Ouvrir les yeux

La pédagogie de la cyber puissance et le plaidoyer en faveur d'une pensée stratégique

Col Richard J. Bailey Jr., PhD*

Les mesures prises et les mesures à prendre sont, bien évidemment, des facteurs majeurs dans la pensée des stratèges, mais ce sont des éléments qu'il convient d'élaborer et de manipuler, et non des leçons strictes entraînant des instructions à suivre.

—Everett Carl Dolman
Pure Strategy (2005)

La pédagogie de la cyber puissance a un aspect énigmatique. Bien que le cyber espace et les technologies associées existent depuis plusieurs décennies, notre *réflexion* à ce sujet demande encore à mûrir. Toutefois, compte tenu du rôle majeur joué par la cyber puissance dans les récents conflits internationaux, la nécessité d'intégrer la technologie dans l'élaboration d'une stratégie militaire présente un défi singulier. Comment *utiliser* la cyber puissance alors que nous n'avons pas fini de la *comprendre* ? Et dans le même ordre d'idée, comment *enseigner* la cyber puissance, en particulier aux professionnels amenés à l'inclure dans la prise de décision stratégique, en dépit de cette insuffisance de connaissance ? Pour résoudre cette énigme, il est indispensable de commencer par examiner les défis que présente l'enseignement de la stratégie, indépendamment des particularités de la cyber puissance. Ensuite, l'étude de l'environne-

*L'auteur est professeur associé en études stratégiques et de sécurité à la School of Advanced Air and Space Studies, Maxwell AFB, Alabama. Il a obtenu une licence en ingénierie à l'United States Air Force Academy en 1992, un master en relations internationales à Washington University de St. Louis en 1997 et un doctorat en sciences politiques à Georgetown University en 2006. Ses recherches portent notamment sur la stratégie militaire, les relations entre la société civile et l'armée, le comportement socio-politique américain et la cyber puissance. Parmi ses derniers travaux figurent : *Strategy: Context and Adaptation from Archidamus to Airpower*, Annapolis, Maryland : Naval Institute Press, 2016 (coéditeur, participation à l'ouvrage collectif) ; *The Baltic Security Puzzle*, Lanham, Maryland : Rowman and Littlefield, 2015 (auteur d'un chapitre) ; « Fighting More Fires with Less Water: Phase Zero and Modified Operational Design », *Joint Force Quarterly* 77 (2e trimestre 2015, pp. 101–108 (coauteur) et « You Can't Take the Human Factor Out of Warfare », Opinion-Editorial, *US News and World Report*, 17 octobre 2014. Le colonel Bailey prendra sa retraite en fin d'année et exercera la fonction de président du Northern New Mexico College.

Ce texte a été présenté sous forme d'article lors de l'*American Political Science Association Teaching and Learning Conference*, à Washington, DC, en janvier 2015 et de l'*International Studies Association National Conference*, à la Nouvelle Orléans, en février 2015. Il sera repris sous forme de chapitre dans un livre à paraître consacré à la cyber stratégie que prévoit de publier les Presses universitaires de Copenhague.

ment du cyberespace révélera les représentations et préjugés étymologiques qui y sont associés, pour éventuellement éclairer la manière dont la société moderne approche les nouvelles technologies. Enfin, l'analyse des incertitudes inhérentes au cyberespace et cyber puissance mettra en lumière les principaux problèmes liés à l'élaboration et à la formulation d'une stratégie dans cet espace virtuel.

Les défis liés à la définition et à l'enseignement de la stratégie

La School of Advanced Air and Space Studies est souvent présentée comme la meilleure école de stratégie du département de la Défense des États-Unis. Son rigoureux programme d'études supérieures d'un an prépare les étudiants à l'éventail vertigineux de problèmes complexes qu'ils devront affronter en tant qu'officiers supérieurs de l'armée. Paradoxalement, si vous demandez aux 14 docteurs dans le corps professoral de définir la *stratégie*, vous obtiendrez probablement 14 réponses légèrement (voire sensiblement) différentes. L'école tire sa réputation de sa capacité à encourager l'ouverture d'esprit, « à créer des modes de pensée et des méthodes d'investigation » qui seront utiles aux diplômés dans leurs futures missions[1]. Autrement dit, comme le rappelle la citation du professeur Dolman en exergue du présent article, il n'y a pas de réponses précises concernant la stratégie. Par conséquent, la multitude de définitions variées élargit l'expérience éducative. C'est la raison pour laquelle nous tenons à ce que nos étudiants définissent leurs propres perceptions de ce qu'est la stratégie dans le cadre de leur cursus. Au sein de la faculté de la School of Advanced Air and Space Studies, chacun d'entre nous (comme vous l'aurez sans doute deviné) considère que sa propre définition est plus utile que celles de ses collègues. Cette rivalité amicale est capitale car elle nous permet non seulement de nous stimuler mutuellement sur le plan intellectuel, mais aussi d'enrichir l'expérience éducative de nos étudiants de haut niveau. La définition de la stratégie que je propose dans cet article est utile pour stimuler la pensée stratégique au sujet de la cyberpuissance, d'autant plus qu'il nous faut aborder cette entreprise avec humilité, ouverture d'esprit et une vive curiosité intellectuelle. Accordons-nous donc pour définir la *stratégie* comme *un effort artistique continu visant à optimiser un avantage concurrentiel grâce à une meilleure compréhension de son propre environnement et une adaptation à l'incertitude*. Plusieurs termes employés dans cette définition méritent d'être explicités.

Continu : La stratégie n'est pas une entreprise limitée dans le temps. Si nous suivons la recommandation de Lawrence Freedman et pensons « la stratégie comme une histoire racontée au futur », alors son application se poursuit nécessairement à l'infini[2]. Dans le domaine de la planification militaire, des termes tels que échéance ou *point de terminaison* font référence au caractère définitif d'une entreprise opérationnelle. Ils sont importants et utiles pour encadrer un effort fini et orienter en conséquence l'utilisation des ressources limitées. La stratégie est toutefois de nature différente car elle est un exercice intellectuel itératif. En effet, si les buts et objectifs sont essentiels aux activités opérationnelles, la stratégie cherche à déterminer la manière dont les mesures prises façonnent la situation globale. Un stratège doit, par exemple, se demander comment la réalisation efficace d'une

tâche particulière modifie le comportement des autres acteurs du scénario. Est-elle susceptible de modifier le calcul décisionnel d'un opposant ? Cette mesure renforce-t-elle ou affaiblit-elle certaines contraintes existantes ? La réalisation d'un objectif ouvre-t-elle de nouvelles possibilités pour des mesures indirectement liées ? Et ainsi de suite. La stratégie doit être considérée comme un processus continu afin que la rigueur intellectuelle s'adapte pour répondre aux nouveaux besoins à mesure que l'environnement évolue.

Artistique : On doit au stratège prussien Carl von Clausewitz la fameuse citation suivante : « Dans la stratégie tout est très simple, mais la chose la plus simple est difficile[3] ». Les complexités inhérentes à notre propre environnement et les problèmes liés à l'adaptation à l'incertitude exigent bien plus que la simple application de principes scientifiques. Selon B. H. Liddell Hart, « Quelle que soit l'étendue de nos connaissances de la guerre, c'est de son art que dépendra son application[4] ». En d'autres termes, il n'y a pour le stratège ni information parfaite, ni compréhension parfaite. Par conséquent, les étudiants, et les professionnels, en stratégie doivent faire preuve d'un esprit innovant et adopter une approche créative dans la résolution des problèmes pour tirer le meilleur parti d'une entreprise.

Optimiser un avantage concurrentiel : La stratégie implique généralement un opposant quelconque. Dans le secteur militaire, l'opposant peut être un ou plusieurs ennemis déclarés. Dans le secteur commercial, il peut prendre la forme d'un ou plusieurs concurrents souhaitant augmenter leur part de marché ou les forces du marché elles-mêmes. Dans tous les cas, la stratégie représente une aide dans un conflit quelconque. Dans la préface de son ouvrage fondamental *Strategy: The Logic of War and Peace*, Edward Luttwak déclare : « Étant donné que la vision d'une stratégie se dégage de l'ombre de lectures, de problèmes examinés et d'opérations guerrières vécues, j'ai constaté que son contenu n'avait rien de la matière prosaïque des platitudes, mais relevait au contraire du paradoxe, de l'ironie et de la contradiction[5] ».

Luttwak emploie le terme *paradoxe* en raison de la présence d'un opposant intelligent dans les initiatives stratégiques. Si la stratégie est centrée sur ses propres ressources, objectifs et contraintes, elle omet entièrement les effets que peut avoir un opposant doté d'une vision stratégique. Un tel ennemi affecte non seulement la dynamique de l'environnement mais il renforce également l'incertitude qui l'anime[6].

Environnement et incertitude : En définitive, la mission première du stratège consiste à mener une réflexion approfondie sur son environnement et à se préparer à la probabilité, ou à l'éventualité, que les choses ne se déroulent pas exactement comme prévu. La complexité de l'environnement découle de sa nature dynamique et de la perception imparfaite que nous en avons. Nos méprises sont le fruit de nos connaissances incomplètes, de nos propres préjugés ou de nos représentations inexactes. De plus, les stratèges ont souvent tendance à penser qu'avoir accès à davantage d'informations permet de maîtriser les forces de l'incertitude. En réalité, c'est souvent l'inverse qui se produit. Dans le domaine de la cyber sécurité, notamment, le défi ne consiste pas tant à obtenir *suffisamment* d'informations qu'à identifier l'information *utile* dans un réservoir apparemment inépuisable.

Le reste de l'article s'appuiera sur ces deux aspects, à savoir l'environnement et l'incertitude, pour tenter de fournir un cadre à l'enseignement de la cyber stratégie.

Enseigner la stratégie suppose, en définitive, d'inciter les étudiants à élargir leurs perspectives et à comprendre leurs propres habitudes intellectuelles. On touche ici à un autre paradoxe dans l'apprentissage de la stratégie : c'est en étant conscients de ce qu'ils ne *savent pas* et, de manière tout aussi importante, de ce qu'ils *ne peuvent pas savoir* que les étudiants tireront le plus grand bénéfice de leur formation à la stratégie. Imagination, créativité, souplesse intellectuelle et haute réactivité sont les instruments qui les guideront dans leur étude de la stratégie et dans ses futures applications.

Dans le cyberespace, il peut paraître impossible de déconstruire l'environnement et de s'adapter à l'incertitude. Toutefois, si les professionnels sont tenus d'intégrer la cyber puissance à une vision stratégique plus vaste du monde, il leur faut explorer ces deux axes de réflexion. Ce sont ces deux aspects que nous nous proposons d'examiner à présent.

Comprendre l'environnement du cyberespace

> *Cyberespace. Une hallucination consensuelle vécue au quotidien par des milliards d'opérateurs légitimes, dans chaque pays, par des enfants à qui l'on apprend les concepts mathématiques… Une représentation graphique de données extraites de chaque ordinateur du système humain. Une complexité inconcevable. Des lignes lumineuses rangées dans les caractères de l'esprit, des clusters et des constellations de données. Comme les lumières d'une ville, qui s'estompent…*
>
> — William Gibson

Dans son roman de science fiction *Neuromancien*, publié en 1984, William Gibson a vulgarisé le terme *cyberespace* qu'il avait introduit dans sa nouvelle intitulée « *Gravé sur chrome* » deux ans auparavant. À l'époque, il n'imaginait sûrement pas que le terme qu'il utilisait pour décrire l'environnement virtuel deviendrait le nom courant de tout ce que nous associons aujourd'hui à l'univers numérique[7]. Trente ans plus tard, l'omniprésence des réseaux d'ordinateurs et leur impact sur la vie humaine demeurent énigmatiques. Si la technologie affecte sans conteste pratiquement tous les aspects de nos vies, son application dans les rapports de force et la stratégie globale reste inexpliquée. Aucun rapport de force n'est jamais *entièrement* expliqué, mais nos premiers pas dans l'exploration du cyberespace nous laissent aussi pantois que la chienne Laïka après le décollage de la fusée. Autrement dit, nous sommes conscients que notre environnement a changé mais ne comprenons probablement pas encore l'ampleur de ces mutations, pourquoi et comment elles se sont produites et où elles nous mèneront. Pour replacer la cyber puissance dans son contexte, il convient de se pencher sur l'étymologie du cyberespace afin de saisir les préjugés et représentations inhérents à la terminologie que nous utilisons et examiner les difficultés que nous rencontrons quand il s'agit de définir le secteur cybernétique.

L'étymologie du cyberespace

Le principal argument soutenu dans la présente section affirme que la terminologie utilisée pour décrire les éléments du cyberespace affecte notre manière de le *penser*. Cette hypothèse a eu de profondes répercussions sur le développement (ou son absence) d'une stratégie cohérente pour son utilisation et a incroyablement compliqué l'enseignement de la cyber stratégie. Pour développer cette argumentation, nous nous proposons d'étudier la cyber terminologie afin de découvrir la manière dont sa sémantique particulière génère des préjugés. Si ces préjugés créent des schémas de compréhension, ils sont susceptibles de limiter notre manière de penser la technologie.

Comme l'a justement fait remarquer le blogueur Mark Forsyth, « les nouvelles choses ont besoin de nouveaux mots, mais on leur en donne habituellement des anciens[8] ». Penchons-nous tout d'abord sur le terme *cyberespace*. Avant même que William Gibson ne vulgarise ce mot, universitaires et professionnels en avaient publié une large palette de définitions, chacune accompagnée de ses propres justifications. Dans les années 1940, Norbert Wiener, professeur de mathématiques au Massachusetts Institute of Technology, plaidait en faveur d'une utilisation accrue de l'analyse statistique pour expliquer les phénomènes de société. Il considérait l'interaction entre les systèmes (biologique, mécanique et sociétal) comme des formes de *communication* dotées de mécanismes de feedback et, plus important encore, de qualités prédictives. Avec ses collègues, il a ainsi fondé un domaine de recherche transdisciplinaire qu'il a baptisé la *cybernétique*. La racine *cyber* est issue du grec *kybernan*, un terme signifiant *gouverner* ou *diriger*[9]. Pour le professeur Wiener, l'étymologie du terme cybernétique évoque une direction du désordre vers l'ordre : « Guidés par le feedback, les organismes biologiques, mécaniques ou sociaux créent des poches d'ordre, des signaux forts dans un océan entropique de bruit[10] ». Au milieu du vingtième siècle, de nombreux stratèges militaires voyaient dans la cybernétique le moyen d'acquérir suffisamment de connaissances sur la guerre grâce aux analyses de feedback ou rétroaction, afin de réduire l'incertitude dans les conflits. Pendant plusieurs décennies, ils ont remis en cause la célèbre formule de Clausewitz soutenant que « la guerre est le domaine du hasard[11] ». C'est ainsi qu'est né le concept de *Révolution dans les affaires militaires* (RMA), selon lequel l'information correctement traitée pouvait modifier fondamentalement l'essence de la guerre. La littérature consacrée à la RMA fait sienne la philosophie vieille de 2500 ans du penseur chinois Sun Tzu, qui affirme : « Celui qui connaît son ennemi et se connaît lui-même mènera cent combats sans risque[12] ». Les critiques formulées à l'égaré de la RMA soutiennent que la confiance excessive des cybernéticiens dans l'information, considérée comme une panacée, ignorait l'omniprésence de l'incertitude dans les combats, ce qui a notamment conduit au « manque d'efficacité et à l'échec spectaculaires » de la stratégie lors de la guerre du Vietnam[13]. Les statistiques quotidiennes du nombre de morts et des sorties n'ont pas permis de saisir la détermination de la population nord-vietnamienne, ni l'érosion du soutien de l'opinion publique américaine.

Comment la sémantique affecte-t-elle donc en définitive notre conceptualisation de la cyber stratégie ? En quelques mots, l'emploi de la racine *cyber* dans *cyberespace* et *cyber*

puissance véhicule depuis toujours l'idée d'un mécanisme visant à créer une forme d'ordre à partir du chaos. L'expérience montre cependant que l'incertitude est indissociable de la guerre ; par conséquent, si nous utilisons ces termes, nous devons être conscients de leurs limites et veiller à les replacer dans la perspective adéquate. La cyber puissance est, par nature, alimentée par l'information. Toutefois, même l'accès le plus performant à l'information ne peut parvenir à dissiper le brouillard de la guerre décrit par Clausewitz. Les étudiants en stratégie doivent accepter cette éventualité et se préparer aux défis intellectuels qu'elle recèle.

Examinons à présent les connotations de la seconde partie du terme *cyberespace*. Ce mot évoque, au tout ou moins suggère, l'image d'un *espace* physique. Ce terme est donc une simple métaphore. Toutefois, si les stratèges pensent le cyberespace uniquement en termes physiques, ils risquent de négliger le potentiel que recèle la technologie et de passer à côté de ses aspects immatériels uniques. La mention du cyberespace en lien avec les domaines physiques contribue à alimenter cette tendance. L'US Air Force a, par exemple, précisé sa mission en 2005, mobilisant ses pilotes pour « voler, combattre et vaincre... dans les airs, dans l'espace et dans le cyberespace[14] ». Quand le cyberespace est associé à l'air et à l'espace comme théâtre d'opérations militaires, l'esprit opère naturellement une analogie avec une entité géo-spatiale imaginaire qu'il place sur un pied d'égalité avec les domaines physiques[15].

Même si nous tentons d'imaginer le cyberespace sur le modèle d'un espace tridimensionnel, il est impossible d'identifier ses frontières. En réalité, le seul espace physique présent dans le cyberespace est l'architecture fournissant l'infrastructure nécessaire à son déploiement. Le cyberespace est en fait une métaphore qui nous aide à visualiser un domaine dans lequel l'information « voyage » via des systèmes informatiques en réseau. L'une des définitions les plus complètes du cyberespace a été formulée par Daniel Kuehl, qui le décrit comme « un domaine caractérisé par l'utilisation de composants électroniques et du spectre électromagnétique pour stocker, modifier et échanger des informations via des systèmes d'information en réseau et des infrastructures physiques[16] ». Martin Libicki est l'un des premiers à avoir identifié trois couches dans le cyberespace : la couche physique (routeurs, câbles, commutateurs, etc.), la couche syntaxique (les systèmes d'information ainsi que les protocoles de formatage et de distribution de l'information) et la couche sémantique (la connexion entre l'information transmise, la réception humaine et la compréhension de l'information)[17]. Pratiquement toutes les études initiales consacrées au cyberespace soulignent qu'il s'agit du seul domaine militaire artificiel. Le concept de base suppose que, contrairement aux autres domaines militaires (terre, mer, air et espace), la présence d'objets d'origine humaine est indispensable à l'existence du cyberespace. Si l'humanité crée des objets pour traverser et optimiser l'utilisation des domaines physiques, le cyberespace est le seul domaine qui requiert notre intervention pour être *créé*. Cependant, même si nous admettons cette spécificité, quelles en sont les implications stratégiques ? En définitive, elles sont inexistantes ou sans incidence. Le seul lien possible existe soit dans un scénario dans lequel quelqu'un ou quelque chose détruit l'ensemble de l'ar-

chitecture internet mondiale ou lors d'un cataclysme tel qu'une impulsion électromagnétique globale.

Le cyberespace ne disposant pas de frontières physiques, il n'existe aucune règle simple régissant la répartition des responsabilités et du contrôle. Par conséquent, les stratèges militaires ont été contraints de s'éloigner des postulats traditionnels concernant l'application de la force militaire dans un environnement physique. Examinons, par exemple, le facteur distance. Dans un affrontement physique, la distance d'une cible ennemie revêt une importance essentielle pour une opération terrestre ou maritime, et une importance relative pour une attaque aérienne, mais elle est quasi négligeable dans le cyberespace. Un pirate habile disposant de connaissances approfondies des vulnérabilités informatiques de son ennemi peut affecter son réseau, voire ses biens physiques. Quel que soit le lieu où se trouve la cible, le pirate peut l'attaquer de n'importe quel endroit de la planète en quelques fractions de seconde. Même les cibles spatiales, comme les satellites, sont vulnérables.

La signification des mots évolue et se transforme au fil du temps. Prenez le terme *computer*. Ce mot est utilisé dans la langue anglaise depuis le XVII^{e} siècle, mais sa signification s'est radicalement transformée. Avant le XX^{e} siècle, il désignait une personne traitant les chiffres à la main. Avec l'avènement du microprocesseur et la popularité croissante des ordinateurs personnels dans les années 1970 et 1980, la société a commencé à utiliser le terme *computer* pour désigner le mécanisme plutôt que la personne réalisant l'opération : « À ce moment, les ordinateurs, comme les cyborgs de la science-fiction, ont achevé leur transformation de l'humain à la machine[18] ».

Pourquoi la terminologie est-elle importante pour les étudiants en stratégie ? Arrêtons-nous sur la double signification des mots et des phrases. D'après Kate Kearns, professeure en linguistique, une phrase « est composée d'une *signification lexicale*, qui est la signification de chaque mot, et d'une *signification structurelle*, qui est la signification de la manière dont sont combinés les mots[19] » (souligné dans l'original). La signification lexicale peut façonner notre manière d'appréhender un sujet aussi bien sur le plan intellectuel qu'émotionnel. Les lobbyistes politiques, particulièrement doués dans ce domaine, utilisent le langage pour influencer le débat national. Prenez l'exemple du débat sur l'avortement aux États-Unis. Les lobbyistes (et les politiques) opposés aux avortements dits *tardifs*, c'est-à-dire qui ont lieu au deuxième ou troisième trimestre de la grossesse, sont parvenus à les renommer avortement *par naissance partielle* sur la scène politique. Ce dernier terme est bien plus évocateur et suggère l'image de l'interruption d'une *vie* humaine. Le langage a le pouvoir d'encadrer notre *réflexion* ou nos *sentiments* à propos d'un sujet, simplement à partir de la signification lexicale des mots utilisés pour le décrire.

Il est utile de transposer cette interprétation aux termes utilisés dans le cyberespace. Étant donné que la signification lexicale des mots employés pour décrire les éléments du cyberespace est ancrée dans les représentations et perceptions d'objets physiques, leur signification structurale s'inscrit dans des représentations archaïques :

> Une vision du langage largement répandue depuis longtemps considère que la signifiance du langage correspond à son « à-propos » (*aboutness*). Les mots et expressions symbolisent et décrivent, et sont donc à propos de, choses et phénomènes du monde qui nous entoure, ce qui nous permet d'utiliser le langage pour transmettre des informations sur la réalité. Par conséquent, la signifiance du langage réside dans les connexions établies entre les mots et expressions et les éléments de la réalité[20].

Comment les stratèges en herbe peuvent-ils faire face à ce dilemme ? Par ailleurs, comment peut-on enseigner la cyber stratégie de manière à s'opposer à cette tendance ? Dans l'idéal, il faudrait inventer pour le cyberespace et ses éléments de nouveaux termes évoquant un cadre intellectuel élargi. Malheureusement, cet effort serait vain. Les mots qui décrivent le cyberespace existent depuis plusieurs décennies et il est peu probable de parvenir à modifier le langage aujourd'hui. La seule solution consiste à comprendre les limites de ces termes et à lutter contre les préjugés qu'ils génèrent inconsciemment. Quoi qu'il en soit, l'enseignement de la cyber stratégie doit commencer par la compréhension du cyber environnement, et une grosse partie de cet environnement est ancré dans le langage que nous utilisons pour le décrire.

Comment appréhendons-nous la nouvelle technologie ? Polarisation et analogies.

La connaissance des préjugés et représentations issus de la terminologie du cyberespace révèle en partie notre compréhension de son environnement culturel mais ne nous offre pas une vision intégrale. Pour compléter cette approche, il convient de prendre en compte l'aspect sociologique. Autrement dit, en étudiant la manière dont la société s'adapte au cyber environnement avec le temps, nous pourrions parvenir à mieux le comprendre. L'application de cette analyse révèle deux aspects majeurs : une polarisation de la littérature et l'emploi d'analogies avec les progrès technologiques du passé.

Avant d'explorer le phénomène de la polarisation dans la littérature, il convient de se demander pourquoi la société a tendance à invoquer des positions extrêmes quand elle est confrontée à des concepts nouveaux. Un scénario inspiré d'Alexander Wendt peut nous éclairer ici[21]. Imaginez que vous allumiez la télévision sur un flash d'information en direct relatant l'atterrissage d'un vaisseau extraterrestre au cœur de Central Park, à New York. Sans autres informations, quelles seraient vos premières pensées ? Qu'évoque pour vous l'image du vaisseau spatial ? Pour nous replacer dans un contexte cinématographique, vous pouvez envisager la situation sous deux angles extrêmes. Vous imaginez peut-être les visiteurs amicaux, bienveillants et attentionnés de *E. T. l'extra-terrestre* ou la scène finale de *Rencontres du troisième type*. Ou bien vous vous représentez les agresseurs sinistres, inquiétants et avides de *La Guerre des mondes* ou *Independence Day*. Rares sont ceux qui imaginent un scénario intermédiaire. Pour simplifier, la plupart d'entre nous envisage généralement la nouveauté ou l'inconnu avec appréhension ou avec l'espoir d'une panacée. L'explication de James Gleick est la plus pertinente : « Chaque nouveau média transforme la nature de la pensée humaine. À long terme, l'histoire est le récit d'une in-

formation qui prend conscience d'elle-même[22] ». À mesure qu'évolue la pensée humaine à propos du cyberespace et de la cyber puissance, salutistes et alarmistes se retranchent dans leurs camps respectifs. L'analyse de la littérature de vulgarisation consacrée à la cyber puissance met au jour ce phénomène.

Lorsque Tim Berners-Lee a créé le world wide web, il était conscient de la puissance sociale potentielle qu'il recelait. Sa conception excluait toute approche exclusive. Au contraire, le web « invitait, *enjoignait,* ses habitants à participer à sa construction. Il s'agissait d'un effort mondial[23] » (souligné dans l'original). Cependant, les concepteurs tels que Berners-Lee et les inventeurs de l'Arpanet (*Advanced Research Projects Agency Network*) avant lui voyaient davantage le potentiel révolutionnaire d'une source d'information sans frontières qu'une éventuelle capacité de nuisance. « Le développement des machines sociales exige le développement de mécanismes permettant aux utilisateurs de ces machines de partager des données plus librement sans avoir à craindre qu'elles ne soient utilisées à mauvais escient[24] ». Ainsi, les portes ont été grandes ouvertes, offrant un accès immédiat aussi bien aux actions bienveillantes que malfaisantes.

Le cyberespace est pour beaucoup porteur d'espoir, l'espoir d'un remède universel permettant de pallier nos maux sociaux. En ce qui concerne la guerre, la cyber puissance pourrait favoriser un recul global des actes de violence destructive, un « assaut assisté par ordinateur contre la violence elle-même[25] ». Elle pourrait également susciter un changement social et politique organique (et pacifique). Evgeny Morozov a nommé ce concept *cyber utopisme*, une « croyance naïve dans la nature émancipatrice de la communication électronique qui repose sur le refus obstiné d'en reconnaître les dangers[26] ». Combien d'entre nous ont pensé que le printemps arabe continuerait à prospérer grâce à l'accès d'un nombre croissant de personnes aux bonnes idées ? L'omniprésence de l'information n'est qu'un aspect de la situation. La façon dont le public traite les messages et la réponse qu'il y apporte sont tout aussi importants. L'argument de Morozov, qui affirme que si l'information peut déclencher un changement positif, elle peut également être utilisée par les régimes en vue de maintenir un contrôle répressif, donne à réfléchir.

D'un point de vue quantitatif, le camp alarmiste semble remporter la bataille sur le camp salvationiste dans la littérature consacrée au cyberespace. L'étude sommaire de la littérature populaire relève également un vaste éventail d'avertissements sur les menaces que recèle la technologie et sur nos vulnérabilités. Richard Clarke, qui a travaillé en tant qu'expert en matière de contreterrorisme pour trois administrations présidentielles différentes, décrit sans détours les dangers de la cyber puissance : « La cyber guerre est une réalité. Ce que nous avons vu jusqu'à présent n'est rien comparé à ce qui est possible. Les cyber armes utilisées dans la plupart de ces escarmouches notoires dans le cyberespace étaient primitives... Ce dont sont capables les États-Unis et d'autres nations dans le cadre d'une cyber guerre pourrait anéantir une nation moderne[27] ». Souvenez-vous de la cyber attaque désormais célèbre contre l'Estonie en 2007. La volonté du gouvernement estonien de déplacer le *Monument aux Libérateurs de Tallinn* (le fameux *soldat de bronze*), qui occupait une place de choix dans la capitale, a déclenché la colère de la population russe (y compris celle des Estoniens d'origine russe), pour qui cette statue est le symbole du

sacrifice et de l'honneur. De nombreux autres Estoniens voient cependant en elle le souvenir de l'occupation répressive des Soviétiques. Deux ans après l'intégration de l'Estonie au sein de l'Organisation du traité de l'Atlantique Nord (OTAN), plusieurs membres du gouvernement ont demandé l'enlèvement du monument[28]. Le 15 février 2007, le Parlement a voté une loi interdisant *toute* structure commémorant l'occupation soviétique. Le président Toomas Hendrik Ilves a toutefois opposé son veto au projet de loi, sans doute par souci de trouver une solution pacifique aux tensions[29]. Plusieurs mois plus tard, le gouvernement local a décidé de déplacer le soldat de bronze du centre ville vers la périphérie, ce qui a provoqué un tollé dans la population d'origine russe. Le 27 avril, plusieurs importants sites web estoniens étaient la cible des premières cyber attaques. Parmi les organisations touchées figuraient la présidence estonienne, le Parlement, les principaux ministères, les partis politiques, trois des six grands organes de presse du pays, deux des principales banques et les plus grandes entreprises de communication[30]. De nombreux observateurs ont vu dans le gouvernement russe l'instigateur probable des attaques. Quoi qu'il en soit, cette offensive représente l'un des premiers exemples célèbres de l'utilisation de la cyber puissance dans ce qui est apparu comme un conflit interétatique. Si ces attaques n'ont fait aucune victime, leurs répercutions sociales, politiques et financières dévastatrices ont poussé l'Estonie à demander une intervention militaire de l'OTAN.

Les états ne sont pas les seules victimes potentielles de la cyber puissance. La cyber attaque lancée contre Sony Pictures en décembre 2014, vraisemblablement par la Corée du Nord, pour protester contre la sortie du film *L'interview qui tue !*, une comédie relatant un complot visant à assassiner le président Kim Jong-un, en est un exemple éloquent. La puissance des attaques était telle que Sony s'est vu contraint de reporter la sortie du film. Le président Obama s'est montré critique face à la capitulation de Sony : « Créer un précédent en laissant le dictateur d'un autre pays perturber par des cyber attaques la chaîne de distribution d'une entreprise ou ses produits, et commencer ainsi à nous censurer nous-mêmes, est problématique[31] ». Bien que la Corée du Nord ait démenti être l'auteur de cette offensive, son gouvernement n'en n'a pas moins menacé de lancer des cyber attaques à l'avenir. Experts et politiques américains avaient des avis divergents sur la manière de qualifier ces attaques. Certains, dont le président Obama, les considéraient comme une forme de vandalisme cybernétique, tandis que d'autres y voyaient quelque chose de bien plus sinistre. Interviewé dans un talk show diffusé un dimanche matin, le sénateur John McCain a déclaré qu'il s'agit là de « bien plus que du vandalisme. Nous sommes impliqués dans une nouvelle forme de guerre et nous devons réagir, et réagir avec fermeté[32] ».

Ces récents exemples démontrent qu'il existe, même dans le camp des alarmistes, des divergences sur la manière de décrire l'étendue des dangers. Comme à chaque fois que nous sommes confrontés à une nouvelle technologie ou à une nouvelle expérience, nous avons recours à des analogies pour faciliter la compréhension. Autrement dit, notre formulation des nouvelles idées et concepts est essentielle à la compréhension embryonnaire que nous en avons. Philip Ball l'explique plus clairement : « Ce sont les idées, et non les chiffres et les mesures, qui font avancer la science, et les idées sont uniquement générées

par les personnes qui réfléchissent aux mécanismes de causalité et les utilisent pour formuler les bonnes questions[33] ». Néanmoins, notre réflexe naturel consiste souvent à établir des analogies avec des idées et concepts qui nous sont familiers, tout comme nous utilisons un langage commun pour les décrire, même si cela entraîne la création de préjugés problématiques. Dans la cyber sphère, les premiers penseurs et auteurs ont été nombreux à étudier les enseignements qu'a tirés la société des débuts de l'aviation et de la puissance aérienne et s'en sont servis comme schéma directeur (et parfois comme outil de prévision) pour l'exploration du cyberespace et de la cyber puissance : « La puissance aérienne est semblable à la cyber puissance parce qu'il s'agit d'un domaine dépendant des progrès techniques[34] ». L'analogie peut être utile à bien des égards. À ses débuts, la puissance aérienne servait, par exemple, d'instrument de reconnaissance et de connaissance situationnelle du champ de bataille avant de devenir une application spécifique de la force militaire[35]. Autrement dit, il n'était plus possible de penser la puissance aérienne comme nous pensions la puissance terrestre ou maritime. La nature tridimensionnelle de la puissance aérienne et sa capacité à contourner les considérations traditionnellement liées au champ de bataille nous ont obligés à *penser* la guerre autrement. Le Centre de recherche sur le cyberespace de l'*Air Force Institute of Technology* l'exprime ainsi : « Le cyberespace est un théâtre d'opérations militaires et nous devons commencer à développer une cyber culture. Le défi réside dans l'absence de doctrine... Il nous faut cependant commencer quelque part. Nous sommes, dans une large mesure, dans la même situation que [Billy] Mitchell et [Giulio] Douhet quand ils débattaient de l'application de la puissance aérienne[36] ». En ce sens, nos premières expériences de la puissance aérienne nous sont utiles pour nos premiers pas dans le cyberespace.

L'application de la cyber puissance est cependant, à bien des égards, fondamentalement différente de toutes les puissances militaires qui l'ont précédé. C'est pourquoi nous devons prendre le temps de réfléchir à ces caractéristiques uniques plutôt que de nous contenter d'appliquer des concepts issus des domaines physiques. Libicki est l'un des premiers à avoir compris qu'il fallait adopter une nouvelle attitude pour prospérer dans un monde digital :

> Avec le temps, les transformations technologiques radicales entraînent des transformations radicales dans l'organisation du travail et de la société en général. À l'origine, le moteur électrique n'a pas davantage booster la productivité que les machines à courroie qu'il remplaçait ; au fil du temps, les usines verticales conçues pour réduire au maximum le nombre de courroies ont laissé la place aux usines horizontales conçues pour faciliter le flux des employés et des matériaux. De même, les ordinateurs ne peuvent apporter une aide considérable aux entreprises tant qu'elles n'auront pas revu leurs modes opératoires pour les adapter à la logique du silicium. Les conflits conventionnels et non conventionnels suivront inévitablement la même voie, en s'adaptant tout d'abord au changement en l'intégrant, avant de se réinventer[37].

C'est là tout le paradoxe de l'utilisation d'analogies dans le cyberespace. L'unique avantage des analogies appliquées à la cyber puissance réside dans le fait qu'elles nous mettent en garde contre les représentations courantes, telles que les analogies.

Les stratèges en herbe confrontés à la cyber puissance doivent comprendre le rapport de la société aux nouvelles technologies, pour se dégager de la polarisation des premiers penseurs, d'une part, et utiliser, tout en s'en méfiant, les analogies avec les anciennes technologies, d'autre part.

S'adapter à l'incertitude inhérente au cyberespace

> *Le télescope… était suffisamment puissant pour discerner les détails qui étaient jusqu'alors hors de vue du commandant, mais pas suffisamment pour produire l'équivalent administratif du principe d'incertitude d'Heisenberg dans le domaine de la physique, selon lequel il est impossible de mesurer les particules subatomiques car le fait même de les mesurer entraînerait leur modification.*
>
> —Martin van Creveld

Dans son ouvrage intitulé *Command in War*, Martin van Creveld nous avertit, qu'en dépit de tous nos efforts pour créer de l'ordre à partir du chaos, l'incertitude demeure une caractéristique intemporelle de la guerre[38]. Le cyberespace est notre nouveau télescope. Il nous donne un accès à l'information jusqu'ici inimaginable. Néanmoins, l'incertitude persiste même à l'ère du Big Data. Comment les étudiants en cyber stratégie peuvent-ils faire face à ce dilemme ? Comme le rappelle la définition de la stratégie énoncée au début de cet article, l'adaptation est fondamentale. Le succès de l'adaptation exige deux choses : 1) comprendre la nature dialectique de la stratégie et 2) évaluer ce qui reste inconnu, et dans quelle mesure.

La stratégie des autres

Le champion de boxe Mike Tyson aurait dit la célèbre phrase « Tout le monde a un plan jusqu'au premier coup-de-poing dans la face[39] ». Si la stratégie consiste à optimiser son avantage concurrentiel, les étudiants en stratégie doivent reconnaître que tout opposant stratégique pensant a voix au chapitre quand il s'agit de déterminer le résultat d'un engagement. Ce seul fait est source d'incertitude pour le stratège. Il incombe par conséquent aux étudiants en stratégie, et plus particulièrement en cyber stratégie, de tenir compte des principaux acteurs actuels du secteur. Comme l'explique Timothy Thomas : « Les cyber stratèges seraient bien avisés de se familiariser avec les méthodes, les définitions et les concepts des cyber-états les plus compétents [40]».

Les États-Unis et l'Europe occidentale ont une longueur d'avance dans le développement des cyber outils et technologies. Il suffit de jeter un œil à la liste du magazine *Forbes* des trois marques les plus valorisées au monde – Apple, Microsoft et Google – pour voir où l'innovation a généré d'énormes profits[41]. Comme le souligne Joseph Nye,

cette avance a eu, à bien des égards, un impact énorme sur la distribution géopolitique de la puissance :

> Au vingtième siècle, la science et la technologie ont apporté de nouvelles dimensions spectaculaires aux ressources du pouvoir... Par conséquent, le rôle central des États-Unis dans la révolution de l'information à la fin du siècle lui a permis d'initier une révolution dans les affaires militaires. La capacité à utiliser les technologies de l'information pour créer des armes de précision, collecter des renseignements en temps réel, établir une vaste surveillance des théâtres régionaux et améliorer le commandement et le contrôle des opérations a permis aux États-Unis de s'imposer comme la seule superpuissance militaire du monde[42].

Selon toute apparence, cet écart tend toutefois à se resserrer. La Chine, la Russie et d'autres états consacrent une part importante de leurs budgets militaires au développement de cyber technologies offensives et défensives. D'après un récent rapport de *TechRepublic* , « Peter W. Singer, directeur du *Center for 21st Century Security and Intelligence* de la Brookings Institution, a déclaré que 100 nations se dotent de commandements militaires pour la cyber sécurité... Il y a 20 acteurs sérieux dont quelques-uns seraient en mesure de mener une vaste cyber guerre[43] ». Les préjugés et représentations résultant de l'étymologie du cyberespace en anglais peuvent s'avérer encore plus problématiques sur la scène internationale :

> Avant même de se pencher sur les divergences dans la perception des attitudes et des menaces, il existe un problème plus fondamental qui réside dans l'absence d'une terminologie commune aux principaux acteurs du cyberespace. Les définitions de termes tels que cyber conflit, cyber guerre, cyber attaque, cyber arme, etc. utilisées par le Royaume-Uni, les États-Unis, la Russie et la Chine ne coïncident pas, même lorsqu'il existe des définitions officielles ou généralement acceptées dans chaque langue. Par ailleurs, la traduction directe de termes spécifiques du russe ou du chinois qui ressemblent à des termes anglais, et vice versa, peut compliquer encore les choses en donnant la fausse impression d'une compréhension mutuelle, alors que ces termes font en réalité référence à des concepts totalement différents[44].

Les états ne sont pas les seuls acteurs engagés dans la bataille. Si la question de l'attribution reste difficile dans le cyberespace, comme nous le verrons plus tard, plusieurs cyber attaques spectaculaires ont été attribuées à des acteurs non étatiques[45]. Contrairement à la domination des domaines physiques, qui requiert soit un effectif massif soit des armes ultrasophistiquées, le coût d'entrée en matière de cyber puissance reste relativement faible. Des connaissances approfondies sont certainement indispensables, mais l'architecture de l'Internet est conçue de telle sorte que ses utilisateurs sont vulnérables aux méfaits venus de toutes parts. Les étudiants en stratégie doivent donc se poser la question suivante : en termes de puissance militaire, les capacités informatiques servent-elles à niveler ce qui apparaissait jusqu'ici comme un terrain de jeu hiérarchique ? Dans ce cas, comment les

armées se préparent-elles, en période de restrictions budgétaires, à cette myriade d'adversaires potentiels ?

En outre, le stratège doit s'efforcer de comprendre, et d'apprécier, la manière dont ces adversaires potentiels *pensent* l'utilisation de la puissance. Par exemple, « En Chine, la pensée stratégique a une très longue tradition. Il suffit de consulter son encyclopédie militaire pour se faire une idée de la centaine de termes chinois définis qui incluent l'adjectif *stratégique*[46] ». Quelles sont les implications de ce constat dans l'utilisation chinoise de la cyber puissance, non seulement aujourd'hui, mais également dans le contexte d'une stratégie à long terme ? De plus, et peut-être plus important encore, quels sont les problèmes de sécurité qui seraient affectés par ces décisions ? Le cyber stratège doit associer recherche réfléchie et libre-pensée pour aborder les questions problématiques de cet ordre en vue de s'adapter à l'incertitude engendrée par la présence d'autres acteurs dans le cyberespace.

L'« inconnu » cybernétique

Dans le cyberespace, l'incertitude n'est pas uniquement liée à la présence d'ennemis intelligents. En réalité, les caractéristiques propres de la cyber puissance produisent un niveau d'incertitude avec lequel les stratèges sont contraints de composer. Les deux exemples classiques sont 1) attribution/investigation et 2) classification/coopération. Paradoxalement, l'un est le produit du progrès technologique tandis que l'autre est le résultat de nos propres politiques nationales.

En 2007, il était facile d'attribuer les attaques contre l'Estonie à la Russie. Leur timing, les protestations passionnées du gouvernement russe contre le déplacement du soldat de bronze, la colère de la population d'origine russe dans les pays baltes et les capacités exhibées par le gouvernement russe à d'autres occasions faisait de Moscou le principal suspect. Il en va de même des attaques lancées contre Sony Entertainment en 2014. Leur timing, la sortie imminente du film *L'interview qui tue* ! et les déclarations publiques du gouvernement nord-coréen (même si l'on tient compte de ses démentis) désignaient Pyongyang. Cependant, devant un tribunal, tous ces facteurs se résumeraient à de simples preuves circonstancielles. Il peut être beaucoup plus difficile d'attribuer la responsabilité d'un acte dans le cyberespace que de déterminer la cause d'une catastrophe nucléaire. Les organisations telles que la *Defense Threat Reduction Agency* disposent désormais de programmes d'analyse nucléo-légale ultra sophistiqués capables d'identifier l'origine du matériau nocif contenu dans des débris radioactifs, voire de localiser sa zone de provenance[47]. Les adresses IP fantômes et autres techniques employées dans le cyberespace rendent l'attribution complexe pour les professionnels de la cyber sécurité et constituent une préoccupation d'autant plus grande dans le domaine de la géopolitique. Comment les dirigeants peuvent-ils prendre des décisions en matière de sécurité nationale et appuyer d'éventuelles interventions militaires sans connaître l'auteur des actions ? Ainsi, si les nations de l'Alliance ont refusé d'agir lorsque l'Estonie a demandé à l'intervention de l'OTAN suite aux attaques de 2007, ce n'est pas simplement en raison de la confusion

quant à l'assimilation des cyber attaques à des actes de guerre, mais parce qu'elles ne pouvaient déterminer avec *certitude* que ces attaques étaient le fait de la Russie (et encore moins du *gouvernement* russe). En substance, les investigations menées dans le cadre de cyber opérations n'ont pas encore atteint le niveau de sophistication rencontré dans les domaines physiques. Par conséquent, l'incertitude qui entoure les actes perpétrés dans le cyberespace peut rendre les décisions d'intervention apparemment évidentes incroyablement complexes.

À terme, la police scientifique appliquée à la cybercriminalité pourrait atteindre un niveau de sophistication comparable à celui des domaines physiques. La recherche et le développement scientifique ouvriront la voie. Lors d'une réunion de dirigeants d'entreprise le 11 octobre 2012, Leon Panetta, alors secrétaire à la Défense, a noté

> qu'au cours « des deux dernières années, le DoD [département de la Défense] a massivement investi dans les moyens d'investigation afin de résoudre ce problème d'attribution et ces efforts commencent à porter leurs fruits. Les agresseurs potentiels doivent savoir que les États-Unis ont les moyens de les localiser et de les contraindre à répondre de leurs actes qui seraient susceptibles de nuire au pays[48].

À cette époque, de nombreuses voix ont mis en doute la validité de cette affirmation, voyant dans le discours du secrétaire davantage une menace dissuasive que la véritable prétention d'améliorer les capacités. Si l'attribution demeure un problème délicat dans le cyberespace, le développement des moyens d'investigation est toutefois en progrès[49]. Les techniques visant à masquer l'identité dans le cyberespace évoluent également, de sorte que la question de l'attribution représente, au moins à court terme, une incertitude problématique pour le cyber stratège.

L'incertitude que génèrent les difficultés de classification apparaît toutefois comme un problème d'origine humaine et la source d'un paradoxe intéressant entre la sécurité et la coopération. Le site web de la présidence des États-Unis en est un exemple frappant. D'une part, la Maison Blanche insiste sur la nécessité de protéger les informations classifiées : « Ce sont les réseaux militaires et de renseignement classifiés qui assurent notre sécurité ». D'autre part, le même site web vante l'importance de la collaboration et de la coopération internationales :

> Étant donné que le cyberespace traverse toutes les frontières nationales, il est impératif de collaborer avec nos partenaires internationaux. Nous nous appliquerons à créer les conditions favorables, et à obtenir un consensus, pour la mise en place d'un environnement international dans lequel les états s'accordent sur la valeur d'un cyberespace ouvert, interopérable, sûr et fiable[50].

Quiconque a travaillé dans le domaine de la cyber puissance militaire vous dira que les procédures de sécurité en matière de classification sont incroyablement rigoureuses, sans doute en raison de l'idée *d'utilisation unique* des cyber armes. Autrement dit, si une cyber arme exploite une vulnérabilité particulière dans un réseau ennemi et que l'ennemi détecte

cette action, il a la possibilité de faire deux choses, presque instantanément : 1) corriger cette vulnérabilité afin d'éviter que des armes similaires ne disposent du même accès et causent les mêmes dommages et 2) utiliser la même arme dans une offensive perpétrée contre toute autre entité présentant la même vulnérabilité. Ainsi, le concept d'arme à utilisation unique entraîne deux comportements majeurs. Premièrement, les utilisateurs potentiels peuvent retarder son emploi le plus longtemps possible parce qu'ils ne souhaitent pas exposer leur connaissance de l'arme. Cette option est, dans une certaine mesure, susceptible de réduire la probabilité d'une attaque car les acteurs peuvent préférer retarder son utilisation éventuelle le plus longtemps possible, ou au moins jusqu'à ce qu'ils aient l'impression d'en avoir *vraiment* besoin. Deuxièmement, et cet aspect est étroitement lié au premier, les acteurs du cyberespace souhaitent préserver à tout prix cette capacité pour éviter que sa connaissance ne se répande et ont donc tendance à classifier ces capacités (et les armes elles-mêmes) au niveau le plus élevé possible.

Cette situation place les efforts de coopération internationale face à un défi unique. Au vu des difficultés qu'ils rencontrent à préserver les informations classifiées de toutes sortes, les acteurs tendent à dissimuler leurs cyber cartes, ce qui entraîne des classifications de sécurité intenses (et parfois éreintantes). Néanmoins, cette attitude va entièrement à l'encontre des pratiques visant à encourager la coopération internationale. Des exemples de coopération fructueuse existent cependant : le Centre d'excellence de l'OTAN pour la cyber défense, en Estonie, apparaît comme un modèle institutionnel possible. Ce centre propose des axes pour l'échange international d'informations et héberge des exercices internationaux et des simulations de bonnes pratiques. L'efficacité d'une telle agence dépend toutefois des informations que les états membres choisissent de partager. Dans bien des cas, les gouvernements individuels continuent de classifier leurs techniques les plus avancées au plus haut niveau national, interdisant ainsi leur divulgation à l'échelle internationale, même avec leurs plus proches partenaires.

L'auto-inspection opérée par le gouvernement américain après les attentats du 11 septembre 2001 révèle une approche intéressante. Dix ans après les attaques, un rapport du sénat des États-Unis souligne que

> les attentats du 11 septembre nous ont montré que l'approche du « besoin d'en connaître » de la Guerre froide dans la gestion des informations classifiées et sensibles a instauré une culture de la sécurité de l'information qui a entraîné d'innombrables cloisonnements et poches secrètes dans le traitement des informations les plus précieuses de la nation. Cette approche a peut-être fonctionné pendant la Guerre froide, mais elle n'était pas apte à assurer la sécurité des États-Unis dans un monde de menaces asymétriques. De nombreuses personnes ont constaté que la protection du pays face à ces nouvelles menaces exigeait une révision complète des modes de fonctionnement du gouvernement[51].

De la même manière, les menaces asymétriques que comporte aujourd'hui la cyber puissance exige de revoir les cloisonnements nationaux et la classification traditionnelle. Il ne s'agit pas de plaider en faveur de l'élimination de toute classification nationale des outils

et techniques cybernétiques, les stratèges doivent toutefois admettre que, sans un échange significatif d'informations, la coopération n'est qu'un tigre de papier qui accroît au final la vulnérabilité de chaque état membre.

Dans la guerre, l'incertitude est omniprésente. Le cyberespace et les technologies associées ont pu initialement laisser penser qu'un accès robuste à l'information permettrait d'ordonner le chaos, mais la réalité est plus proche du contraire. Notre accès actuel au cyberespace a, d'une certaine manière, compliqué la situation. Paradoxalement, l'ubiquité de l'information augmente l'incertitude en obligeant le stratège à se concentrer sur la *hiérarchisation* de l'information disponible plutôt que sur son *accès*, ce qui rend l'adaptation et la flexibilité plus importantes que jamais, en particulier pour le stratège.

La formation à la cyber stratégie : quelques exemples

Au cours des vingt dernières années, et plus particulièrement des dix dernières, plusieurs états ont mis en place des programmes de formation visant à stimuler la réflexion des stratèges sur le cyberespace et la cyber puissance. L'examen rapide de ces programmes montre que nombre d'entre eux sont axés sur le développement des compétences tactiques et opérationnelles au détriment de la pensée stratégique.

Le Royaume-Uni en est un exemple intéressant. En 2011, le pays a publié sa stratégie nationale en matière de cyber sécurité, mettant l'accent sur quatre objectifs principaux :

- faire du Royaume-Uni l'un des endroits les plus sûrs de la planète pour faire des affaires dans le cyberespace ;
- rendre le Royaume-Uni plus résilient aux cyber attaques et mieux protéger nos intérêts dans le cyberespace ;
- contribuer à créer un cyberespace ouvert, dynamique et stable qui soutiennent les sociétés ouvertes ;
- développer les connaissances, compétences et capacités du Royaume-Uni en matière de cyber sécurité[52].

Si l'on considère la définition de la stratégie mentionnée plus tôt dans cet article, on peut affirmer que le Royaume-Uni attache une grande importance à la pensée stratégique mais que ses objectifs nationaux sont principalement de nature tactique. Même le quatrième objectif, bien qu'il fasse référence au développement des connaissances, semble davantage tourné vers la formation tactique que vers l'éducation stratégique. En 2013, une évaluation gouvernementale de cette stratégie a « identifié le manque de compétences en matière de cyber sécurité comme un défi majeur... Si le Royaume-Uni souhaite se donner les moyens de lutter contre les cyber menaces, le secteur de la cyber sécurité étant amené à croître, nous devons renforcer notre réservoir de cyber talents et préparer les étudiants à exercer des fonctions de débutant dans le domaine de la sécurité[53] ». Cette prise de position a incité la *Higher Education Academy* et d'autres programmes d'éducation à mettre en place des cursus de formation musclés dans le domaine de la cyber sécurité. Étant donné

l'impact du cyberespace, ce genre de formation est indiscutablement important voire nécessaire à la défense nationale, mais elle doit s'accompagner d'une formation stratégique plus approfondie.

Le programme d'études militaires professionnelles (PME) des États-Unis est conçu pour préparer chaque individu à l'ensemble de sa carrière militaire. Le PME de l'armée de l'Air vise, par exemple, à former

> des professionnels qualifiés dans le métier des armes, dotés d'une approche intuitive de la conduite des opérations interarmées, reposant sur des compétences individuelles. L'objectif consiste à former des diplômés capables de servir aux niveaux de guerre appropriés dans un environnement interarmées et de développer une pensée tactique, opérationnelle et stratégique de qualité dans une perspective commune[54].

Les programmes de formation militaires proposent, à différentes étapes clés d'une carrière militaire, un rappel sur les responsabilités uniques des professionnels des forces armées ainsi qu'une mise à niveau concernant la doctrine, les tactiques et les stratégies relatives au déploiement de la puissance militaire. Les cours spéciaux proposés par l'Air Force Institute of Technology (AFIT) s'adressent aussi bien aux professionnels qu'aux superviseurs de la cyber puissance. En avril 2015, l'AFIT a invité l'auteur à réviser le module stratégie du cursus pour les cours Cyber 300 (superviseur de niveau supérieur). Les responsables du cours avaient constaté que leur module stratégie était davantage axé sur la *politique* nationale que sur la *stratégie* nationale. Nous nous sommes donc appliqués à élargir les leçons (et les exercices associés) afin de stimuler la réflexion stratégique plutôt que de se contenter d'examiner les politiques associées[55].

Le Centre d'excellence de l'OTAN pour la cyber défense déploie d'importants efforts dans le but d'encourager la pensée stratégique. Son site web propose des liens vers les stratégies nationales de chaque état membre en matière de cyberespace ainsi que tous les textes juridiques pertinents[56]. Le centre est toutefois probablement mieux connu pour un livre publié en 2013. Le *Tallinn Manual on the International Law Applicable to Cyber Warfare* est la première tentative de codification des normes internationales de la cyber puissance[57]. S'il n'est pas juridiquement contraignant (l'OTAN ne l'a même pas officiellement examiné), ce manuel a le mérite de définir un cadre en déterminant dans quelle mesure la cyber puissance peut être intégrée aux normes juridiques établies pour les domaines physiques. Le *Tallinn Manuel* était révolutionnaire dans la mesure où il s'agit de la première tentative de codification des normes internationales relatives à la cyber puissance. Le centre accueille des exercices tactiques qui gagnent tous les ans en popularité au sein des états membres et propose des programmes de formation dans divers domaines, mais ses principales formations stratégiques sont essentiellement axées sur les questions de droit international[58].

Tel que nous l'avons démontré dans le présent article, la pensée stratégique, notamment dans le domaine du cyberespace, exige une évolution des mentalités. Comme l'explique Timothy Thomas : « Il faut adopter une approche holistique pour former un cyber

stratège, en raison de la nature mondiale et de la vitesse vertigineuse des chiffres[59] ». L'explosion récente du nombre de formations consacrées au cyberespace est une bonne chose qui montre que les états prennent les effets de la cyber technologie au sérieux. Cependant, la *formation* doit s'accompagner d'une éducation. Si nous souhaitons développer de futurs cyber stratèges, l'introduction aux outils cybernétiques n'est que la première étape. Une formation plus complète à la cyber stratégie devra inclure une connaissance plus approfondie de la dynamique du cyber environnement ainsi que le respect des imprévus.

Conclusion : l'aventure continue

Comme l'illustre le présent article, mener une réflexion stratégique sur la cyber puissance n'est pas chose aisée. L'enseignement et l'apprentissage de la stratégie sont suffisamment complexes, d'autant plus si l'on considère les nombreuses définitions, et perceptions, de la stratégie elle-même. Si la stratégie dépend au final de la compréhension de notre propre environnement et de l'adaptation à l'incertitude, il nous reste beaucoup à faire dans le domaine du cyberespace. Les préjugés et représentations, souvent d'origine étymologique, entravent souvent notre compréhension de l'environnement cybernétique. De plus, la confusion contextuelle entraîne souvent une polarisation des premières publications et une tendance à l'utilisation d'analogies anachroniques visant à faciliter la compréhension, qui représentent toutes deux un défi pour la pensée stratégique. Dans le cyberespace, l'incertitude est le produit de la nature dialectique de la stratégie et des limites de l'information utile, à la fois organique et synthétique, inhérentes au cyberespace et à notre utilisation de la cyber puissance. Dans ce contexte, l'adaptation est essentielle pour le cyber stratège.

Les militaires professionnels sont confrontés à un défi colossal. On leur demande d'intégrer le cyberespace et la cyber puissance dans une série d'applications militaires déjà complexes. Cependant, les premières expériences acquises avec la technologie révèlent que nous n'avons pas fini d'en comprendre toutes les subtilités. Les étudiants en cyber stratégie se doivent de reconnaître et de respecter l'énormité de l'inconnu. Pour parvenir à concevoir et à formuler une stratégie cohérente de la cyber puissance, il faudra sans doute encore plusieurs années et davantage de rigueur intellectuelle. En attendant, les professionnels qui souhaitent mener une réflexion stratégique sur la cyber puissance doivent s'efforcer de comprendre l'environnement complexe du cyberespace et se montrer suffisamment flexibles pour s'adapter aux incertitudes omniprésentes. Enfin, le cyberespace et la cyber puissance sont des questions importantes que nos étudiants en stratégie doivent maîtriser ; parallèlement, cette technologie présente une richesse intellectuelle susceptible de favoriser le développement et l'exploitation d'une réflexion stratégique plus approfondie, à condition d'adopter une approche appropriée.

Notes

1. Un remerciement particulier au Dr. Thomas Hughes pour cette formule perspicace.
2. FREEDMAN, Lawrence, *Strategy: A History*, New York : Oxford University Press, 2013, p. XIV.
3. VON CLAUSEWITZ, Carl, *On War*, éd. et trad. HOWARD, Michael, et PARET, Peter Princeton, NJ : Princeton University Press, 1976, p. 178.
4. LIDDELL HART, Basil Henry *Strategy*, Londres : Faber and Faber, 1954, p. 323.
5. LUTTWAK, Edward N., *Strategy: The Logic of War and Peace*, Cambridge, MA : Belknap Press of Harvard University Press, 1987, p. XII.
6. Voir également LONSDALE, David J., *The Nature of War in the Information Age: Clausewitzian Future*, Londres : Frank Cass, 2004, pp. 229–230. Il soutient que la nature de la guerre est déterminée par cinq facteurs, parmi lesquels *la logique paradoxale* basée sur la présence d'un ennemi intelligent.
7. William Gibson, *Neuromancer*, Princeton, NJ : John Wiley, 1984, p. 51.
8. FORSYTH, Mark, *The Etymologicon: A Circular Stroll through the Hidden Connections of the English Language*, New York : Berkley Books, 2011, p. 103.
9. *Dictionary of Etymology: The Origin of American English Words*, éd. BARNHART, Robert K., New York : HarperCollins, 1995, p. 181.
10. BRATE, Adam, *Technomanifestos: Visions from the Information Revolutionaries*, New York : Texere, 2002, p. 18.
11. Clausewitz, *On War*, p. 101.
12. Sun Tzu, *The Art of War*, trad. SAWYER, Ralph D., New York : Barnes and Noble, 1994, p. 179.
13. BOUSQUET, Antoine, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, New York : Columbia University Press, 2009, p. 160.
14. L'US Air Force publie sa mission, ainsi que ses valeurs, ses compétences clés et son histoire sur son site web accessible au public. « Mission », US Air Force, consulté le 9 mai 2016, www.airforce.com/learn-about/our-mission/.
15. Les concepts exposés dans ce paragraphe et les deux suivants sont tirés de l'un de mes essais intitulé « *Four Dimensions to the Digital Debate* », récemment publié sous forme de chapitre dans BAILEY, Richard J. Jr., FORSYTH, James W. Jr., et YEISLEY, Mark O., éd., *Strategy: Context and Adaptation from Archidamus to Airpower*, Annapolis : Naval Institute Press, 2016, pp. 186–207.
16. KUEHL, Daniel T., « From Cyberspace to Cyberpower: Defining the Problem », in *Cyberpower and National Security*, éd. KRAMER, Franklin D., STARR, Stuart H., et WENTZ, Larry K., Dulles, VA : Potomac Books, 2009, p. 26.
17. LIBICKI, Martin C., *Conquest in Cyberspace: National Security and Information Warfare*, New York : Cambridge University Press, 2007, pp. 8–9.
18. HAYES, Justin Cord, *The Unexpected Evolution of Language*, Avon, MA : Adams Media, 2012, p. 67.
19. KEARNS, Kate, *Semantics*, 2e éd., Londres : Palgrave Macmillan, 2011, p. 3.
20. *Id.*, p. 6.
21. Le professeur Wendt a utilisé ce scénario pour démontrer que les menaces sociales ne sont pas des phénomènes naturels mais des constructions sociales. Voir WENDT, Alexander, « Anarchy Is What States Make of It: The Social Construction of Power Politics », *International Organization* 46, no. 2, printemps 1992 : p. 405.
22. GLEICK, James, *The Information: A History, a Theory, a Flood*, New York : Pantheon Books, 2011, p. 12.
23. BRATE, *Technomanifestos*, p. 231.
24. HENDLER, Jim, et BERNERS-LEE, Tim, « From the Semantic Web to Social Machines: A Research Challenge for AI on the World Wide Web », *Artificial Intelligence* 174, no 2, février 2010, pp. 156-161.
25. RID, Thomas, *Cyber War Will Not Take Place*, New York : Oxford University Press, 2013, p. XIV. Note de l'auteur : lors d'un entretien téléphonique avec l'auteur au cours de l'été 2013, le professeur Rid a déclaré qu'en dépit du titre de son livre, sa position n'était pas forcément optimiste. Il soutient uniquement que la

cyber puissance est une alternative moins violente aux mécanismes conflictuels tels que le sabotage, l'espionnage et la subversion et que cette option pourrait réduire la propension générale à la violence.

26. MOROZOV, Evgeny, *The Net Delusion: The Dark Side of Internet Freedom*, New York : Public Affairs, 2011, p. XIII.

27. CLARKE, Richard A., et KNAKE, Robert K., *Cyber War: The Next Threat to National Security and What to Do about It*, New York : HarperCollins, 2010, pp. 30–31.

28. À cette époque, l'Union de la patrie et Res Publica était le parti le plus véhément au sein du gouvernement estonien. Pour de plus amples informations, voir ALAS, Joel, « Bill Paves Way for Statue Removal », *Baltic Times*, 15 novembre 2006, www.baltictimes.com/news/articles/16812/.

29. Pour le reportage complet, voir « Law to Remove Memorial Vetoed by Estonia's Leader », *South Bend Tribune*, 23 février 2007, http://articles.southbendtribune.com/2007-02-23/news/26801820_1_bronze-soldier-president-toomas-hendrik-ilves-soviet-war-memorial.

30. TRAYNOR, Ian, « Russia Accused of Unleashing Cyberwar to Disable Estonia », *Guardian*, 16 mai 2007, www.theguardian.com/world/2007/may/17/topstories3.russia.

31. MULLEN, Jethro, « North Korea and the Sony Hack: The War of Words Escalates », *CNN*, 22 décembre 2014, www.cnn.com/2014/12/22/world/asia/north-korea-us-sony-hack-who-says-what/index.html.

32. *Id.*

33. BALL, Philip, « Machine Envy », *Aeon Magazine*, 7 janvier 2014, http://aeon.co/magazine/science/science-is-becoming-a-cult-of-hi-tech-instruments/.

34. ANDRESS, Jason, et WINTERFELD, Steve, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham, MA : Elsevier-Syngress, 2011, p. 27.

35. Pour une analyse des différentes étapes de la pensée, et du positionnement, de l'US Air Force, voir THORNHILL, Paula G., « Over Not Through »: The Search for a Strong, Unified Culture for America's Airmen, Santa Monica, CA : RAND Corporation, 2012, www.rand.org/content/dam/rand/pubs/occasional_papers/2012/RAND_OP386.pdf.

36. MILLS, Robert F., RAINES, Richard A., et WILLIAMS, Maj Paul D., *Developing Cyberspace Competencies for Air Force Professional Military Education*, Wright-Patterson AFB, OH : Center for Cyberspace Research, Air Force Institute of Technology, 2007, p. 1.

37. LIBICKI, Martin C., *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, McNair Paper 28, Washington, DC : Institute for National Strategic Studies, National Defense University, 1994, p. 3.

38. VAN CREVELD, Martin, *Command in War*, Cambridge, MA : Harvard University Press, 1985, p. 142.

39. BERARDINO, Mike, « Mike Tyson Explains One of His Most Famous Quotes », *Sun Sentinel*, 9 novembre 2012, http://articles.sun-sentinel.com/2012-11-09/sports/sfl-mike-tyson-explains-one-of-his-most-famous-quotes-20121109_1_mike-tyson-undisputed-truth-famous-quotes.

40. THOMAS, Timothy, « Creating Cyber Strategists: Escaping the 'DIME' Mnemonic », *Defence Studies* 14, no. 4, 28 août 2014, p. 382.

41. BADENHAUSEN, Kurt, « Apple, Microsoft, and Google Are World's Most Valuable Brands », *Forbes Magazine*, 5 novembre 2014, www.forbes.com/sites/kurtbadenhausen/2014/11/05/apple-microsoft-and-google-are-worlds-most-valuable-brands/.

42. NYE, Joseph S. Jr., *Soft Power: The Means to Success in World Politics*, New York : Public Affairs, 2004, p. 18.

43. RANGER, Steve, « Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar », *TechRepublic*, 24 avril 2014, www.techrepublic.com/article/inside-the-secret-digital-arms-race/.

44. GILES, Keir et HAGESTAD, William III, « Divided by a Common Language: Cyber Definitions in Chinese, Russian and English », in *Proceedings: 5th International Conference on Cyber Conflict*, éd. PODINS, K., STINISSEN, J., et MAYBAUM, M., Tallinn, Estonie : NATO Cooperative Cyber Defence Centre of Excellence, 2013, pp. 414–415.

45. Pour une analyse approfondie des effets des acteurs non étatiques dans le cyberespace, voir SIGHOLM, Capt Johan, « Non-State Actors in Cyberspace Operations », *Journal of Military Studies* 4, no. 1, 2013, www.ida.liu.se/~g-johsi/docs/JMS_4-1_Sigholm_Non-State_Actors_in_CyberOps.pdf.

46. THOMAS, « *Creating Cyber Strategists* », p. 381.

47. Voir « *Nuclear Technologies* », Defense Threat Reduction Agency and USSTRATCOM Center for Combating WMD and Standing Joint Force Headquarters-Elimination, consulté le 10 mai 2009, www.dtra.mil/Research/NuclearTechnologiesDepartment.aspx.

48. PANETTA, Leon E., secrétaire de la Défense, « *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City* », Département américain de la Défense, 11 octobre 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

49. STEINBERG, James, et O'HANLON, Michael E., *Strategic Reassurance and Resolve: U.S.-China Relations in the Twenty-First Century*, Princeton, NJ : Princeton University Press, 2014, p. 176.

50. « *Foreign Policy: Cybersecurity* », Maison Blanche, Président Barack Obama, consulté le 9 mai 2016, www.whitehouse.gov/issues/foreign-policy/cybersecurity.

51. Sénat, *Déclaration de Zoe Baird Budinger et Jeffrey H. Smith, Comité sur la Sécurité intérieure et les Affaires gouvernementales du Sénat des États-Unis : Ten Years after 9/11; a Status Report on Information Sharing*, 112e Cong., 1re sess., 12 octobre 2011, www.fas.org/irp/congress/2011_hr/101211smith.pdf.

52. Cabinet Office, *The UK Cyber Security Strategy: Report on Progress and Forward Plans*, décembre 2014, www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

53. « *Learning and Teaching in Cyber Security* », Higher Education Academy, consulté le 9 mai 2016, www.heacademy.ac.uk/funding-call/learning-and-teaching-cyber-security.

54. MILLS, RAINES, et WILLIAMS, *Developing Cyberspace Competencies*, p. 3.

55. Pour une description complète des cours Cyber 200 et 300 de l'AFIT, voir « *Cyberspace 200/300 Courses* », AFIT Graduate School of Engineering and Management, 8 Décembre 2015, www.afit.edu/CCR/programs.cfm?p=60&a=pd&page=162&tabname=Tab1A.

56. Voir « *Cyber Security Strategy Documents* », NATO Cooperative Cyber Defence Centre of Excellence, 3 août 2015, https://ccdcoe.org/strategies-policies.html.

57. SCHMITT, Michael N., éd., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, UK : Cambridge University Press, 2013.

58. Pour une liste des formations et cursus proposés par le centre, voir « *Cyber Security Training events* », NATO Cooperative Cyber Defence Centre of Excellence, consulté le 9 mai 2016, https://ccdcoe.org/events.html.

59. THOMAS, « *Creating Cyber Strategists* », p. 390.