la cyberdéfense et de la stratégie du Canada. Il est également membre du comité de rédaction de la plateforme francophone Le Rubicon, consacrée à l'analyse des affaires internationales et stratégiques.

Dans leur roman 2034 (publié en 2021), Elliot Ackerman et l'ancien amiral de la marine des États-Unis James G. Stavridis imaginent un conflit majeur opposant les États-Unis et la Chine.¹ Les premières pages s'ouvrent sur un incident au cours duquel un chasseur américain F-35 est soudainement capturé par l'Iran, après qu'une cyberattaque a permis à ce dernier de prendre le contrôle à distance de l'appareil. Plus loin dans le livre, confrontée à une situation désespérée, la Marine américaine décide de retirer sa flotte de F-35 du service et de remettre en service ses anciens F-18, dont la plupart des systèmes électroniques embarqués ont été retirés. Comme ses adversaires ont réussi à compromettre ses aéronefs de haute technologie, les États-Unis sont contraints de revenir à des appareils d'une génération antérieure, jugés plus sûrs sur le plan numérique.

Bien qu'il s'agisse d'un scénario fictif fascinant,² la situation décrite dans 2034 renvoie à une idée qui gagne du terrain dans la littérature stratégique : les approches fondées sur la supériorité technologique, qui caractérisent les forces armées occidentales depuis près de quarante ans, pourraient désormais constituer une vulnérabilité.³ À mesure que les capacités de cyberguerre progressent, les adversaires semblent désormais en mesure d'exploiter les dépendances émergentes ainsi que les vulnérabilités potentielles associées aux technologies fortement interconnectées. En outre, des pratiques inégales de gestion collective des risques, la présence de systèmes existants vieillissants et l'élargissement de la surface d'attaque accroissent l'exposition aux cyberattaques sophistiquées ainsi qu'aux composants

électroniques, aux systèmes, aux processus, aux technologies et aux personnes susceptibles d'être compromis. Les conflits géopolitiques actuels illustrent déjà cette convergence et cette complexité. Ainsi, face à l'invasion russe toujours en cours, les forces armées ukrainiennes ont remis en service d'anciens téléphones de campagne le long de la ligne de front, craignant que leurs systèmes modernes de transmission ne soient compromis par l'adversaire.⁴

Dans le présent article, nous adoptons une conception large de la cyberguerre et des technologies connectées, qui englobe à la fois le cyberspace et la guerre électronique. Même si les opérations, menées dans le cyberspace et dans le spectre électromagnétique, présentent des caractéristiques distinctes, notamment en ce qui concerne les unités, les capacités et l'expertise mises en œuvre, nous nous intéressons principalement aux conséquences des vulnérabilités, des capacités et des activités humaines et technologiques qui leur sont associées. De façon plus générale, nous inscrivons cette réalité dans un concept global du cyberspace, où les moyens électromagnétiques, comme le brouillage des radiofréquences, et les tactiques cybernétiques, comme le piratage informatique, s'inscrivent dans un espace dynamique où les personnes et les technologies interagissent au sein d'un environnement à la fois numérique et physique.⁵ Cet environnement soulève des défis dans tous les domaines d'opérations. Nous soutenons donc qu'il faut agir tant sur les vulnérabilités humaines que sur les vulnérabilités techniques.

La problématique des technologies interconnectées et des menaces qui y sont associées revêt une importance particulière dans le domaine de l'aviation, où les avions, les drones, les hélicoptères⁶ ainsi que les infrastructures numériques et physiques qui les soutiennent sont désormais fortement numérisés et interconnectés. Dans un scénario qui a peut-être inspiré Ackerman et Stavridis, les États-Unis ont perdu, en 2011, un drone de surveillance après que l'Iran a piraté son système GPS afin de le faire atterrir sur une base iranienne.⁷ Les drones ne sont plus considérés comme les composantes d'une « force aérienne du pauvre »,⁸ surtout lorsqu'ils sont associés à de nouvelles tactiques⁹ et procédures¹⁰ cybernétiques ainsi qu'à des technologies commerciales de plus en plus accessibles.¹¹ D'autres auteurs ont également montré que le F-35, désormais utilisé par un nombre croissant de forces armées occidentales, représente l'exemple même d'un système d'armes fortement exposé aux cybermenaces.¹² Les cybermenaces ne relèvent plus de l'hypothèse. Elles constituent une réalité à laquelle les forces aériennes modernes doivent continuellement se préparer, répondre et s'adapter, tout en comprenant les liens étroits qui unissent désormais les environnements numériques et physiques. Le défi est clair : protéger les forces contre ces menaces sans sacrifier les avantages opérationnels que procurent les technologies de pointe.

L'un des principaux enjeux réside dans le fait que le « techno-solutionnisme » militaire, hérité des années 1990 et 2000,¹³ pourrait céder la place à un « techno-pessimisme », dans lequel les forces armées en général, et les forces aériennes en particulier, perdraient progressivement confiance dans leurs technologies de pointe et finiraient par en abandonner certaines, comme c'est le cas dans 2034. En effet, la grande force des capacités tient non seulement à leur capacité de compromettre la disponibilité et l'utilité des technologies militaires, mais aussi à leur aptitude à éroder la confiance que les décideurs leur accordent. En instillant simplement un doute quant à l'intégrité d'un système, une cyberattaque peut dissuader un acteur d'utiliser un éventail beaucoup plus large de capacités et produire ainsi des effets disproportionnés par rapport à son incidence réelle. Certains auteurs, dont Christopher Coker,¹⁴ avancent qu'une telle approche pourrait constituer une stratégie d'avenir pour des puissances étrangères comme la Chine. Plutôt que de chercher à égaler un adversaire technologiquement supérieur, un État pourrait tenter de le convaincre que certaines de ses technologies sont compromises ou devenues inefficaces, afin de le pousser à en réduire lui-même l'utilisation.

Dans cette perspective, maintenir et protéger la confiance que les forces armées occidentales accordent aux technologies qu'elles utilisent et dans lesquelles elles ont investi des ressources considérables constitue un enjeu stratégique de première importance.¹⁵ Cet enjeu devient encore plus crucial en période de crise, lorsque des décisions rapides et difficiles doivent être prises quant à la fiabilité des technologies de l'information. Le présent article propose des pistes de solution à ce défi. Nous préconisons

une approche qui place les personnes au cœur de la protection de la puissance aérienne contre les cybermenaces. Cette approche consiste à développer le capital humain et les structures organisationnelles nécessaires au maintien d'un haut niveau de confiance et de résilience technologique au sein d'une force aérienne. Alors que l'Aviation royale canadienne (ARC) célèbre son centenaire, adapte ses capacités afin de défendre et de protéger le Canada et continue de contribuer, avec les États-Unis, à la défense de l'Amérique du Nord, le moment est particulièrement propice pour examiner l'interconnexion croissante entre les domaines, les technologies et le rôle toujours essentiel des personnes dans un environnement en constante évolution.

BOYD 2.0 : RÉINVENTER LA BOUCLE

Pour bien comprendre l'enjeu, il faut d'abord revenir aux origines du paradigme du techno-solutionnisme, et plus particulièrement à l'un de ses concepts fondamentaux : la célèbre « boucle OODA » (observation, orientation, décision, action), élaborée par le colonel de l'United States Air Force, John Boyd, dans les années 1980.¹⁶ Conçue pour décrire le processus par lequel un acteur perçoit une situation, l'analyse, délibère, puis agit en conséquence, la boucle OODA a depuis acquis une notoriété considérable et a été appliquée, avec plus ou moins de succès, à une multitude de domaines non militaires, allant des affaires au sport. Dans le domaine militaire, le concept de la boucle OODA a progressivement donné naissance à une véritable théorie de la victoire, adoptée par plusieurs grandes forces armées occidentales,¹⁷ notamment celles des États-Unis, du Royaume-Uni et de la France.¹⁸ En résumé, le principe fondamental veut que l'acteur qui parvient à franchir les étapes de la boucle OODA le plus rapidement acquière un avantage sur son adversaire. Entre autres avantages, l'exécution rapide de cette boucle est censée procurer une meilleure connaissance de la situation et, ultimement, permettre de maîtriser le rythme des opérations.¹⁹ Au cours des années 1990, cette logique a conduit les forces armées à se doter de technologies de commandement, de contrôle, de communications, d'informatique, de renseignement, de surveillance et de reconnaissance (C4ISR) toujours plus perfectionnées afin d'accélérer l'exécution de la boucle OODA.

Toutefois, le paradigme de la boucle OODA paraît aujourd'hui fragilisé par la complexité croissante et le développement des capacités de guerre électronique et de cyberguerre. Puisque les cybermoyens peuvent compromettre les technologies de l'information, dont dépend largement la fluidité de la boucle OODA, ils semblent remettre en cause un mode de conduite de la guerre fondé en grande partie sur la supériorité technologique et informationnelle.²⁰ Certaines approches de conceptualisation des cyberopérations montrent qu'il est possible de neutraliser un adversaire dans un conflit ouvert, en compromettant ses capacités de collecte du renseignement ou ses systèmes de communication.²¹ À cet égard, les cybermenaces revêtent

une importance particulière dans le domaine aérien, où les technologies numériques sont non seulement omniprésentes et essentielles à l'accomplissement des missions, mais constituent également des vecteurs d'attaque potentiels. Les forces aériennes doivent désormais composer avec des cybermenaces, les risques associés à l'utilisation de technologies complexes et à leur interconnexion, ainsi qu'avec diverses formes d'intervention humaine, comme l'usurpation des signaux GPS,²² le piratage des logiciels embarqués²³ ou la compromission des liaisons de données,²⁴ sans oublier les menaces visant les bases aériennes et les infrastructures physiques. Ainsi, durant la crise du golfe d'Oman en 2019, les forces armées des États-Unis ont infiltré une base de données, exploitée par le Corps des gardiens de la révolution islamique, afin de neutraliser les capacités de ciblage de l'Iran, notamment celles utilisées pour les drones d'attaque.²⁵ Lorsqu'un adversaire exploite les vulnérabilités décrites précédemment, il peut ralentir considérablement, voire paralyser, l'exécution de la boucle OODA.

Malgré les nombreux usages - et mésusages - dont elle a fait l'objet au fil des ans, la boucle OODA demeure un cadre d'analyse utile pour notre propos, puisqu'elle met en évidence deux aspects essentiels de la gestion des cybermenaces. Premièrement, le principe de la boucle OODA s'applique aux situations liées aux cyberattaques, à la posture et à la planification. Lorsqu'une force armée est confrontée à un cyberincident, elle doit être en mesure d'observer les effets des activités de piratage, de *s'orienter* dans l'environnement perturbé par l'attaque, de *décider* avec assurance quelles capacités sont compromises et lesquelles demeurent opérationnelles, puis d'*agir* à partir de cette analyse. Le concept de la boucle OODA peut ainsi servir à comprendre les effets d'une attaque et à déterminer les mesures qui s'imposent. Certes, la boucle OODA ne constitue pas une méthode d'intervention en cas de cyberincident. Elle offre néanmoins un cadre utile pour renforcer la confiance envers les personnes et les technologies, comme nous le montrerons plus loin.²⁶

Deuxièmement, même si les technologies de l'information constituent d'importants facteurs facilitants et accélérateurs de la boucle OODA, elles n'en représentent nullement les seules composantes. Les processus par lesquels une force armée recueille et traite l'information reposent également sur des dimensions humaines et organisationnelles essentielles, dont l'importance est comparable à celle des technologies elles-mêmes.²⁷ Comme l'ont montré plusieurs auteurs, les forces armées modernes n'exploitent pas toujours pleinement les technologies les plus avancées, en raison d'une gestion insuffisante des facteurs humains et organisationnels.²⁸ Bien entendu, la rapidité d'exécution de la boucle OODA ne constitue pas, à elle seule, la clé du succès des opérations militaires contemporaines. Il n'en demeure pas moins que les facteurs humains et organisationnels jouent un rôle déterminant dans ce processus et doivent continuer à évoluer afin d'en préserver la fluidité. Le véritable défi consiste donc à déterminer comment tirer le meilleur parti des ressources

humaines et organisationnelles disponibles afin de maintenir, ou de rétablir, la fluidité de la boucle OODA dans un contexte où les technologies sont—ou semblent être—dégradées.

Dans les sections qui suivent, nous présentons des exemples tirés de l'expérience des alliés internationaux du Canada ainsi que des pistes visant à renforcer la résilience dans les environnements de conflit numériques et physiques. Enfin, nous regroupons notre analyse et nos recommandations dans le contexte de la modernisation du NORAD et de la coopération binationale, telles qu'elles sont mises en évidence dans la récente mise à jour de la politique de défense *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*. Ce faisant, nous mettons en lumière les liens étroits qui unissent les dimensions aérienne, humaine et du cyberspace de la puissance militaire.

S'ENTRAÎNER ET PLANIFIER : SE PRÉPARER AUX SCÉNARIOS DE CRISE

Les forces armées disposent de plusieurs moyens pour anticiper les cyberattaques majeures et s'y préparer. Parmi ceux-ci figurent les exercices simulant la compromission de systèmes militaires. Dès 1997, le ministère de la Défense des États-Unis (DoD) a mené un premier exercice de ce type, *Eligible Receiver 97*, au cours duquel une équipe rouge de la National Security Agency (NSA) a tenté d'infiltrer les réseaux du Commandement Indo-Pacifique des États-Unis.²⁹ Bien que les résultats se soient révélés catastrophiques pour les défenseurs, cet exercice a permis de mettre en évidence plusieurs cybervulnérabilités au sein du DoD et de démontrer différentes façons de renforcer les défenses. Depuis, ce type d'exercice est devenu beaucoup plus courant³⁰ et prend diverses formes.

Ces exercices sont souvent organisés chaque année. Ils peuvent faire intervenir plusieurs pays, réunir principalement des spécialistes du cyberspace et viser à simuler la défense active d'un réseau contre des acteurs hostiles fictifs. D'autres exercices mobilisent des forces conventionnelles afin de développer leur capacité à poursuivre leurs opérations dans un contexte de cyberattaque, dans le but de renforcer la résilience numérique des unités. La France, par exemple, organise de plus en plus d'exercices dans des « conditions de dégradation numérique » afin de mieux préparer ses unités à exécuter leurs missions même lorsque certaines technologies deviennent indisponibles ou inutilisables.³¹

Les exercices qui combinent des volets numériques et conventionnels, présentent un intérêt particulier, puisqu'ils réunissent des spécialistes du cyberspace et des militaires des forces conventionnelles et permettent aux unités de coordonner leurs opérations avec les activités de protection et de rétablissement des systèmes. Plusieurs auteurs qualifient cette synergie d'« assurance de la mission », concept selon lequel la capacité d'une organisation à accomplir sa mission est préservée grâce à des processus précis en cas de défaillance d'un système.³²

Ainsi, au début de 2024, l'armée française de l'Air et de l'Espace a simulé une cyberattaque, visant le système embarqué d'un avion d'avitaillement et de transport *Phénix*,³³ ainsi que son rétablissement, en réunissant des aviateurs et du personnel de cyberdéfense dans le cadre de l'exercice annuel majeur DEFNET.³⁴ Dans de tels exercices, il ne s'agit pas seulement d'entraîner un état-major à revenir à des technologies plus anciennes, comme dans 2034, mais aussi à s'exercer à déterminer avec assurance quels systèmes demeurent fiables et lesquels semblent compromis, ainsi qu'à évaluer la faisabilité et la rapidité de leur remise en service.³⁵ Autrement dit, ces exercices permettent de mettre en pratique les phases *observation* et *orientation* de la boucle OODA dans un contexte de cyberattaque.

Ces exercices permettent également aux forces armées de développer un autre élément essentiel de leur résilience : les plans de contingence. Des procédures préétablies peuvent préciser les mesures à prendre dans un scénario de crise, où certaines capacités technologiques sont dégradées. Dans le domaine aérien, l'United States Air Force teste actuellement des méthodes de navigation fondées sur l'analyse des anomalies du champ magnétique terrestre afin de permettre à ses pilotes de s'orienter même si leur système GPS est neutralisé.³⁶ Il ne s'agit là que de quelques exemples de procédures pouvant être élaborées et mises en œuvre en cas de cyberattaque. Toutefois, ces mesures doivent s'inscrire dans des plans de contingence complets, qui prévoient notamment une formation minimale permettant au personnel d'utiliser des méthodes de rechange ou des moyens « à faible composante technologique ». Lorsqu'ils sont bien conçus et largement diffusés, ces plans facilitent les phases *décision* et *action* de la boucle OODA. Ils offrent aux commandants des options éprouvées et potentiellement viables tout en veillant à ce que le personnel chargé de leur mise en œuvre dispose de toute l'information nécessaire.

S'ORGANISER : GARDER SES ALLIÉS À PROXIMITÉ

Un autre ensemble de mesures susceptibles d'accroître la résilience d'une force aérienne face aux cybermenaces concerne sa structure organisationnelle et administrative, plus particulièrement la place qu'y occupent les spécialistes de la cyberdéfense. À l'image d'un casse-tête, la cohérence d'une organisation militaire dépend non seulement de la présence de toutes les pièces, mais aussi de leur emplacement dans l'ensemble. Le défi consiste ici à organiser les « cyberpièces » d'une force aérienne de manière à lui permettre de réagir efficacement en situation de crise.

Comme dans bien des organisations, l'un des principaux défis tient au fait que les spécialistes et les unités de cyberdéfense demeurent souvent des éléments de soutien périphériques, relativement éloignés des centres décisionnels. Les commandants sur le terrain et les spécialistes de la cyberdéfense collaborent rarement et ne se *connaissent* pas vraiment sur le plan professionnel.

Pour compliquer davantage la situation, ces deux groupes peuvent avoir des parcours de formation différents ainsi que des façons distinctes d'aborder et de communiquer les problèmes opérationnels; ils ne se *comprennent* donc pas nécessairement bien. Comme le déplorait Michael Hayden, ancien général de l'United States Air Force et ancien directeur de la National Security Agency : « Après quelques phrases, l'exposé du spécialiste en cyberdéfense commence à évoquer vaguement *l'Homme de la pluie* pour la plupart des hauts dirigeants présents dans la salle. Après quelques phrases de plus, la plupart en sont convaincus ». ³⁷ Parler un langage commun et être capable de passer d'un langage à l'autre peut contribuer à combler les écarts entre la planification stratégique et la planification opérationnelle.

Cette situation est particulièrement problématique, parce que les cybermenaces peuvent profondément ébranler la confiance que les forces armées accordent à leurs technologies si les interactions complexes entre les composantes numériques et physiques sont mal comprises. Cette confiance repose notamment sur celle que les militaires des forces « conventionnelles » accordent aux spécialistes chargés de protéger leurs systèmes.³⁸ Il va de soi que la protection des systèmes ne relève pas uniquement des spécialistes de la cyberdéfense; les commandants et leurs états-majors ont eux aussi un rôle essentiel à jouer. Dans le milieu militaire, comme ailleurs, il est plus facile de faire confiance à une personne que l'on connaît et dont on a déjà pu apprécier les compétences. Il pourrait donc être opportun d'accorder une priorité organisationnelle à une intégration plus étroite des spécialistes de la cyberdéfense dans l'ensemble des opérations aériennes, tout en favorisant des relations de confiance réciproques permettant aux commandants de mieux comprendre leur dépendance envers le cyberspace. Les commandants devraient veiller à ce qu'eux-mêmes et leur état-major, y compris les spécialistes de la cyberdéfense, contribuent activement à la protection des systèmes. Le développement de cette confiance et de cette expertise revêt une importance particulière, puisque de nombreuses cyberattaques exploitent à la fois des vulnérabilités humaines et techniques.

Une intégration plus poussée pourrait notamment prendre la forme de mécanismes d'apprentissage réciproque, permettant au personnel de mieux comprendre le rôle des spécialistes de la cyberdéfense, leur façon de travailler et la contribution de leurs activités au fonctionnement stratégique, opérationnel et organisationnel d'une force aérienne. D'autres initiatives pourraient simplement consister à rapprocher physiquement les spécialistes de la cyberdéfense de certains secteurs d'opérations. Ainsi, dans le conflit qui se déroule actuellement en Ukraine, les forces ukrainiennes et russes auraient commencé à déployer des cyberéquipes près de la ligne de front afin d'améliorer leur coordination avec les unités avancées, une décision qui s'explique notamment par la nécessité d'assurer le fonctionnement efficace des drones.³⁹ En plus de raccourcir la chaîne de communication, le rapprochement des différentes équipes peut aider

les spécialistes de la cyberdéfense et le personnel des forces conventionnelles à mieux comprendre leurs besoins respectifs et à développer de meilleures synergies.⁴⁰ L'établissement de cette proximité et de cette connaissance mutuelle peut ainsi contribuer à accroître l'efficacité de la boucle OODA.

INSPIRER : CRÉER LES BONS INCITATIFS

L'isolement des spécialistes de la cyberdéfense ne découle pas uniquement de leur place dans l'organigramme; il s'enracine également dans des cultures organisationnelles qui influencent la façon dont la communauté militaire les perçoit. Qu'il s'agisse de l'armée de terre, de la marine ou de l'aviation, les organisations militaires entretiennent des normes, des valeurs et des traditions qu'elles perpétuent au fil du temps.⁴¹ Ces cultures ont une incidence directe sur le fonctionnement des organisations, mais elles peuvent aussi contribuer à certaines difficultés touchant la posture opérationnelle.

Dans un article, Rebecca Slayton montre que la persistance du culte de la « figure du guerrier » contribue directement à la marginalisation des spécialistes de la cyberdéfense au sein des forces armées des États-Unis.⁴² Le paradigme de la figure du guerrier renvoie à la valorisation institutionnelle de militaires, appartenant à certaines spécialités, notamment les forces spéciales ou les armes de combat, dont les fonctions sont jugées plus nobles parce qu'elles correspondent davantage à l'idéal martial de l'archétype du soldat.⁴³ Dans le domaine aérien, cette logique s'applique tout particulièrement à la figure du pilote, associée à une image d'autorité largement entretenue par la culture populaire.⁴⁴ Par conséquent, ces fonctions bénéficient souvent d'une plus grande crédibilité au sein de l'institution militaire, au détriment de spécialités perçues comme moins directement liées au combat, telles que la logistique ou les communications. Le culte de la figure du guerrier entraîne des conséquences concrètes. Par exemple, les fonctions considérées comme les plus prestigieuses donnent souvent un accès privilégié à certains postes ou commandements,⁴⁵ ce qui peut rendre certains parcours professionnels plus attrayants que d'autres.

Les spécialistes de la cyberdéfense, qui ne sont généralement pas perçus comme de « véritables guerriers », peuvent subir les effets négatifs de cette culture. Ces effets se traduisent notamment par une affectation plus fréquente à des tâches de moindre importance, par une progression plus lente dans la hiérarchie militaire et par un accès plus limité à certains commandements prestigieux.⁴⁶ Cette réalité pousse inévitablement de nombreux candidats potentiels vers d'autres spécialités militaires ou incite des spécialistes expérimentés à poursuivre leur carrière dans le secteur civil, où les perspectives d'emploi dans ce domaine sont nombreuses.⁴⁷ Aux États-Unis, l'United States Air Force est historiquement l'armée qui s'est montrée la plus accueillante envers les spécialistes de la cyberdéfense, sans doute en raison d'une culture institutionnelle de longue date fondée sur l'idée

que la victoire repose sur la supériorité technologique.⁴⁸ Même dans ce cas relativement favorable, le statut du cybercombattant demeure largement éclipsé par celui du pilote, qui continue d'incarner la figure idéale du guerrier. Dans une étude publiée en 2019, la RAND Corporation concluait que les pilotes de chasse, suivis des pilotes de bombardier, représentaient de loin les parcours les plus prometteurs pour accéder aux plus hauts échelons de l'United States Air Force.⁴⁹

Si une force aérienne veut relever efficacement les cybermenaces de demain, elle doit rehausser le statut des spécialistes de la cyberdéfense et mettre en place des incitatifs plus attrayants afin d'encourager le personnel à choisir cette spécialité. Cela peut passer par une réforme des mécanismes de recrutement, de formation et de maintien en poste existants, que Nicholas Romanow regroupe sous l'appellation de « triade de gestion des talents cybernétiques ».⁵⁰ Selon Romanow, même si les dirigeants militaires reconnaissent l'importance des cyberopérations, les effectifs demeurent insuffisants pour pourvoir les postes spécialisés, notamment en raison de la concurrence exercée par le secteur privé et d'une culture militaire peu attrayante pour la communauté cyber. Une façon de remédier à cette situation consiste à investir dans le développement de leaders solides en cyberdéfense tout en s'appuyant sur la culture de service propre aux forces armées.⁵¹ L'United States Air Force a récemment lancé un programme visant à accélérer l'octroi d'une commission d'officier aux spécialistes de la cyberdéfense.⁵² Dans le cadre d'une révision du parcours professionnel militaire traditionnel, ce programme vise notamment à mieux reconnaître les compétences liées au cyberspace par rapport à d'autres expériences militaires plus conventionnelles. Il cherche également à permettre aux spécialistes de la cyberdéfense d'accéder plus facilement à un grade et à une rémunération qui sont comparables à ceux offerts dans le secteur civil.

Comme l'ont montré des auteurs tels que Max Smeets, le développement des cybercapacités d'une force armée exige une combinaison judicieuse de compétences et de profils variés, qui dépasse largement le seul personnel technique.⁵³ Si le capital humain joue un rôle essentiel dans la confiance que les forces armées accordent à leurs technologies et s'il constitue une composante déterminante du bon déroulement de la boucle OODA, les spécialistes de la cyberdéfense doivent se sentir véritablement valorisés et pleinement associés à cet effort. Dans cette perspective, les programmes de formation et d'enseignement pourraient être élargis afin de s'adresser non seulement aux spécialistes de la cyberdéfense, mais également aux dirigeants et au personnel généraliste. En définitive, tous les militaires, et plus particulièrement ceux qui exercent des fonctions de commandement, doivent posséder les connaissances nécessaires pour comprendre dans quelle mesure leur mission dépend du cyberspace et pour jouer pleinement leur rôle dans la gestion des risques cybernétiques liés à cette mission.

CONCLUSION

Le maintien de la confiance envers les technologies numériques face aux cybermenaces doit aller de pair avec la confiance envers les personnes et leur capacité à travailler ensemble. Comme nous l'avons montré, la mise en pratique régulière de scénarios de cyberattaque et l'élaboration de plans de circonstance adaptés à ces situations contribuent à instaurer et à préserver cette confiance. Une autre approche consiste à agir sur les structures organisationnelles afin de mieux intégrer les spécialistes de la cyberdéfense et de favoriser une meilleure connaissance mutuelle ainsi que de plus grandes synergies avec les autres membres du personnel. L'évolution de la culture organisationnelle peut également jouer un rôle déterminant, en renforçant la confiance grâce à des incitatifs qui encouragent le personnel à choisir des fonctions liées au cyberspace.

Dans la récente mise à jour de la politique de défense, le ministère de la Défense nationale présente plusieurs projets, visant l'intégration de nouvelles technologies au sein du NORAD, notamment dans les domaines de l'information et des communications, en soulignant que les capacités de commandement et de contrôle doivent « être numérisées pour fonctionner à la vitesse de la machine ».⁵⁴ Dans cette perspective, le Canada a entrepris l'adoption et l'intégration de systèmes de commandement et de contrôle infonuagiques dans les installations canadiennes du NORAD.⁵⁵ Même si ces nouvelles technologies offrent des possibilités accrues en matière de circulation de l'information, de collecte de données et d'analyse pour améliorer la connaissance de la situation, elles doivent être considérées comme les composantes d'un système dont l'être humain demeure au cœur. Un autre élément mérite également une attention particulière : le NORAD repose sur un partenariat fondé sur l'interopérabilité et la confiance mutuelle. Par conséquent, la confiance envers les technologies de l'information revêt une importance fondamentale. De la même façon que le personnel des forces conventionnelles

doit avoir confiance dans la capacité des spécialistes de la cyberdéfense à protéger leurs systèmes, les deux partenaires doivent maintenir une confiance réciproque dans leur aptitude à préserver l'intégrité des réseaux liés au NORAD. Accorder une attention particulière à la dimension humaine de la cybersécurité pourrait également contribuer à résoudre les difficultés de recrutement et de maintien en poste auxquelles font face les Forces armées canadiennes (FAC).⁵⁶ Les FAC en général, et l'ARC en particulier, ont donc tout intérêt non seulement à demeurer un employeur attrayant pour les spécialistes de la cyberdéfense, mais aussi à tirer pleinement parti du potentiel d'innovation des personnes qui œuvrent déjà dans ce domaine.

Si les technologies de l'information constituent à la fois un élément essentiel et une source de vulnérabilité pour les forces armées modernes, les facteurs humains et organisationnels représentent des garanties indispensables au maintien de leurs capacités opérationnelles. Dans le présent article, nous avons cherché à situer les enjeux liés au cyberspace dans le contexte du domaine aérien. Les questions soulevées méritent l'attention des dirigeants de l'ARC, tant de façon autonome qu'en collaboration avec l'Armée canadienne et la Marine royale canadienne. La planification à long terme de la cybersécurité exige une approche, mobilisant l'ensemble des forces plutôt qu'une organisation en vase clos. Nous avons montré que divers outils existent déjà, ou sont en cours de développement, et qu'ils peuvent être mis à profit de manière concrète. À mesure que l'intégration des technologies émergentes devient une priorité pour la défense continentale et les autres partenariats de confiance,⁵⁷ les alliés devront veiller à préparer dès maintenant leurs capacités technologiques et humaines aux défis de demain afin de pouvoir assurer leur défense de manière concertée. Face au risque d'un techno-pessimisme excessif, les forces aériennes peuvent ainsi préserver la confiance envers leurs technologies numériques, en veillant à préserver l'intervention humaine.

Notes

- 1 Elliot Ackerman et amiral de l'USN James Stavridis (retraité), *2034*, Paris, Éditions Gallmeister, 2022.
- 2 Pour d'autres exemples de scénarios fictifs similaires, voir P. W. Singer et August Cole, *La flotte fantôme*, Gallimard, 2022. Pour un point de vue critique sur l'utilisation de la fiction spéculative, voir Col. Mark D. Jacobson, « The Uses and Limits of Speculative Fiction: Three Novels about a US-China War », *Journal of Indo-Pacific Affairs*, août 2023, 1-10.
- 3 Voir Bruce Schneier et Tara Wheeler, « Hacked drones and busted logistics are the cyber future of warfare », Brookings Institution, 4 juin 2021. Source d'origine : <https://www.brookings.edu/articles/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/>
- 4 Jonathan Beale, « Ukraine war: How old tech is helping Ukraine avoid detection », *BBC World*, 3 mai 2023. Source d'origine : <https://www.bbc.com/news/world-europe-65458263>
- 5 Pour une analyse de la distinction et de la convergence entre la cyberguerre et la guerre électronique, voir Ryan J. Worrell, *EW and Cyber Convergence: Beyond Information Warfare*, Air Force Fellows Program, 2020. Source d'origine : <https://apps.dtic.mil/sti/pdfs/AD112357.pdf>
- 6 Note terminologique : dans le contexte de l'aviation, les drones et les hélicoptères constituent tous deux des aéronefs. La classification des drones varie selon la doctrine nationale, qui peut notamment retenir les notions de système d'aéronef sans pilote, d'aéronef non habité ou d'aéronef télépilote. Chacune de ces catégories présente des caractéristiques et des vulnérabilités cybernétiques distinctes. Pour une analyse plus détaillée des différents types de classification des drones, voir Maj. Osman Aksu et al., *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, Joint Air Power Competence Centre, janvier 2021.
- 7 Scott Peterson, Payam Faramarzi, « Iran hijacked US drone, says Iranian engineer », *Christian Science Monitor*, 15 décembre 2011. Source d'origine : <https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer>
- 8 Nick Waters, « The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria », *Bellingcat*, 12 janvier 2018. Source d'origine : https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/
- 9 Dan Black et Gabby Roncone, « The GRU's Disruptive Playbook », *Mandiant Blog*, 12 juillet 2023 [mise à jour : 3 avril 2024]. Source d'origine : <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>
- 10 Mauro Gilli et Niklas Masuhr, « Drones enhance defences in the Ukraine war », *Binding Hook*, 10 janvier 2024. Source d'origine : <https://bindinghook.com/articles-hooked-on-trends/drones-enhance-defences-in-the-ukraine-war/>

- 11 Voir, par exemple, dans Sam Skove, « Army puts drones front and center in unfunded wishlist », *Defense One*, 22 mars 2024. Source d'origine : <https://www.defenseone.com/technology/2024/03/army-puts-drones-front-and-center-newly-obtained-budget-docs/395182/>. Sam Skove, « Army announces plan to help spread commercial drones across infantry units », *Defense One*, 27 mars 2024. Source d'origine : <https://www.defenseone.com/threats/2024/03/army-announces-plan-help-spread-commercial-drones-across-infantry-units/395260/>. Maxine Baen, « Army tests commercial satellite internet in pilot program », *U.S. Army*, 28 février 2022. Source d'origine : https://www.army.mil/article/254316/army_tests_commercial_satellite_internet_in_pilot_program
- 12 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare*. Oxford University Press, 2022, 97-99.
- 13 Pour un aperçu du paradigme du techno-solutionnisme militaire, voir Jon R. Lindsay, « The Technology Theory of Victory », dans *Information Technology and Military Power*. Cornell University Press, 2020, 13-31.
- 14 Christopher Coker, *Future War*, Polity Press, 2015, 171-172.
- 15 Voir Martin C. Libicki, « Cyberwar as a Confidence Game », *Strategic Studies Quarterly* vol. 5, n° 1, 2011, 132-147.
- 16 Pour un aperçu des travaux de John Boyd, voir Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War*, Little, Brown and Company, 2002.
- 17 Bien que la boucle OODA tire son origine de la puissance aérienne, ce concept a pris une importance croissante dans l'ensemble des domaines conventionnels de la guerre. Par exemple, voir Brian R. Price, « Colonel John Boyd's Thoughts on Disruption: A Useful Effects Spiral from Uncertainty to Chaos », *Journal of Advanced Military Studies*, vol. 14, n° 1, 2023, 98-117.
- 18 Pascal Venesson, « Fighting, Fast and Slow? Speed and Western Ways of War », dans Sten Rynning, Olivier Schmitt, Amelie Theussen, *War Time: Temporality and the Decline of Western Military Power*, Brookings Institution Press, 2021, 211-229.
- 19 Certes, la boucle OODA ne repose pas uniquement sur la rapidité. Comme le soutiennent notamment Luft et Kollars, elle repose également sur le rythme et le choix du moment. Voir Alastair Luft, « The OODA Loop and the Half-Beat », *The Strategy Bridge*, 17 mars 2020, et Nina A. Kollars, « War at Information Speed: Multi-Domain Warfighting Visions », dans Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 230-252. Source d'origine : <https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat>
- 20 Joseph Henrotin et Stéphane Taillat, « Military Operations: What If Digital Technologies Fail on the Battlefield? », dans Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 275-291.
- 21 Daniel Moore, *op. cit.*, 186-200.
- 22 Shah Zahid Khan, Mujahid Mohsin, et Waseem Iqbal, « On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions », *PeerJ Computer Science*, n° 7, 2021, e507.
- 23 Eduard Kovacs, « BAE Releases New Cybersecurity System for F-16 Fighter Aircraft », *Security Week*, 14 octobre 2022. Source d'origine : <https://www.securityweek.com/bae-releases-new-cybersecurity-system-f-16-fighter-aircraft/>
- 24 Kim Hartmann et Keir Giles, « UAV Exploitation: A New Domain for Cyber Power », 8th International Conference on Cyber Conflict: Cyber Power, Centre d'excellence OTAN pour la cyberdéfense en coopération, 2016, 205-221.
- 25 Julian E. Barnes, U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say », *The New York Times*, 28 août 2019. Source d'origine : <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>
- 26 Le cadre de cybersécurité du National Institute of Standards and Technology (NIST) des États-Unis sert généralement à intervenir en cas de cyberincident. Ce cadre comprend les fonctions de déterminer, protéger, détecter, répondre et rétablir. Les liens entre ce cadre, une cybersécurité axée sur l'humain et la culture organisationnelle feront l'objet d'une analyse approfondie dans des travaux à paraître de Csenkey et Furlong.
- 27 Jon R. Lindsay, *op. cit.*, 32-70.
- 28 Jon Lindsay, *op. cit.*
- 29 Fred Kaplan, *Dark territory: The secret history of cyber war*, New York, Simon & Schuster, 2016, 68-71.
- 30 Pour une histoire plus approfondie des débuts des cyberconflits, notamment de l'exercice ELIGIBLE RECEIVER et d'autres événements, voir Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013.
- 31 Comité d'éthique de la défense, *Avis sur l'environnement numérique des combattants*, ministère des Armées, 13 avril 2022. Source d'origine : https://www.defense.gouv.fr/sites/default/files/tronc_commun/20220413_Comit%C3%A9_d%C3%A9thique_de_la_d%C3%A9fense_-_Avis_sur_l%27environnement_num%C3%A9rique_des_combattants.pdf
- 32 Brad Bigelow, « Mission Assurance: Shifting the Focus of Cyber Defence », 2017 9th International Conference on Cyber Conflict (CyCon), CCD COE de l'OTAN, 2017, p. 1-12, <https://doi.org/10.23919/CYCON.2017.8240327>.
- 33 Airbus Defence and Space A330-200 Phénix Multi-Role Tanker Transport.
- 34 Commandement de la Cyberdéfense, *DEFNET 2024 : une cyberattaque simulée sur le plan de vol du Phénix*, ministère des Armées, 29 mars 2024. Source d'origine : <https://www.defense.gouv.fr/comcyber/actualites/defnet-2024-cyberattaque-simulee-plan-vol-du-phenix>
- 35 Daniel T. Sullivan, Edward J.M. Colbert, Blaine E. Hoffman et Alexander Kott, « Best practices for designing and conducting cyber-physical-system war games », *Journal of Information Warfare*, vol. 17, n° 3, 2018, 92-105.
- 36 David Roza, « C-17 Tests Magnetic Navigation System That Works When GPS Doesn't », *Air & Space Forces Magazine*, 7 juin 2023. Source d'origine : <https://www.airandspaceforces.com/air-force-magnetic-navigation-gps/>
- 37 Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, Penguin Press, 2016, 147.
- 38 Diane Henshel, *et al.*, « Trust as a human factor in holistic cyber security risk assessment », *Procedia Manufacturing*, vol. 3, 2015, 1117-1124.
- 39 Gordon Corera, « Ukraine war: Cyber-teams fight a high-tech war on front lines », *BBC*, 5 septembre 2023. Source d'origine : <https://www.bbc.com/news/world-europe-66686584>
- 40 *Ibid.*
- 41 Joseph Soeters, « Organizational Cultures in the Military », *Handbook of the Sociology of the Military*, Springer, 2018, 251-272.
- 42 Rebecca Slayton, « What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967-2018 », *Texas National Security Review*, vol. 4, n° 1, 2021.
- 43 *Ibid.*
- 44 Voir Michael Wayne Hankins, *The Cult of the Lightweight Fighter: Culture and Technology in the U.S. Air Force, 1964-1991*, dissertation doctorale, Kansas State University, 2018.
- 45 Pour une analyse de cette dynamique dans le domaine aérien, voir Michael R. Worden, *Rise of the fighter generals: the problem of air force leadership, 1945-1982*, Air University Press, 1998.
- 46 Josh Lospinoso, « Fish Out of Water: How the Military Is an Impossible Place for Hackers, and What to Do About It », *War on the Rocks*, 12 juillet 2018. Source d'origine : <https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/>
- 47 Lee Lunn, « Cyber Operator: Are you sure you want to do that? », *The Blue Knight Review*, 2021. Source d'origine : <https://www.cmrj-rmcsj.forces.gc.ca/cb-bk/art-art/2021/art-art-2021-7-eng.asp>
- 48 Sarah P. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, dissertation doctorale, Harvard University, Graduate School of Arts & Sciences, 2019.
- 49 S. Rebecca Zimmerman, Kimberly Jackson, Natasha Lander, Colin Roberts, Dan Madden et Rebeca Orrie, *Movement and Maneuver: Culture and the Competition for Influence Among the U.S. Military Services*, RAND Corporation, 25 février 2019.
- 50 Nicholas Romanow, « Leadership, Culture, and the Military Cyber Workforce », *War on the Rocks*, 11 avril 2024. Source d'origine : <https://warontherocks.com/2024/04/leadership-culture-and-the-military-cyber-workforce/>
- 51 *Ibid.*
- 52 Air Force Recruiting Public Affairs, « Cyber Direct Commissioning Program enhancement to onboard future cyber officers », US Air Force, 19 avril 2023. Source d'origine : <https://www.af.mil/News/Article-Display/Article/3368057/cyber-direct-commissioning-program-enhancement-to-onboard-future-cyber-officers/>
- 53 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, Oxford University Press, 2022, 75-79.
- 54 Ministère de la Défense nationale, *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*, 9 avril 2024. Source d'origine : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/nord-fort-libre-2024.html>
- 55 Maxime Cliché, *Canadian Air Defence Sector introduces new cloud-based command-and-control system*, Commandement de la défense aérospatiale de l'Amérique du Nord, 26 janvier 2024. Source d'origine : <https://www.norad.mil/Newsroom/Article/3657967/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-syst/>
- 56 Aaron D'Andrea, « Canada's military facing 'death spiral' on recruitment, minister says », *Global News*, 7 mars 2024. Source d'origine : <https://globalnews.ca/news/10341588/canadian-forces-recruitment-death-spiral/>
- 57 Kristen Csenkey et Nina Bindel, « Post-Quantum Cryptographic Assemblages and the Governance of the Quantum Threat », *Journal of Cybersecurity* vol. 9, n° 1, 2023, 1-14, <https://doi.org/10.1093/cybssec/tyad001>