Les enjeux de la numérisation du champ de bataille

Amaël Cattaruzza, Stéphane Taillat

Les enjeux de la numérisation du champ de bataille

Amaël Cattaruzza et Stéphane Taillat[*], Centre de recherche des écoles de Saint-Cyr Coëtquidan

Introduction

En décembre 2016, la société de sécurité informatique CrowdStrike (Crowdstrike, 2016) publie un rapport concernant une attaque persistante qu'elle impute à un groupe de hackers lié au renseignement militaire russe et ayant ciblé des pièces d'artillerie ukrainiennes. Selon ce document, le groupe Fancy Bear aurait introduit un malware dans une application Android développée en 2013 par Jaroslav Sherstuk – officier de l'artillerie ukrainienne qui souhaitait améliorer la transmission de données entre les batteries d'obusiers D 30 et améliorer la précision de ces derniers – permettant ainsi la géolocalisation et la destruction d'une grande partie de ces pièces. En dépit de l'inexactitude de nombre des affirmations formulées par la firme américaine (Carr, 2017), cette anecdote illustre la façon dont peut se déployer la numérisation du champ de bataille. Celle-ci n'est pas limitée aux initiatives des organisations militaires dans la mesure où elle inclut des aspects civils (médias sociaux, vie numérique des combattants, etc.). Cet aspect suscite donc des vulnérabilités supplémentaires que les organisations doivent prendre en compte. D'autre part, les modes hiérarchiques et la manière dont se diffusent et se déploient les informations et les innovations questionnent les structures des organisations à la fois en temps de paix et pour le combat. Si la structure en réseaux, caractérisée par l'auto-organisation et la synchronisation d'unités distribuées, est présentée comme plus avantageuse que la structure hiérarchique centralisée, elle nécessite d'opérer constamment des compromis dans la recherche de l'efficacité militaire.

Le projet de numérisation du champ de bataille trouve son origine dans les débats stratégiques américains au sujet de l'intégration des nouvelles technologies de l'information et de la communication (NTIC) dans le champ militaire. Ces réflexions sont centrées autour du rôle de l'information, comprise comme connaissance autant que comme capacité à échanger des données (Arquilla & Ronfeldt, 1993). S'y trouve déjà contenue la double dimension de mise en données du champ de bataille et de mise en réseau des forces combattantes.

[*] Amaël Cattaruzza et Stéphane Taillat sont enseignants chercheurs aux écoles de Saint-Cyr Coëtquidan. Ils conduisent leurs travaux dans le cadre du pôle « Mutation des conflits » du Centre de Recherche.

Elles trouvent leur maturation à la fin des années 1990 par l'adjonction de l'impératif de *transformation* à l'analyse du « combat réseau-centré » (*network-centric warfare*). Dans un article fondateur, le vice-amiral Arthur K. Cebrowski et l'analyste John J. Gartska en expliquent les logiques (Cebrowski et Gartska, 1998)[1]. L'impact révolutionnaire des NTIC se traduit par la nécessité de maîtriser « *des interactions à forte intensité d'information entre les nœuds de calcul du réseau* » (*ibid.*, 19). La clé de la supériorité militaire réside donc dans la capacité à traiter et disséminer très rapidement de l'information dans une organisation structurée en réseau. D'autre part, la multiplication des capteurs doit permettre une connaissance opérationnelle en temps réel de la réalité mouvante du champ de bataille. Il devient donc nécessaire de réformer en profondeur les forces armées, tant dans leur armement que dans leur logique de commandement et de contrôle ou dans la manière de combattre. En ce sens, la *Transformation* est bien la première incarnation doctrinale de la numérisation du champ de bataille. La notion elle-même est inscrite au cœur des impératifs d'adaptation des forces armées de l'OTAN comme en témoigne l'importance de l'*Allied Command Transformation* (ACT) dans l'organigramme militaire de l'Alliance[2]. Au-delà des déboires de ce programme de mutation des armées américaines après les guerres en Irak et en Afghanistan, le concept de « combat réseau-centré » se trouve à la croisée entre deux développements doctrinaux. D'une part, il complète et corrige les débats sur la « révolution des affaires militaires » (RMA) du début des années 1990 (Henrotin, 2008) en ce sens qu'il dépasse la conception de ses principaux promoteurs selon laquelle le chaos du combat peut être prédit et contrôlé (Owens, 2000). D'autre part cependant, il appréhende l'incertitude du champ de bataille sous l'angle d'une information insuffisamment collectée, traitée et disséminée, à rebours de l'approche promue au sein du Corps des Marines dans le « combat de manœuvre » (*maneuver-warfare*) et selon laquelle il est futile de chercher à « *imposer un contrôle précis et positif sur les événements […] dans la mesure où il est déraisonnable d'attendre du commandement et du contrôle qu'il fournisse un ordre précis, prévisible et mécanique du système complexe qu'est la guerre* » (US Marine Corps, 1996 : 46-47). Les promoteurs de la *Transformation* ne semblent adopter la lecture des sciences de la complexité et des théories du chaos que pour mieux en répudier les enseignements. Persiste en effet une vision mécanique et cybernétique du combat comme un système clos régulé et contrôlé au moyen de l'information (Bousquet, 2009 : 215-233)[3].

[1] Le vice-amiral Cebrowski est nommé directeur de l'*Office of Force Transformation* par le secrétaire à la Défense Donald Rumsfeld en 2001, poste qu'il occupe jusqu'à sa mort en 2005, à la suite de laquelle l'organisme est démantelé.

[2] Son officier commandant, le général Denis Mercier, a d'ailleurs rappelé à plusieurs occasions l'importance de la numérisation pour l'avenir des forces de l'OTAN, voir Guibert, 2018.

[3] Cela contraste notamment avec les recommandations qu'avait pu en tirer l'aviateur John Boyd dans les années 1970 avec sa « boucle » OODA (Observer, s'Orienter, Décider, Agir). Loin d'être un système purement itératif, celle-ci repose en effet sur la remise en question continuelle de la manière de percevoir et concevoir l'environnement du combat, voir notamment Boyd 1976.

Par ailleurs, la réponse propre de l'US Army consiste à intégrer ces impératifs dans ses projets existants (Force XXI) en réduisant leur portée par des adaptations limitées : passage aux « brigades modulaires », numérisation des unités et des matériels (Croser, 2007a : 12-14). Ainsi, le cas américain illustre une représentation particulière de la numérisation comme réponse fonctionnelle aux mutations technologiques. Selon cette approche, ces dernières sont des données brutes et neutres auxquelles il convient de s'adapter par leur intégration technique, organisationnelle et doctrinale. En retour, celle-ci est perçue comme condition sine qua non de la supériorité militaire.

Cet article postule que l'enjeu de la numérisation n'est pas fonctionnel. Il s'agit bien d'intégrer les NTIC dans des structures de forces, des organisations et des doctrines en vue de maximiser l'efficacité militaire tout en minimisant les menaces et les risques. Par conséquent, la numérisation est un processus. Néanmoins, celui-ci découle de l'articulation de deux dynamiques. D'une part, la numérisation s'inscrit dans des tendances, des logiques, des représentations développées par les acteurs militaires américains au sujet de l'émergence des NTIC. Il s'agit d'un processus « par le haut » qui se comprend à travers les choix effectués par les forces armées à travers des programmes de numérisation. D'autre part, elle dépend de transformations sociales plus profondes liées au développement du domaine numérique. On peut ici parler de numérisation « par le bas », largement subie, résultant de changements sociaux opérés en dehors ou à la marge des organisations militaires. La numérisation est donc pour partie programmée et pour partie subie. Par conséquent, elle échappe largement au contrôle des acteurs qui la mettent en œuvre. Sur un plan conceptuel, la numérisation du champ de bataille s'inscrit donc dans l'évolution croissante du champ de la conflictualité vers la forme d'un système adaptatif complexe.

Par ailleurs, la numérisation croise deux processus constitutifs : la mise en donnée d'une part, la mise en réseau de l'autre. Si chacun d'entre eux relève de logiques présentes historiquement dans les pratiques militaires, ils se caractérisent par la croyance en leur aspect objectif et neutre.

Ainsi, ce processus organisationnel ne peut être décorrélé de transformations sociales plus profondes. La numérisation ne peut donc être pensée comme une simple adaptation technique tâchant de tirer parti des opportunités apportées par des changements technologiques et s'efforçant d'en limiter les risques. Dit autrement, il n'existe pas un modèle unique et définitif d'intégration des NTIC dans le champ de la conflictualité : l'enjeu n'est pas de découvrir le meilleur usage de ces dernières mais de comprendre comment leur déploiement est la source de propriétés émergentes et de comportements contingents.

D'autre part, les mutations sociotechniques ne répondent pas à des logiques linéaires et centralisées mais dépendent de multiples facteurs selon une logique distribuée. S'interroger sur ce phénomène nécessite de comprendre comment s'articulent les outils techniques et les usages opérationnels qui en sont fait. Se dessine alors un processus non-linéaire et continu qui se traduit par une intégration évoluant selon plusieurs facteurs. Ainsi, les usages et les modes de comportement différenciés témoignent de son caractère toujours inachevé et fluide. Alors que la littérature sur le changement militaire cherche à identifier les facteurs qui guident ces processus d'adaptation et d'innovation, notre approche s'intéresse davantage à leurs impacts et conséquences[4]. Plus particulièrement, cet article s'attache à analyser les usages de la numérisation à partir d'études de cas et de retours d'expérience. Ce faisant, il entend éclairer les enjeux sous plusieurs dimensions : individuelles et organisationnelles, opérationnelles aussi bien que stratégiques.

Ainsi, il est nécessaire de penser ce processus dans un contexte global à partir d'une grille d'analyse sociotechnique. De fait, il n'est pas possible de réfléchir aux enjeux des technologies sur le champ de bataille sans prendre en compte le contexte humain, à la fois politique et social, dans lequel elles s'insèrent tant en amont qu'en aval. Au niveau politique, les représentations des décideurs, tant vis-à-vis des technologies que vis-à-vis des besoins opérationnels des armées, et les relations qu'ils entretiennent avec les acteurs industriels, peuvent ainsi fortement influer sur les politiques de « technologisation » et les programmes mis en place. Au niveau social, les pratiques des utilisateurs, soldats et officiers, sont également importantes à prendre en considération car elles peuvent avoir des impacts forts sur l'effectivité de ces nouveaux instruments sur le terrain. En effet, au-delà des questions d'ergonomie qui sont souvent prises en compte par les industriels, la réception et l'usage de ces outils dépend aussi de la manière dont ils ont été présentés et introduits dans les routines et les procédures des agents. L'outil peut sembler très pertinent dans ces caractéristiques techniques, mais faire l'objet d'un rejet (manque de formation des agents, changement d'habitudes mal acceptées, stress face aux transformations opérationnelles, etc.) qui rende son usage *in fine* handicapant sur le terrain. Enfin, la sociologie des sciences, avec en particulier la formulation de la notion d'acteur-réseau, nous invite à considérer l'introduction de ces technologies, au travers de l'ensemble de la chaîne d'acteurs, industriels, politiques et militaires, qui la rend possible, la conforte ou la critique. Ces outils techniques, objets de controverses éthiques ou scientifiques, de débats, relevant d'intérêts divers (économiques, stratégiques, politiques, etc.), modifient en profondeur les relations entre les acteurs de cette chaîne (relations public/privé, mode de fonctionnement au sein des organisations, entre autres).

[4] Pour une bonne synthèse de cette littérature, voir Grissom, 2015 ; Schmitt, 2018.

Aussi, les anomalies et les dysfonctionnements émergents peuvent ne pas être d'ordre technique (l'outil fonctionne) mais d'ordre sociotechnique (blocage au sein de la chaîne d'acteur). Ils peuvent tout aussi bien produire de nouveaux comportements, induits par cette dynamique de numérisation, mais non prévue par l'ingénieur et l'acteur industriel. Par conséquent, l'enjeu central consiste à comprendre comme s'opèrent des compromis continuels entre la recherche de l'efficacité militaire d'une part, la gestion des menaces et des risques d'autre part[5]. A l'heure où la modernisation des forces armées est définie comme un impératif au niveau politique et où la numérisation se déploie à travers le programme SCORPION (Synergie du contact renforcée par la polyvalence et l'infovalorisation) de l'armée de Terre (L'Obs, 2018), cet article propose deux apports. Il s'agit en premier lieu de préciser les contours de la « numérisation du champ de bataille » afin de guider les réflexions institutionnelles. En second lieu, nous souhaitons montrer comment les avantages attendus ou la limitation des risques et des menaces dépendent de choix et d'une appréciation souple des effets de la numérisation. Le « 5ème domaine de la guerre » ne peut ainsi être cloisonné aux seules opérations militaires.

Notre contribution procédera en deux temps. Elle propose tout d'abord d'analyser les deux éléments constitutifs de la numérisation, à savoir la mise en donnée et la mise en réseau, afin d'en éclairer les logiques et de montrer les représentations et les débats que ces deux phénomènes suscitent. Elle s'attachera ensuite à mettre en lumière les enjeux de la numérisation en matière d'appréhension et de gestion de la complexité par deux études de cas.

Mise en données et mise en réseau : la numérisation de l'espace de bataille en question

En premier lieu, il est important de revenir sur ce que sous-tend le processus de numérisation - à savoir l'association d'une mise en données de l'objet numérisé et d'une mise en réseau de ces données - chacune de ces étapes demandant une réflexion critique préalable quant à la nature de ces actions. En effet, distinguer la mise en données et la mise en réseau permet de dissocier deux ensembles de représentations qui sont ici confondues et se confortent. La mise en données est un processus assez ancien. Viktor Mayer-Schönberger et Keneth Cukier rappellent que ce terme de « données », au sens de « fait », était déjà le titre d'un ouvrage d'Euclide, dans lequel celui-ci s'appliquait à expliquer la géométrie à partir de ce qui était connu et attesté comme tel (Mayer-Schönberger et Cukier, 2014 : 96). Or, ce processus s'inscrit souvent dans une conception naturaliste qui voit dans la donnée un simple reflet objectif de la réalité, alors même que celle-ci est d'abord une construction sociale, impliquant des dimensions politiques, stratégiques,

[5] Une bonne synthèse de ce thème émergent de la recherche se trouve dans le volume dirigé par Reiter, 2017.

économiques, éthiques, entre autres. Aussi, l'idée que l'accumulation de données pourrait, à elle-seule, constituer un avantage décisif sur l'adversaire, est erronée. De la même manière, la notion de réseau a fait l'objet de nombreux débats dans les cercles stratégiques, qui ont souvent aboutit à surévaluer les atouts de la « connexion du champ de bataille », en sous-évaluant (ou en éludant) les vulnérabilités ainsi générées. On comprend donc aisément en quoi la numérisation, qui implique à la fois mise en données et mise en réseau, peut susciter de l'intérêt, voire de l'enthousiasme. Entendons-nous bien, notre objet n'est pas ici de mettre en doute les apports de ces technologies sur le terrain, mais d'inciter à une analyse critique, qui nécessite donc de distinguer ces deux processus et leurs implications.

Concernant *la mise en données*, penser que les débats autour des données et de leurs traitements sont nouveaux, c'est oublier que chaque époque a vu l'émergence de ses propres technologies pour les valoriser. Mais le sens du mot « donnée » a progressivement évolué pour désigner un fait qui se laisse enregistrer, analyser et réorganiser. En ce sens, la donnée représente la transcription d'un phénomène en un certain nombre de chiffres qui vont pouvoir être organisés et analysés. Mayer-Schönberger et Cukier proposent le terme de « mise en données ». Ils rendent compte ainsi du processus de construction qui permet de générer des données. Ce processus de mise en données a pris une dimension particulière au XIXe siècle, avec la révolution industrielle, et plus encore avec l'émergence et la prolifération des données numériques. Celles-ci ont en effet pris une importance particulière du fait de leur multiplication exponentielle, sans précédent dans l'histoire. Néanmoins, quel que soit leur nombre, et l'augmentation en parallèle des capacités de traitement, celles-ci n'en sont pas moins des éléments construits qui doivent faire l'objet de critique.

Ainsi, une définition plus aboutie de la donnée amène à remettre en cause l'image intuitive d'une « donnée brute » objective et neutre, reflet fidèle de réalité extérieure. Comme le suggère Bruno Latour : « *La tentation de l'idéalisme vient peut-être du mot même de données qui décrit aussi mal que possible ce sur quoi s'appliquent les capacités cognitives ordinaires des érudits, des savants et des intellectuels. Il faudrait remplacer ce terme par celui beaucoup plus réaliste,* d'obtenues *et parler par conséquent de* base d'obtenues*, de* sublata *plutôt que de* data *pour parler à la fois latin et anglais* » (Latour, 2007 : 609). La donnée est donc en soi le produit d'une démarche intellectuelle, le résultat d'un processus, le fruit d'une stratégie déjà à l'œuvre en amont. En ce sens, les sociologues Gilles Bastin et Jean-Marc Francony avancent une comparaison pertinente entre les processus de production de données (ou *datafication*) et ceux de production de faits (ou *factualisation*) dans la sociologie spontanée, qu'ils qualifient « d'illusion de la transparence » (Bastin & Francony, 2016).

Dans les deux cas, *faits* et *données* sont issus d'un processus de production, qui révèle beaucoup de son auteur, de ses représentations et de ses objectifs, ainsi que du contexte technique, politique, économique, social, philosophique dans lequel il s'inscrit.

Les données ne peuvent donc pas être considérées comme des éléments bruts et objectifs, mais participent d'un processus dialectique de production de connaissances, dans lequel elles interagissent avec l'information et le savoir pour orienter la prise de décision finale. Dans le même temps, la décision est également au cœur et en amont de l'ensemble de cette dynamique. Elle intervient sur le processus de production des données (quelles données rechercher ? pour quel objectif ? par quelle méthode de collecte l'obtenir ? avec quel matériel ? etc.), ainsi que sur celui de production de l'information (quelle hiérarchie pour les données ? quelle méthodologie d'assemblage ? etc.), de production du savoir et de l'intelligence (travail d'abstraction et d'application relevant de choix épistémologiques, méthodologiques, etc.).

Or, ce processus décisionnel, qui est nécessaire dans la création et le traitement des données, qu'il soit conscient ou non, renvoie plus largement à ce que Rob Kitchin appelle « l'assemblage sociotechnique des données ». Il précise : « *Cet assemblage des données est composé de nombreux dispositifs et éléments qui sont étroitement liés, se développent et se transforment dans le temps et dans l'espace* » (Kitchin, 2014 : 24). Les données sont *in fine* le fruit de l'articulation de différentes dimensions sociales, économiques, politiques, culturelles, techniques (cf. tab. 1).

Attributs	**Éléments**
Système de pensée	Modes de pensée, philosophies, théories, modèles, idéologies, rationalités, etc
Formes de connaissances	Textes de recherche, manuels, magazines, sites web, expérience, bouche à oreille, forums de discussion, etc.
Finance	Modèles d'affaires, investissement, capital-risque, subventions, philanthropie, bénéfices, etc.
Economie politique	Politique, régimes fiscaux, opinion publique et politique, considérations éthiques, etc.
Gouvernementalités & légalités	Normes de données, formats de fichiers, exigences du système, protocoles, règlements, lois, licences, régimes de propriété intellectuelle, etc.

Matérialités & infrastructures	Papiers / stylos, ordinateurs, appareils numériques, capteurs, scanners, bases de données, réseaux, serveurs, etc.
Pratiques	Techniques, manière de faire, comportements acquis, conventions scientifiques, etc.
Organisations & institutions	Archives, sociétés, consultants, fabricants, détaillants, agences gouvernementales, universités, conférences, clubs et sociétés, comités et conseils, communautés de pratiques, etc.
Subjectivités & communautés	Des producteurs de données, des conservateurs, des gestionnaires, des analystes, des scientifiques, des politiciens, des utilisateurs, des scientifiques, etc.
Lieux	Labs, bureaux, sites de terrain, centres de données, fermes de serveurs, parcs d'affaires, etc., et leurs agglomérations.
Marché	Pour les données, ses dérivées (e.g. : texte, tableaux, graphiques, cartes), analyses, logiciels analytiques, interprétations, etc.

Tableau 1 – Les éléments sociotechniques de l'assemblage des données (Kitchin, 2014, p.25)

Concernant *la mise en réseau*, elle permet à la fois l'échange de données, leur diffusion, leur collecte, et *in fine* une certaine centralisation et valorisation. La centralisation du commandement transparaît à travers la datafication du champ de bataille. Elle engendre une segmentation et une spécialisation du traitement, de l'analyse et de la mise en forme des données au profit de l'échelon décisionnel, ce qui induit une bureaucratisation accrue. Dans le même temps, la multiplication des sources de données, des capteurs intégrés à divers systèmes d'armes, pour partie autonomes, doit nous interpeller. Différents types de données et de réseaux sont ainsi générés, qui font apparaître un système polymorphe de communication. Dans ces systèmes, les données deviennent des intermédiaires, impliquant tout un jeu de relations complexes homme/homme (relation hiérarchique, échange informationnel entre terrain et centre de commandement), homme/machine (traitement algorithmique des données, outil d'aide à la décision), voire même machine/machine (véhicules autonomes). Ainsi, dans les cas où la machine intervient dans le réseau, l'algorithme devient un élément essentiel de la décision finale.

Or, d'un point de vue éthique, comment prendre une décision aussi lourde que celle qui engagera la vie d'hommes et de femmes sur le terrain, par le prisme d'un mécanisme algorithmique dont on ignore les principes et les limites. Le champ de bataille mis en données et mis en réseau, s'il ouvre tout une gamme de nouvelles possibilités, nous amène à considérer l'ensemble de ces implications opérationnelles (quid des relations entre les hommes sur le terrain et le commandement ?), politiques (quid du décideur politique dans le déroulé des opérations ?), juridique (en quoi cette nouvelle chaîne de commandement perturbe la hiérarchie des responsabilités ?) et éthiques (quelle confiance accordée aux algorithmes ? quelle part d'autonomie pour les systèmes d'armes, les systèmes d'information et de communication, les systèmes de commandement ?). D'où de multiples interrogations : comment prendre une décision humaine face au flot d'information en temps réel qui circulent dans le réseau ? Celle des temporalités pourrait également être ajoutée. La gestion des données numériques implique en effet un bouleversement temporel majeur pour les décideurs : celui d'avoir à agir sur la base d'informations communiquées en temps réel. Quelles conséquences ce renforcement soudain d'une connaissance « instantanée » peut-elle bien avoir sur des constructions et des interactions sociales dont les échelles de temps sont toujours plus longues (temps court, moyen, long) ? Autre question : quel est le seuil d'obsolescence d'une donnée produite « en temps réel » ? En quoi l'analyse différée de données systématiquement périmées peut-elle rester pertinente ? Devons-nous détruire ces données après un certain temps, ou les conserver ? Mais alors, avec quels coûts et/ou pour quels usages ? Ne pas s'interroger sur ces différentes problématiques peut être lourd de conséquences pour les acteurs militaires. Ainsi, Charles J. Dunlap, Jr. évoque l'une des impacts possibles de la numérisation du champ de bataille pour les forces à travers le processus qu'il appelle « hyperpersonnalisation de la guerre » (Dunlap, Jr., 2014). Cette hyperpersonnalisation suppose que les soldats puissent être identifiés individuellement au combat, via leurs données sur les réseaux publics ou privés. Or, ce phénomène a déjà provoqué d'importantes vulnérabilités dans des cadres opérationnels qui méritent d'être évoquées, tant d'un point de vue social que stratégique (possibilité de privilégier des cibles-clefs dans le combat, fragilisation de la psychologie des forces en tant que tout, identification des combattants et menaces sur leur famille et leurs proches, etc.). Ainsi, le processus de numérisation est intimement lié à la question de la complexité des conflits mais aussi du combat. Si d'une part, il s'agit de tirer parti de cette complexité pour accroître l'efficacité militaire, la numérisation s'impose également aux individus et aux organisations en raison de ses propriétés émergentes et des effets non-linéaires qu'elle produit. Deux études de cas nous permettent de mieux en délimiter les impacts en interrogeant l'interaction entre les usages et les développements sociotechniques.

Commander et combattre dans la complexité : la 1ère division de cavalerie américaine en Irak (2004)

Déployée à Bagdad après la chute de Saddam Hussein, la 1ère division de cavalerie (1st Cav) est l'une des premières unités numérisées de l'US Army. Sous l'impulsion de son commandant, le général Peter Chiarelli, ses officiers mettent en oeuvre des outils permettant d'améliorer la connaissance de la zone d'opérations afin d'augmenter l'efficacité dans la planification et la conduite des opérations de contre-insurrection. Caroline Croser a mené une enquête ethnographique au sein de cette unité afin d'analyser les usages du *Command Post of the Future* (CPOF) (Croser, 2006 ; Croser, 2007b). Le CPOF est une suite logicielle et une interface utilisateur fonctionnant sous Windows qui se présente sous deux aspects. En premier lieu, il s'agit d'un système de représentation géographique permettant de compiler, de croiser et de rafraîchir des données diverses provenant des capteurs électroniques (comme le système *Blue Force Tracking* permettant de localiser les unités amies) aussi bien que de sources humaines ou administratives à des échelles modulables (du pâté de maison à l'ensemble de l'agglomération de Bagdad). Sous ce premier aspect de mise en données de la zone d'opération, le CPOF opère comme un outil d'aide à la compréhension et à la décision dans la mesure où il permet d'objectiver la complexité et l'incertitude du conflit contemporain et de corréler une base de données d'actes significatifs (*Significant Activity Reports* - SIGACTS) avec des données globales portant sur l'économie, les infrastructures, la composition sociale, etc. En ce sens, il se veut aussi un outil d'élucidation de schémas d'action voire de prédiction (Gregory, 2010 : 269). En second lieu, le CPOF est une plate-forme collaborative comprenant des outils de partage et de communication (à la voix comme par email). Durant le déploiement de 2004, les officiers de la 1st Cav ont utilisé cette fonction afin de mieux coordonner la planification et la conduite des opérations entre les différents secteurs d'activité des brigades de la division. Sous cet aspect, le CPOF est un outil de commandement et de contrôle dans la mesure où il s'est révélé être le moyen par lequel le général Chiarelli s'assurait de l'unité d'action au sein de son unité (Croser, 2006 : 199), mais il est également un outil collaboratif permettant une action simultanée bien que séparée.

D'un côté en effet, les officiers commandant les brigades avaient l'initiative quant à l'usage de l'outil et au partage des éléments avec leurs pairs, de l'autre les données étaient collectées et centralisées par un officier du centre d'opérations. Caroline Croser conclut son enquête sur deux observations. La première concerne le rapport à l'outil cartographique : celui-ci devient le premier filtre par lequel le champ de bataille est appréhendé comme un système fluide, incomplet et constamment mis à jour. Par conséquent, l'utilisateur doit gérer le rythme mais aussi l'incertitude qui découle de la complexité (*Ibid.* : 200).

La seconde concerne l'utilisation de l'outil selon le contexte opérationnel : alors que les périodes de calme se caractérisent par une planification pro-active, les regains de violence produisent un retour à la planification et à la conduite en réaction à des événements (*Ibid.* : 201).

Les enseignements tirés de cette étude de cas importent dans la mesure où la numérisation est conçue comme un moyen d'organiser voire de réduire la complexité du champ de bataille. À ce titre, les usages nous renseignent également sur les vulnérabilités et les compromis à opérer dans l'intégration des outils numériques au coeur des opérations. Le programme SCORPION de l'Armée de Terre définit ainsi les avantages attendus d'un unique système d'information et de communication : « *partage de l'information, combat collaboratif (accélération de l'action au combat) et optimisation de la préparation opérationnelle (simulation embarquée)* » (Armée de Terre, 2017). Mise en données du champ de bataille et mise en réseau des forces armées doivent ainsi permettre d'améliorer la coordination entre les unités, l'intégration de leurs actions locales à l'ensemble de la manœuvre globale et l'adaptation aux changements dynamiques du combat.

Les expérimentations menées par le Commandement des Opérations Interarmées (CPOIA) dans le domaine du commandement soulignent cependant une appréciation nuancée des apports de la numérisation. Du côté des atouts confirmés : l'amélioration du partage de la situation opérationnelle entre les niveaux tactique et stratégique, le renforcement du principe de subsidiarité et l'aide accrue aux processus de ciblage et de renseignement. L'étude semble mettre en lumière des risques et vulnérabilités liées à l'excès d'informations inutilisées et au défaut d'intégration des informations en raison d'un cloisonnement de ces dernières selon des logiques organisationnelles (EMA, 2018). En d'autres termes, l'enjeu central est celui de la structure que doivent adopter les organisations afin d'équilibrer les impératifs d'adaptation et d'unité d'action. Une structure décentralisée voire réticulaire apporte des avantages quant au premier mais impose des risques quant au second alors qu'une structure hiérarchique favorise ce dernier par rapport au premier. Comme le montre Didier Danet (2015), dans certaines configurations dominées par le leadership transactionnel, la mise en réseau et la mise en données favorisent un pouvoir de structuration plus fort et un leadership fondé sur le contrôle des subordonnés.

Parallèlement, les processus de numérisation suggèrent des possibilités croissantes de circulation horizontale des informations et imposent donc des adaptations structurelles et continuelles afin de conserver le niveau de performance. Dans les organisations ayant opté pour le leadership transformationnel, ces mêmes processus offrent une opportunité aux décideurs comme aux subordonnés de développer des innovations propres à augmenter l'efficacité opérationnelle (Fig.1 ci-après).

	Personnalité	Comportement	Contingence	Transformationnel
Définition Les leaders sont identifiés par	Des qualités et caractéristiques personnelles (openness, conscientiousness, extraversion, agreeableness, neuroticism)	Des comportements spécifiques articulés autour de l'intérêt préférentiel pour la production ou pour les hommes	La combinaison d'un style de leadership (comportement) et de variables caractérisant l'environnement (relations leader/membres, structuration des tâches, pouvoir hiérarchique)	L'influence exercée sur les subordonnés pour qu'ils transcendent leurs intérêts personnels au profit des buts de l'organisation.
Auteurs	Tupes et Christal	Blake et Mouton	FIedler	Bass
Rôle du cyber	Affecte à la marge Openness et Extraversion	Renforce les capacités de structuration	Modifie l'adéquation entre le style de leadership et les variables environnementales	
Impact	Faible	Moyen	Fort mais conditionnel	Fort et partagé
Opportunités	Occasion de faire valoir certains traits (ouverture aux idées nouvelles)	renforcement de la direction et du contrôle des équipes	Renforce l'efficacité de la structuration si les relations sont bonnes entre leader et subordonnés	Offre de nouvelles possibilités de stimulation intellectuelle et de considération personnelle
Menaces	Mise à l'épreuve de la capacité à gérer le changement	Circulation d'informations entre subordonnés (réseaux sociaux)	Impose une adaptation du style de leadership pour conserver le niveau de performance	Aucune

Fig.1: l'impact différenciée de la numérisation sur les organisations selon les modes de leadership (Danet, 2015:49)

Dans le cas des organisations militaires, la disponibilité plus importante des informations et leur fusion au niveau du chef pourraient plutôt renforcer la centralisation technologique du commandement et du contrôle. Comme le notait Milan Vego (2003), « *avoir une 'Common Operational Picture' pourrait conduire les décideurs à s'impliquer davantage dans des décisions purement tactiques au lieu de se focaliser sur les aspects opératifs et stratégiques propres à leur niveau de responsabilités* ». Deux risques en découleraient : d'une part, l'accroissement de la complexité dans la gestion des informations, d'autre part, le risque de paralysie en cas de décapitation ou d'indisponibilité des réseaux d'échanges d'information.

Les solutions retenues autour du développement d'un *cloud* de Défense permettent partiellement de pallier ces risques et d'accroître l'efficacité stratégique comme opérationnelle. Elles prennent notamment en compte la nécessité de centraliser le traitement des données dans un contexte opérationnel où la bande passante reste limitée. Néanmoins, persistent les risques d'hypercentralisation et de dépendance excessive aux données numériques (Bômont, 2017). Commander dans la complexité nécessite donc d'accepter la part d'incertitude qui en découle et d'encourager une part d'innovation.

Au sein de la 1st Cav, s'établit ainsi un système de partage des enseignements et des retours d'expérience selon des logiques horizontales en profitant de l'opportunité ouverte par le Web 2.0 (forums de discussion). Le réseau CAVNET - dont la raison sociale est de « se préparer à la prochaine patrouille, pas à la prochaine guerre » - hébergé sur le réseau sécurisé SIPRnet, aurait ainsi permis une adaptation plus rapide aux réalités du combat contemporain (PBS, 2005).

Défense et vulnérabilité en profondeur des organisations militaires face aux propriétés émergentes : l'application STRAVA

Le domaine numérique se caractérise par la manière dont il imprègne la vie sociale, collective autant qu'individuelle, selon des logiques non-linéaires et distribuées. Cette complexification croissante dessine les contours d'une numérisation subie du champ de bataille. Le 27 janvier 2018, un jeune étudiant australien nommé Nathan Ruser analyse la carte globale créée par l'application sportive STRAVA à partir du partage des données de ses utilisateurs. Sa découverte devient rapidement virale : les parcours de certains utilisateurs réguliers laissent apparaître la localisation de certaines emprises militaires, connues ou plus discrètes (Adam, 2018 ; Manac'h, 2018a). Dès lors, les organisations militaires rappellent les consignes de sécurité au sujet de ces applications utilisation la géolocalisation pour enregistrer et partager les performances sportives (Tual, 2018 ; Berlinger et Vazquez, 2018). Cet « effet de bord » souligne d'une part l'impact des technologies et usages civils sur les organisations militaires mais aussi l'importance de la vie numérique des combattants (DFRLab, 2018). Ainsi, le journaliste Jean-Marc Manac'h parvient-il à identifier plusieurs agents de la Direction Générale de la Sécurité Extérieure (DGSE) et de la Direction Générale de la Sécurité Intérieure (DGSI) par un travail d'enquête en sources ouvertes et à partir des données fournies par STRAVA. Non seulement car ces derniers semblent avoir parfois oublié de désactiver la géolocalisation lorsqu'ils utilisaient l'application en mission et à leur domicile, parce qu'ils ont alterné l'usage de pseudos avec celui de leur véritable nom, mais aussi en raison des croisements possibles entre les données issues de plusieurs médias ou applications en ligne (cartographiques, photographiques, etc.) et les données administratives (adresse, annuaire téléphonique, etc.) (L'Express, 2018 ; Manac'h, 2018b).

De fait, le danger posé par l'utilisation d'appareils géolocalisés en opération n'est pas neuf (LiveScience, 2012). En revanche, il éclaire à quel point le processus de numérisation invite à penser toutes les porosités. C'est le cas concernant le brouillage entre les différentes dimensions de la vie du combattant : sur le terrain, au quartier ou dans sa vie privée. Cela se traduit dans les menaces émanant des usages émergents des médias sociaux : lorsqu'un groupe de hackers se réclamant du « Cyber Califat » pirate le compte Twitter du *Central Command* américain en janvier 2015, il s'empresse de publier une liste d'officiers généraux américains avec leurs coordonnées

personnelles, transformant leurs proches en cibles potentielles (Gombert & Libicki, 2015). Même si ces données sont accessibles via des recherches en sources ouvertes, elles témoignent de la vulnérabilité induite par la vie numérique des militaires dans la mesure où certains réseaux deviennent des cibles potentielles pour des action de renseignement (Linkedin étant un exemple possible dans la mesure où y apparaissent en filigrane les organigrammes de nombreuses organisations).

Néanmoins, les distinctions entre ces divers aspects de la vie du combattant individuel ressurgissent dès lors que l'on mesure le degré de vulnérabilité découlant des usages ou de l'exposition aux médias sociaux. Ainsi, la régulation institutionnelle permet de mieux gérer les risques sur le terrain ou au quartier, mais moins en ce qui concerne la vie privée numérique des combattants qui devient le talon d'Achille des organisations. Car il est nécessaire de prendre également en compte la profondeur historique de l'empreinte numérique laissée par les individus. En l'absence d'un droit à l'oubli généralisé, l'archive numérique est une vulnérabilité supplémentaire pour les individus comme pour les organisations. D'autant plus que les principaux médias sociaux atteignent leur première décennie d'existence et basent une partie de leur modèle économique sur la monétisation des données de leurs utilisateurs. Comme l'illustre l'affaire posée par *Cambridge Analytica*, celles-ci peuvent être exploitées y compris sans que la plate-forme numérique n'y consente ou ne le sache (Grasseger & Krogerus, 2017).

La complexification croissante résultant de ce processus de numérisation que subissent les organisations militaires invite à repenser leur sécurité opérationnelle et leurs vulnérabilités en termes de défense en profondeur. Dans cette optique, les usages induits par la connexion croissante des individus et l'épaisseur de leur vie numérique imposent des compromis en matière de sécurisation. S'il semble possible d'augmenter la sécurité dans la dimension professionnelle de l'activité militaire, les données privées des militaires se prêtent davantage à une approche en termes de gestion des risques. D'une part, la révélation publique de ces failles produit des incitations positives pour les entreprises numériques à sécuriser davantage les données.

Dès le mois de février, STRAVA a ouvert la possibilité à ses utilisateurs de déconnecter plus facilement la géolocalisation de leurs données (Lausson, 2018). Reste néanmoins la question des options de partage et des autorisations données par l'utilisateur lorsqu'il installe ces applications : celle-ci relève d'un côté du développeur (lisibilité des options, réduction du volume parfois kilométrique des contrats d'utilisateurs finaux) et de l'autre de l'individu ou de l'organisation militaire (hygiène personnelle, règlements de sécurité).

D'autre part, la mise en place sur les médias sociaux de mesures visant à tromper les algorithmes de collecte et de traitement des données privées par ces derniers peuvent contribuer à mieux cloisonner les différentes dimensions de la vie du combattant (Rogers, 2018). Semer la confusion peut très bien relever d'une stratégie personnelle de gestion de sa vie numérique par l'individu appartenant aux organisations militaires, mais peut également dépendre des mesures de sensibilisation, voire de formation aux usages numériques, développées en leur sein. Néanmoins, plusieurs éléments peuvent faire obstacle à cette approche. En premier lieu, la prédominance des structures hiérarchiques se marie difficilement avec l'incitation à la prise d'initiative par les échelons subordonnées. Ce point est étroitement dépendant du style de leadership favorisé au sein de l'institution et de la personnalité de certains décideurs. En second lieu, le cloisonnement entre les tâches liées au « cœur de métier » et celles dont dépendent la sécurité personnelle de l'individu dans l'organisation peuvent gêner la prise de conscience d'un enjeu crucial : les séances de sensibilisation tendent donc à la loi des rendements décroissants au fur et à mesure de leur répétition. Enfin, la confusion entre la socialisation et l'apprentissage de procédures routinières standards peut empêcher l'intériorisation de bonnes pratiques et maintenir ce cloisonnement. Surmonter ou prendre en compte les compromis induits par ces processus est ainsi nécessaire au développement d'une défense en profondeur dont l'individu est la clé.

Conclusion

Cette analyse rapide des contours et des enjeux des processus de numérisation dans le champ de la conflictualité invite à repenser les représentations au sujet de sa complexité et des moyens d'y faire face. Les travaux au sujet des forces armées américaines ont bien souligné l'imprégnation précoce des sciences de la complexité dans la pensée stratégique (Lawson, 2011 ; Lawson, 2013). Néanmoins, deux limites ont été soulignées. D'une part, il persiste un décalage entre une conception embrassant cette approche et une structure organisationnelle hiérarchique (Niva, 2013). De l'autre, demeure prégnante une vision orientée par les représentations cybernétiques, c'est à dire par la volonté d'imposer de l'ordre dans le chaos de la guerre par le contrôle et la maîtrise de l'information (Bousquet, 2009 : 233-234).

Le processus croisant mise en données et mise en réseau selon des logiques non-linéaires et distribuées rend d'autant plus crucial une approche embrassant la complexité dans toutes ses dimensions. Cette étude nous invite aussi à repenser les limites traditionnellement associées au champ de bataille et aux modes organisationnels militaires. Plus qu'une porosité entre « arrière » et « front », ce processus accentue le décloisonnement entre zone de guerre, spécifiquement militaire, et zone de paix, plutôt civile. Nous ne pouvons donc plus penser la notion de théâtre

d'opération comme Clausewitz, qui évoquait "une partie du territoire en état de guerre, telle qu'elle soit protégée et couverte sur ses côtés, de manière à constituer en quelque sorte à elle seule une portion indépendante de territoire » (Clausewitz, 1886). L'idée d'un territoire clos, fermé sur lui-même, déjà érodée par les pratiques terroristes, est rendue définitivement obsolète dans ce processus de numérisation[6]. Il en va de même du découpage organisationnel entre les domaines terrestres, maritimes et aériens - qui, au-delà des simples aspects géographiques, correspond à toute une division bureaucratique de l'action militaire, fruit d'une construction historique et politique. Or, le domaine numérique est un domaine englobant, qui ne s'inscrit pas dans ces distinctions organisationnelles. Bien plus, le processus de numérisation programmé sous-tend la fusion des données et des réseaux entre « capteurs » et « effecteurs », quelle que soit leur appartenance bureaucratique. Il pourrait donc contribuer à l'accentuation des tensions pesant sur les frontières entre les armées, voire entre tous les acteurs du secteur de sécurité.

Aussi, notre réflexion sur la numérisation du champ de bataille montre que cette dynamique invite en réalité le stratège à reformuler l'ensemble des périmètres opérationnels des décideurs dans la guerre : quelle sera la place du chef militaire face au décideur civil? Comment organiser les interactions entre les acteurs combattants? Et comment définir l'acteur combattant lui-même? Le champ est immense et doit être interrogé, en parallèle des travaux sur les problèmes techniques et juridiques, qui restent bien évidemment tout aussi essentiels.

Bibliographie

Adam, Louis (2018), « Strava : les montres connectées inquiètent les militaires », *ZDNet*, 30.01.2018, en ligne: http://www.zdnet.fr/actualites/strava-les-montres-connectees-inquietent-les-militaires-39863380.htm (accédé le 28.03.2018).

Arquilla David et Ronfeldt (1993), « Cyberwar is Coming », *Comparative Strategy*, vol.12, n°2, pp.141-165.

Armée de Terre (2017), « Scorpion: présentation », 6.07.2017, en ligne: https://www.defense.gouv.fr/terre/equipements/a-venir/scorpion/presentation (accédé le 27.03.2018).

Bastin Gilles & Jean-Marc Francony (2016), « L'inscription, le masque et la donnée. Datafication du web et conflits d'interprétation autour des données dans un laboratoire invisible des sciences sociales », *Revue d'anthropologie des connaissances*, 2016/4, vol.10, pp.505-530

Berlinger, Joshua et Vazquez, Maegan (2018), « US military reviewing security practices after fitness app reveals sensitive info », *CNN*, 29.01.2018, en ligne: https://edition.cnn.com/2018/01/28/politics/strava-military-bases-location/index.html (accédé le 28.03.2018).

[6] Pourtant, il s'agit de la conception encore en vigueur au sein du département de la Défense des Etats-Unis (Département de la Défense, 2016: 242.

Bômont, Clotilde (2017), « Résilience des SIC militaires: cloud défense et hyperconnectivité des théâtres d'opérations », *Revue de la gendarmerie nationale*, 4ème trimestre, pp.39-45.

Bousquet, Antoine (2009), *The Scientific Way of Warfare: Order and Chaos on the Battlefield of Modernity*, Londres: Hurst&Co.

Boyd, John R. (1976), *Destruction and Creation*, U.S. Army Command and General Staff College, 3 septembre 1976, en ligne: http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf (accédé le 26.03.2018).

Carr, Jeffrey (2017), « The GRU-Ukraine Artillery Hack That May Never Have Happened », *Medium*, 3.01.2017, en ligne: https://medium.com/@REEL_ICO_TALK/the-gru-ukraine-artillery-hack-that-may-never-have-happened-820960bbb02d (accédé le 26.03.2018).

Cebrowski, Arthur K. et Gartska, John J., « Network-centric Warfare: Its Origins and Future », *Proceedings Magazine*, 124/1, janvier 1998, pp.11-39.

Chiarelli, Peter W. et Michaelis, Patrick R., (2005), « Winning the Peace: the Requirement for Full-Spectrum Operations », *Military Review*, vol. LXXXV, n°4, juillet-août, pp.4-17.

Croser, Caroline (2006), « Commanding the Future: Command and Control in A Networked Environment », *Defense and Security Analysis*, 22, 2, pp.197-202.

Croser, Caroline, (2007a), « Organising Complexity: Modes of Behaviour in A Networked Battlespace », *Land Warfare Studies Center Working Paper*, 133.

Croser, Caroline (2007b), « Networking Security in the Space of the City: Event-Ful Battlespaces and the Contingency of the Encounter », *Theory and Event,* 10, 2

Crowdstrike (2016), « Use of Fancy Bear Android malware in tracking of Ukrainian field artillery units », 22.12.2016, en ligne: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf (accédé le 25.02.2018).

Danet, Didier (2015), « Cyberwar et leadership (1ère partie) », *Défense et Sécurité internationale*, 110, janvier, pp.46-50.

Département de la Défense (2016), *JP 1-02 Department of Defense Dictionary of Military and Associated Terms*, en ligne: https://fas.org/irp/doddir/dod/jp1_02.pdf (accédé le 02.04.2018).

DFRLab (2018), « Data and Defense: the Case of Strava », *Medium*, 2.02.2018, en ligne: https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2 (accédé le 28.03.2018).

Dunlap Jr., C. J. (2014), « The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict », *Georgetown Journal of International Affairs*, 15, International Engagement on Cyber IV, pp. 108–118.

Etat-Major des Armées (2018), « Numérisation du commandement des opérations interarmées: vaincre par l'anticipation technologique », 20.03.2018, en ligne: https://www.defense.gouv.fr/ema/transformation/actualites/vaincre-par-l-anticipation-technologique (accédé le 28.03.2018).

Gombert, David et Libicki, Martin C., « Decoding the Breach: the Truth About the CENTCOM Hack », *The RandBlog*, 03.02.2015, en ligne: https://www.rand.org/blog/2015/02/decoding-the-breach-the-truth-about-the-centcom-hack.html (accédé le 28.03.2018).

Grasseger, Hannes et Krogerus, Mikael (2017), « The Data That Turned the World Upside Down », *Motherboard*, 28.01.2017, en ligne: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win (consulté le 28.03.2018).

Gregory, Derek (2010), « Seeing Red: Baghad and the Event-Ful City », *Political Geography*, 29, pp.266-279.

Grissom, Adam (2015), « Innovation et adaptation », in Henrotin, Joseph, Schmitt, Olivier et Taillat, Stéphane (dirs.), *Guerre et stratégie: approches, concepts*, Paris: PUF, pp.351-377.

Guibert, Nathalie (2018), « Comment l'Otan se prépare aux guerres du futur », *Le Monde*, 30.03.2018, en ligne: http://www.lemonde.fr/europe/article/2018/03/30/pour-la-guerre-de-demain-la-ressource-strategique-est-la-donnee_5278849_3214.html (accédé le 31.03.2018)

Henrotin, Joseph (2008), *La technologisation militaire en question : le cas américain*, Paris: Economica.

Kitchin, Rob (2014), *The Data Revolution*, Sage, Londres

Latour, Bruno (2007), « Pensée retenue, pensée distribuée », in *Lieux de savoir, I*, Christian Jacob (dir.), Paris, Albin Michel

Lausson, Julien (2018), « L'application de sport Strava simplifie la désactivation du partage de données », *Numérama*, 02.03.2018, en ligne: https://www.numerama.com/tech/333171-lapplication-de-sport-strava-simplifie-la-desactivation-du-partage-de-donnees.html (accédé le 25.03.2018)

Lawson, Sean (2011), « Cold War military systems science and the emergence of a nonlinear view of war in the US military », *Cold War History*, 11, 3, Août, pp.421-440.

Lawson, Sean (2013), *Nonlinear Science and Warfare: Chaos, complexity and the U.S. military in the information age*, Londres: Routledge.

L'Express (2018), « Des espions de la DGSE identifiés à cause de l'appli sportive Strava », 22.02.2018, en ligne: https://lexpansion.lexpress.fr/high-tech/des-espions-de-la-dgse-identifies-a-cause-de-l-appli-sportive-strava_1987031.html (accédé le 28.03.2018)

Livescience (2012), « Insurgents Destroyed US Helicopters Found in Online Photos », *LiveScience*, 16.03.2012, en ligne: https://www.livescience.com/19114-military-social-media-geotags.html (accédé le 28.03.2018).

L'Obs (2018), « Macron à Mourmelon salue la modernisation de l'armée de Terre », 1.03.2018, en ligne : https://www.nouvelobs.com/politique/20180301.AFP6955/macron-a-mourmelon-salue-la-modernisation-de-l-armee-de-terre.html (accédé le 27.03.2018).

Manac'h, Jean-Marc (2018a), « Appli: ces militaires bretons que l'on peut suivre à la trace », *Le Télégramme*, 28.02.2018, en ligne: http://www.letelegramme.fr/france/appli-ces-militaires-bretons-qu-on-peut-suivre-a-la-trace-28-02-2018-11870265.php (accédé le 31.03.2018).

Manac'h, Jean-Marc (2018b), « Des militaires et certains membres des services secrets français utilisent l'application sportive Strava lorsqu'ils font leur jogging. Le problème ? Cette application les géolocalise », *Loopsider sur Twitter*, 30.03.2018, 10:45, en ligne: https://twitter.com/Loopsidernews/status/979640744926437376?s=09 (accédé le 31.03.2018).

Mayer-Shonberger Viktor et Kenneth Cukier (2014), *Big Data. La révolution des données est en marche*, Robert Laffont

Niva, Steve (2013), « Disappearing violence: JSOC and the Pentagon's new cartography of networked warfare », *Security Dialogue*, 44, 3, pp.185-202.

Owens, William A. (2000), *Lifting the Fog of War*, New-York: Farrar, Strauss, Giroux.

PBS (2005), « A Company of Soldiers: Innovating & Improvising », *Frontline*, 22.02.2005, en ligne: https://www.pbs.org/wgbh/pages/frontline/shows/company/lessons/ (accédé le 28.03.2018)

Reiter, Dan (dir.) (2017), *The Sword's Other Edge: Trade-offs in the Pursuit of Military Effectiveness*, New-York: Cambridge University Press.

Rogers, Kaleigh (2018), « Don't Just Delete Facebook, Poison Your Data First », *Motherboard*, 28.03.2018, en ligne: https://motherboard.vice.com/en_us/article/qvxv4x/how-to-delete-facebook-data (accédé le 31.03.2018).

Schmitt, Olivier (2018), « Innover dans les armées: les enjeux du changement militaire », *Revue Défense Nationale*, n°809, avril

Tual, Morgane (2018), « L'armée française met ses troupes en garde contre l'application de jogging Strava », *Le Monde.fr*, 30.01.2018, en ligne: http://www.lemonde.fr/pixels/article/2018/01/30/l-armee-francaise-met-ses-troupes-en-garde-contre-l-application-de-jogging-strava_5249157_4408996.html (accédé le 28.03.2018).

US Marine Corps (1996), *Marine Corp Doctrinal Publication 6: Command and Control*, Quantico: Marine Corps Combat Development Command.

Vego, Milan (2003), « Net-Centric is Not Decisive », *Proceedings Magazine*, 129, 1, janvier.