Revue COSSI

N° 4 | 2018
Méthodes et stratégies de gestion de l'information par les organisations : des big data aux thick data

De la RMA à la guerre infocentrée : retours d’expérience quant aux limites des promesses de la numérisation et des big data

Patrick Cansell
Docteur
DICEN-Idf
University of Paris-Est, Champs-sur-Marne
Lucile Desmoulins
UPEM - Laboratoire DICEN-Idf
6-8 cours du Danube, 77700 SERRIS

Édition électronique :
URL :
https://revue-cossi.numerev.com/articles/revue-4/1831-de-la-rma-a-la-guerre-infocentree-retours-d-experience-quant-aux-limites-des-promesses-de-la-numerisation-et-des-big-data
DOI : 10.34745/numerev_1603
ISSN : 2495-5906
Date de publication : 04/09/2018

Pour **citer cette publication** : Cansell, P., Desmoulins, L. (2018). De la RMA à la guerre infocentrée : retours d’expérience quant aux limites des promesses de la numérisation et des big data. *Revue COSSI*, (4). https://doi.org/https://doi.org/10.34745/numerev_1603

Dans les années 1980, les forces armées amorcèrent une révolution technologique et organisationnelle, par l'intégration massive de technologies de l'information et de la communication. La *Revolution in Military Affairs*, initiée aux États-Unis, vise à métamorphoser l'approche du commandement et de la réalisation des opérations militaires à travers le développement de solutions intégrées de renseignement, d'interconnexion et de commandement. La RMA s'incarne aujourd'hui à l'échelle du combattant individuel français dans un concept de « système fantassin » valorisé par l'information et qui contribuerait à la « domination informationnelle » sur des théâtres d'opération. Les premiers retours d'expérience, en particulier ceux d'Irak et d'Afghanistan, invitent toutefois à relativiser les capacités analytiques et prédictives des mécanismes algorithmiques nourris par des « systèmes fantassin » en situation réelle de conflit armé. Ils évoquent aussi l'infobésité des usagers au niveau du management opérationnel, leur méfiance quant à la fiabilité des transmissions et décisions stratégiques.

Mots-clefs :
Big data, Intelligence artificielle, Guerre, Intelligence stratégique, Décision, Network Centric Warfare, RMA

Abstract : In the 1980s, the armed forces began a technological and organizational revolution, through the massive integration of information and communication technologies. The Revolution in Military Affairs, initiated in the United States, aimed to transform the approach to command and execution of military operations through the development of integrated intelligence, interconnection and command solutions. The RMA is today embodied at the individual soldier level by the concept of "infantry soldier system" valued by information. This equipment is supposed to contribute to "information domination" during military operations. Initial feedbacks, especially from Iraq and Afghanistan, however, suggest that the analytical and predictive capabilities of algorithmic mechanisms fueled by "infantry soldier system" in real situations of armed conflict should be put into perspective. They also stress on the infobesity of users at the level of operational management, their mistrust as to the reliability of transmissions and strategic decisions.

Keywords : Decision, Network Centric Warfare, War, Strategic Intelligence, big data, artificial intelligence, RMA

INTRODUCTION

Les « big data » s'étalent sur les couvertures des magazines, tantôt présentées comme le moyen d'améliorer le quotidien, la santé, la sécurité de tout un chacun, tantôt comme le nouvel or noir digital des entreprises. Elles souffrent en contrepartie d'un soupçon de risque majeur en termes de limitation des libertés publiques et de surveillance généralisée. La mise en œuvre des promesses des big data sur le travail au sein d'une organisation singulière, les forces armées, permet de nuancer concrètement les promesses de la numérisation et des big data. Les forces armées se caractérisent par le caractère historique précoce de la réflexion et du pilotage stratégique des démarches d'intelligence et de « numérisation ». L'intégration du numérique et des big data dans les démarches d'intelligence, de commandement et de déploiement des opérations aux niveaux stratégique, opératif et tactique, y est donc a fortiori très avancée. Les informations intégrées dans le cycle du renseignement et les moyens de collecte, de traitement et de diffusion de ces informations sont par exemple désormais numérisés. De leurs côtés, les États-majors ont investi massivement dans un concept de combat « infocentré » et dans l' « infovalorisation » des forces, depuis plus de 15 ans. Du fait de leur singularité, l'observation des forces armées peut d'ores et déjà fournir un retour d'expérience et des pistes de réflexion pour d'autres types d'organisations (entreprises, autres institutions, ONGs).

NUMÉRISATION, CULTURE NUMÉRIQUE GÉNÉRALISÉE ET RÉVOLUTION DANS LES AFFAIRES MILITAIRES

Au tournant des années 1980, les forces armées amorcèrent une révolution technique, technologique et organisationnelle par l'intégration massive des technologies de l'information et de la communication. La Revolution in Military Affairs (RMA) initiée aux États-Unis a métamorphosé l'approche du commandement et des opérations militaires. Les efforts d' « infovalorisation » se dirigèrent vers l'investissement et le développement de solutions numériques d'acquisition, de transmission et de traitement de renseignements, ainsi que de commandement intégré (Command & Control) : outils, systèmes, tels que satellites, drones, radars, moyens de navigation, moyens d'influence ou de guerre électronique (« ELINT ») et « cyber ». L'idéal d'interconnexion et d'interopérabilité des systèmes d'armes s'incarne jusqu'au niveau du combattant individuel, intégré dans un « système fantassin ».

Dans un contexte de gigantisme du volume des données produites et traitées en amont comme lors des opérations militaires, la domination informationnelle s'est imposée comme un objectif intermédiaire dans des espaces de bataille hyper-numérisés. Ce combattant symbolise, au même titre que les robots ou les drones armés, l'évolution de l'approche du commandement et de la mise en œuvre des opérations militaires à travers le développement de nouvelles solutions de renseignement et de traitement de l'information, d'interopérabilité et de commandement intégré.

Dans la lignée des travaux de Josyane Jouet, l'étude des modalités concrètes de fabrication des datas par des usagers (le stratège qui pilote une opération ou le militaire présent sur un théâtre d'opération) contribue à illustrer « la prééminence du social dans les modalités d'utilisation des objets techniques » (Jouët, 1992, p.26). Elle s'intègre aussi dans une réflexion critique de l'idéalisation des potentialités des big data en termes de performance, d'efficacité de la prise de décision, de prédictibilité des comportements de l'ensemble des parties prenantes à un conflit ou à une action militaire de stratégies (Brasseur, 2013) et de résorption d'éventuels dilemmes éthiques. Elle apporte un éclairage sur les modalités, processus d'intégration et usages par les forces armées des technologies et des systèmes d'information et de communication, entamée il y a plus de 20 ans. Cette enquête illustre ainsi les débuts d'une prise de conscience des limites de la pensée dominante quant à l'omnipotence analytique et prédictive des data et des algorithmes visant à automatiser la décision et l'action qu'il s'agisse de dominer un théâtre d'opérations militaires, ou un marché.

Fruit de la réflexion conjointe de deux enseignants-chercheurs en sciences de l'information et de la communication, passionnés de stratégie militaire qui exercent en tant que consultants spécialistes de la gestion de crise, des stratégies d'influence et des démarches d'intelligence économique auprès de forces armées, cette communication fait suite à un travail poussé de veille, à une série de rencontres et de discussions informelles dans le cadre d'une forme d'ethnographie organisationnelle extensive. L'un des auteurs a mis à profit ses expériences d'officier de réserve, diplômé « Etat-Major », au sein de la Direction du Renseignement Militaire, en charge de questions de prospective.

Le concept de « Revolution in Military Affairs » (RMA) s'est développé aux États-Unis à la fin des années 1970 (Gros, 2010). La notion de « révolution » est ici considérée comme une rupture doctrinale majeure menant à un emploi des forces radicalement innovant, susceptible de remporter la décision non du simple fait d'une supériorité quantitative ou technologique des matériels, mais grâce à leur emploi. La Blitzkrieg allemande de 1940, considérée comme l'une de ces « révolutions », reposait ainsi non sur le seul développement de nouveaux chars et de nouveaux avions - puisque les Alliés disposaient eux-mêmes de matériels comparables -, mais sur une utilisation de rupture. La combinaison d'armes anciennes et nouvelles généra de nouvelles capacités et doctrines d'emploi qui se sont révélées décisives, face à un ennemi imprégné jusqu'à l'aveuglement par les concepts de guerres de position et d'usure. On parle de révolution non pas parce que le changement de doctrine a été brusque, mais parce qu'il a été d'une amplitude diamétrale (« magnitude ») (Welch, 1999).

Le contexte d'émergence de la RMA est tout sauf anodin : à la fin des années 1970, les stratèges du Pentagone ne sont pas parvenus à penser de nouvelles doctrines et usages rendus possibles par les technologies de l'information et de la communication et par l'électronique, à l'inverse des officiers soviétiques qui inventèrent le concept de « révolution militaro-technique ». Les forces soviétiques supprimèrent en effet les échelons hiérarchiques intermédiaires et parvinrent à des concepts tels que celui de « reconnaissance – frappe » où celui qui collecte l'information (l'observateur qui a les

jumelles et voit l'adversaire), ordonne directement le tir des moyens d'appui-feu sur l'adversaire en sans passer par les étapes traditionnelle de validation par les différents échelons hiérarchiques. La prise de conscience de la supériorité stratégique soviétique fut un véritable choc pour les stratèges américains Dès lors, c'est-à-dire au milieu des années 1980, ces derniers considérèrent que les forces US étaient obsolètes, incapables de remporter un conflit autrement que par la masse des moyens déployés : « being bigger, not smarter » déplore alors le Général David C. Jones, chef d'État-major des armées des États-Unis (Luttwak, 1985).

En réponse à la posture innovante des Soviétiques, la « RMA », mise en œuvre à partir de la fin des années 1980, a visé à bouleverser l'appareil militaire américain, selon trois axes. Le premier axe est technologique avec un basculement des efforts de R&D vers les TIC, les outils de commandement (Command & Control), les moyens de reconnaissance terrestre, aérienne et satellitaire, le renseignement (HUMINT, ELINT, SIGINT) ou encore la cyber-sécurité et la guerre électronique ; il s'agit notamment d'intégrer l'information et ses technologies aux équipements et de les organiser en réseau. On parle en France à ce sujet d'« infovalorisation ».

Le deuxième axe est matériel. De nombreux équipements sont modernisés pour améliorer leur intégration au sein de ce que l'on appelle un « système » de forces. Beaucoup d'équipements sont remplacés car jugés obsolètes et « data-incompatibles ». Les équipements et systèmes nouveaux intègrent dès leur conception les enjeux et les moyens de leur « infovalorisation » et même une capacité à intégrer des technologies futures lors de leur modernisation. Un système d'armes peut en effet rester en service plusieurs décennies. Le concept de « Soldier System », par exemple, traduit en français par « Système Fantassin » décrit un combattant « infovalorisé », à savoir nourri, traversé, médiateur et capteur d'informations. Capteurs et effecteurs sont ainsi « dé-solidarisables », les capteurs (moyens de reconnaissance, de ciblage, etc.) et les effecteurs (armes et munitions) communiquant entre eux à distance. Les munitions de précision peuvent entrer en scène et générer de nouveaux paradigmes tels que la guerre « zéro mort », ou des concepts tels que celui de « frappe chirurgicale ». La Guerre du Golfe, en 1991, « a été un vrai tournant dans l'histoire militaire. (…) Les nouvelles technologies ont en effet permis aux avions et aux armements de devenir extrêmement précis et d'agir de manière permanente : de jour, de nuit et par mauvais temps. (…) On a beaucoup parlé du guidage par laser, mais il existe d'autres moyens, comme le GPS, le radar ou des systèmes optiques. Si on possède les coordonnées précises d'une cible, on ne peut pas la rater » explique à la presse le Général Jean Rannou, chef d'État-major de l'Armée de l'air française de 1995 à 2000 (Jean Dominique Merchet, « La première stratégie c'est le renseignement », in Libération, 23/10/2001). La surmultiplication des capteurs est le corollaire de cette tendance. Celle des masses et des flux de données, en est la conséquence.

La RMA comprend enfin un axe humain. Tant au niveau des hommes sur le terrain qu'au niveau du commandement, la réalisation des missions a été repensée en intégrant la dimension numérique. Les forces armées semblent parvenir à une certaine maturité dans leur numérisation, mais les retours d'expérience au niveau du « management »

opérationnel ont dénoncé précocement les effets pervers de l'infobésité et de l'automatisation des transmissions de données, ainsi que les capacités prédictives limitées des mécanismes algorithmiques appliquées aux situations de conflits armés, notamment lors de l'opération Iraki Freedom).

Dès 2003, la première brigade numérique américaine a été déployée en opération en Irak, suite à d'ambitieux programmes de digitalisation des forces armées, notamment l'Army Transformation, un impressionnant programme de modernisation des forces terrestres américaines. Le déploiement de cette première « BCT », (Brigade Combat Team), unité entièrement « infovalorisée » et équipée de matériels légers (blindés à roues Stryker notamment), devait marquer la rupture avec les « Legacy Forces », les lourdes unités conventionnelles héritées de la Guerre Froide, caractérisées par l'absence du digital et en principe condamnées à disparaître.

UN PARALLÈLE ENTRE LA PENSÉE STRATÉGIQUE INTÉGRATIVE DU MONDE CIVIL ET L'OBJECTIF RÉMANENT DE RÉDUIRE LE « BROUILLARD DE LA GUERRE »

La pensée stratégique française considère l'information comme la matière première de la décision et de l'action militaire (Lacoste, 1995). Dans les entreprises, les démarches d'intelligence stratégique (IS) intègrent l'ensemble des actions outillées, précises et ciblées désignées par les vocables de documentation, de(s) veille(s), de « due diligence », de sécurité de l'information, de protection du patrimoine immatériel, d'analyse concurrentielle, d'aide à la décision, de prospective ou d'influence/contre-influence. L'adjectif stratégique n'a donc ici aucune acception militaire, il vient caractériser le niveau où les démarches d'intelligence peuvent être mises profit. En l'occurrence, le niveau le plus élevé de la prise de décision en entreprise, celle du projet et de la stratégie d'entreprise peuvent bénéficier de démarches d'intelligence économique. De la même manière, l'intelligence économique peut intéresser des prises de décisions d'investissement en R&D, en matières premières, des décisions en matière de choix de fournisseurs, des décisions commerciales, marketing, packaging, etc. La principale caractéristique de l'IS est qu'elle ne se limite pas à des actions "partielles" menées isolément dans des fonctions différentes des organisations, elle suppose une réflexion qui articule le stratégique et le tactique, et une coordination des actions d'intelligence économique. Le succès de ces actions procède alors de la cohérence de la réflexion en amont et d'un pilotage en continu, ainsi de leur degré d'intégration. Par intégration, on entend « interaction entre tous les niveaux de l'activité, auxquels s'exerce la fonction d'intelligence économique depuis la base ([les acteurs] internes à l'entreprise) en passant par des niveaux intermédiaires (interprofessionnels, locaux) jusqu'aux niveaux nationaux (stratégies concertées entre les différents centres de décision), transnationaux (groupes multinationaux) ou internationaux (stratégies d'influence des États-nations [et des organisations internationales]) » (Martre, 1994, p.12).

Du côté des militaires, les systèmes d'armes deviennent communicants, "intelligents", complémentaires et intégrés, ce qui a permis une accélération majeure du rythme des batailles, de leur « tempo », et la nécessité d'une gestion stratégique en temps réel de la masse des données générées (Luttwak, 1985, Ibrügger, 1998, Gros, 2010, Gerasimov, 2016). Les parallèles entre le monde des entreprises et des organisations civiles, et le monde des forces armées s'impose en lien avec ce critère de l'accélération (Rosa, 2010).

Deux concepts clefs sont au cœur de la RMA. Tout d'abord, celui d'« Information Dominance » ou « supériorité informationnelle » représente l'« avantage opérationnel obtenu par la capacité à collecter, traiter et disséminer un courant ininterrompu d'informations, tout en exploitant ou interdisant à l'adversaire cette même capacité » (Vandomme, 2010). Nous retrouvons ici une conception particulièrement proche des définitions originelles de maîtrise et de protection de l'information que doit permettre l'Intelligence Economique. Notons que ces définitions sont postérieures de quelques années seulement aux premiers programmes visant à l'application de la RMA. Le deuxième concept, celui de Network-Centric Warfare (NCW) ou guerre infocentrée implique l'intégration en réseau de l'ensemble des capteurs et effecteurs du champ de bataille, « le traitement en temps réel (ou quasi-réel) des données et des informations, leur transformation en savoir et leur transmission vers les unités de feu pour un combat de précision » (De Neve, 2011). Dans le monde civil, se sont progressivement développés des outils de veille devenus « collaboratif », des « réseaux sociaux d'entreprise » supposés faciliter les flux et la création d'informations et de connaissances et autres plateformes visant à la mise en réseau des acteurs, porteurs de savoir et décideurs (Cansel, 1995, David, 2005, Mesguisch et al., 2008, Moinet, 2009, Rouach, 2010, Saleh et al., 2013, Husson, 2017).

Pour les forces armées, la numérisation doit contribuer à réduire ce que Clausewitz appelait le « brouillard de la guerre ». Lors des campagnes de la Révolution et de l'Empire, la notion de brouillard correspondait à la part d'incertitude inhérente à la conduite des opérations, à la méconnaissance de la réalité de ses propres capacités comme de celles de l'adversaire, aux « frictions » générées par les erreurs et incidents, et qu'il fallaitt s'efforcer de réduire par la pratique du renseignement tactique (Clausewitz, 1832). Aujourd'hui ce « brouillard » naît notamment de la complexité du terrain (zones urbaines ou montagneuses, grottes, jungle), du contexte politico-diplomatique, ou encore de la nécessité d'identifier et localiser des adversaires, parfois mêlés aux civils, et ses propres troupes pour éviter notamment tout « friendly fire », ces tirs fratricides à l'origine de pertes inacceptables.

La supériorité informationnelle n'est pas ici synonyme d'accès privilégié à des informations en masse (big data) ou de capacité accrue de traitement d'informations à forte valeur ajoutée (thick data – ce qui est le cas pour les métiers du « renseignement » y compris. militaire). Il s'agit, à l'échelle de l'organisation des forces, de la capacité à interconnecter les systèmes d'armes et des combattants eux-mêmes devenus des éléments du « système de force » avec les systèmes de commandement, de communication, de surveillance et de renseignement (integrated weapons and data

systems) pour créer des flux spécifiques de données et d'informations à forte valeur ajoutée. S'ajoute à cela le critère de l'anticipation car ces flux ne peuvent jouer de rôle-clé que s'ils ont préalablement pensés et structurés en fonction d'enjeux opérationnels, techniques, logistiques, etc. Ce système de commandement intégré (Command & Control, C2, ou C4ISTAR plus dans sa version élaborée) a été formalisé par l'Amiral Owens de l'US Navy, qui conceptualisa la notion désormais incontournable de « System of systems », que l'on peut traduire ainsi par « méta-système » de forces.

En terme de mise en œuvre, ce méta-système inclut l'architecture et la gestion des interactions de tous les systèmes d'armes et capteurs, et de toutes les données issues ou générées par les plateformes, les blindés, les véhicules logistiques, les robots, les outils de « vétronique » pour traiter ces données, par et pour les combattants (localisation, ordres, voix, image, et demain paramètres vitaux, niveau de stress, ou encore état des approvisionnements en munitions, niveaux des batteries, etc.), par et pour les moyens de soutien ainsi que le commandement. Précisions que concrètement, les outils de « vétronique » sont des sortes de boitiers embarqués sur des véhicules militaires, ces derniers permettent la gestion centralisée des systèmes d'information et de contrôle des ressources électroniques et informatiques captées et reçues, ils intègrent des calculateurs embarqués hyper puissants et compacts.

Le concept d'Information Warfare intègre ainsi l'ensemble des mesures prises par un chef militaire pour imposer sa supériorité dans la maîtrise de l'information des forces engagées (guerre électronique, chiffrement, furtivité, contre-influence, etc.) : celle de ses forces comme celle de l'adversaire.

LES LIMITES DES AMBITIONS DU BIG DATA

Dans les entreprises, les directeurs, managers et simples salariés sont comme enjoints d'adhérer à une idéologie enchanteresse accréditant des promesses numériques de rapidité, d'accessibilité, d'efficacité, d'opportunités à saisir, idéologie qui procède directement d'un paradigme gestionnaire de rationalité pure. Les dispositifs de veille poussent des messages vers les collaborateurs, chacun devenant analyste de son propre environnement informationnel. De tels dispositifs d'autonomisation et d'accès facilité à l'information ont été testés au sein des forces armées, y compris par la création d'un « internet du champ de bataille ». L'opération Iraki Freedom a été l'occasion d'expérimenter à grande échelle, dès 2003, ces solutions innovantes de remontée, partage et diffusion d'informations, exploitant la masse de données produites par tous les échelons des forces.

Dès son premier déploiement, la « Brigade Combat Team » (BCT) a été marquée par l'échec, outre le fait qu'elle arriva trop tard pour combattre les forces conventionnelles de Saddam Hussein, elle n'était pas prête pour l'offensive terrestre initiale et son déploiement fut ralenti par des soucis diplomatiques avec la Turquie qui refusera notamment son passage. Elle ne fut donc engagée que dans des opérations de contre-insurrection face aux « insurgés irakiens ». Cet échec est en premier lieu conceptuel. Les systèmes d'information et en particulier l'« internet du champ de bataille » mis à

disposition des différents échelons de combattants fonctionnèrent essentiellement en mode « pull » : on mit à la disposition des combattants, des chefs d'unités, de sections, une masse d'informations supposées intéressantes pour qu'ils puissent littéralement y piocher des informations utiles. Mais en fait les combattants n'en eurent pas le temps et se perdirent dans les méandres de ces ressources.

Le second effet est encore plus grave puisqu'il concerne la valeur ajoutée supposée d'une unité digitalisée. Un ancien commandant d'un régiment de cavalerie de l'armée américaine, Col. H.R. McMaster, le formule ainsi : « Les chefs auront tendance à attendre de recevoir des informations plutôt que de prendre des décisions claires. En effet, ils doivent agir avec prudence pour protéger la survie de leurs troupes. On observe toute l'ironie de forces créées pour être rapides et agiles, mais qui se révèlent être l'exact inverse » (Grossman, 2005). Le problème que génère la surinformation, est que les chefs militaire sur le terrain, qui sont l'équivalent militaires des managers de proximité, hésitent à déployer leurs troupes tant qu'ils ne sont pas sûrs de ne plus obtenir d'informations plus pertinentes et/ou précises dans la double visée d'optimiser les chances de succès d'une opération et d'économiser des ressources - en particulier la vie d'hommes. En voulant rationaliser la prise de décision, et donc en attendant de recevoir plus d'informations pour réduire au maximum les incertitudes, les BCT expérimentèrent un paradoxe : ces forces numérisées supposées être plus rapides car info-valorisées, se montrèrent plus lentes et indécises, et donc moins agiles que des combattants plus rustiques, ayant moins informations et basant leurs décisions tactiques sur une forme d'instinct sans soubassements conceptuels. À ces problèmes décisionnels, s'ajoute le problème prosaïque du poids d'équipements high-tech dénoncé par les soldats dans leurs retours d'expérience.

La masse de données collectée pose de surcroit deux problèmes majeurs. En premier lieu, on distingue un problème de traitement des données, face à une volumétrie considérable et en croissance exponentielle, alimentée par la multiplication des capteurs interconnectés et des moyens de renseignement de tous types. Le Big Data et l'intelligence artificielle sont supposés apporter, à un horizon non déterminé mais supposé proche, une réponse satisfaisante à cette impasse digitale. Le big data est en effet supposé être couplé, à terme, à des logiciels de traitement analytique et à des algorithmes prédictifs, visant en particulier à rendre intelligibles des masses de données éparses, à anticiper l'évolution du contexte des opérations comme les comportements de l'adversaire. Les stratèges souhaitent ainsi anticiper des événements et comportements très variés : les actions des forces adverses, les embuscades, les mouvements de population, l'opinion publique, les décisions politico-stratégiques des adversaires… En second lieu, cette masse de données génère une dépendance croissante à ce que l'on appelle « l'infostructure », dépendance proportionnelle à la masse d'informations collectée, traitée, diffusée. Or, les déploiements récents ont lieu dans des zones où les communications passent particulièrement mal : milieux complexes (centres urbains en 3 dimensions, montagnes) ou vastes territoires non homogènes (plateaux désertiques), où les défaillances et insuffisances des technologies et capacités de l'infostructure militaire sont patentes.

En observant l'évolution technico-opérationnelle du combat, on peut distinguer trois paradoxes évidents quant à l'exposition sur le terrain et à la perception que les politiques se font du rôle des combattants infovalorisés. Tout d'abord, les combattants directement exposés à leur adversaire sont parmi ceux qui ont le plus besoin d'« intelligence » et donc d'information à forte valeur ajoutée, validée, précise et pertinente, mais aussi ceux qui ont le moins de temps pour consommer de l'information. Ensuite, les combattants directement exposés à leur adversaire sont une source essentielle d'« intelligence », capables de produire la meilleure information sur celui-ci, mais sont ceux qui ont peu de temps pour en produire. La tendance est d'ailleurs à les équiper ou à les faire accompagner ou survoler de capteurs capables de transmettre en temps réel des données sans perturber leur engagement.

Enfin, les technologies sont présentées comme des « démultiplicateurs » de force, mais leur implémentation est souvent réalisée en parallèle de réductions importantes des effectifs opérationnels. Les TIC ont été un prétexte à la réduction des effectifs. Et les big datas sont aujourd'hui présentées, à l'instar d'un argumentaire prégnant dans le civil, comme une solution miracle susceptible de palier à toutes les difficultés. Chaque génération d'équipements est supposée être toujours plus performante, et justifier la réduction des effectifs. Cependant, les autorités ont pris leurs distances vis-à-vis de ce paradigme désormais, face aux engagements extérieurs et aux opérations intérieures (face au terrorisme notamment). En France comme aux Etats-Unis, on recompte en « boots » les unités déployables / déployés. Le « paradigme augmentatif » a été réinstauré en lieu et place d'un « paradigme substitutif » (Zacklad, 2012). Les premiers retours d'expérience soulignent ainsi les limites de la numérisation et des big data, et notamment les résistances qu'ils suscitent en terme de méfiance quant aux promesses d'automatisation des transmissions, de capacités prédictives des mécanismes algorithmiques, et de limites opérationnelles (infobésité, notamment du « management », à savoir le commandement opérationnel).

En toute logique, les forces armées limitent le champ d'exploitation des big data aux activités du renseignement militaire et d'intérêt militaire, en particulier dans les opérations « hybrides », soit des missions restreintes de surveillance des médias sociaux, de création de corpus documentaires permettant des requêtes ciblées sur des individus précis. La réalité des usages militaires reste éloignée des ambitions d'anticipation algorithmiques d'attaques terroristes supposées contribuer à une forme de « situation awareness ». D'autres applications plus réalistes concernent la guerre-cyber ou « cyberwarfare » (Haridas, 2015), qui offre de vraies potentialités notamment dans le tracking des hackers et la détection de signaux d'alerte parfois qualifiés de faibles (Alloing, Moinet, 2016). Les big data ne sont en fait qu'une ressource complémentaire, essentielle pour certaines applications dites de renseignement, utiles pour capter et traiter des flux de données structurées liées à certaines situations d'emploi des forces, mais elles ne sont pas une panacée.

Derrière la notion de « big data » appliquée au champ des études stratégiques réside le travail de capitalisation par les forces armées de tout ce qu'elles peuvent collecter pour éventuellement, le cas échéant, lors d'une enquête sur une personne précise, être en

mesure de disposer de ressources pour des actions de renseignement et de monitoring des cyber menaces. Les big datas ont donc principalement un intérêt pour la surveillance des médias sociaux, la création de corpus documentaires pour permettre des investigations sur des individus, et appréhender des questions de cyber-sécurité. Or, ces usages ne sont pas absolument pas transposables au civil, et ils n'ont pas de liens avec les usages de démarche d'intelligence stratégique et des situations de prise de décision au niveau du top-management des entreprises !

Enfin, concernant les risques d'attaque terroriste, les militaires sont formels quant à l'inanité des outils de big datas. Si une patrouille peut avoir une connaissance de terrain qui lui permettra d'estimer « au doigt mouillé » le degré de réalité d'un risque d'attaque terroriste. Un algorithme pourra lui aussi montrer qu'un risque existe à partir des données remontées par une patrouille, mais il sera incapable de le confirmer en avance de phase, de le prédire suffisamment précocement et avec suffisamment de certitude pour qu'une patrouille puisse intégrer cette donnée dans sa prise de décision. Prévoir le passage à l'acte de civils radicalisés jusqu'au terrorisme fait partie de sphère du fantasme bien illustrée par l'intrigue de films comme I-Robot ou Minority Report. Et nulle force armée répondant aux critères occidentaux d'engagement de la force n'oserait par exemple justifier une frappe préventive sur des civils en arguant du fait qu'il s'agit de la décision optimale d'un algorithme. Pire, les situations de conflit armé ne sont pas modélisables selon des critères permanents, logiques et rationnels tels que l'on peut en trouver dans la finance, le droit ou même la médecine : « Pour une armée bien préparée, chacun des éléments qui concourt à la conduite des opérations se réduit à une formule simple : déplacement d'un point à un autre ; maniement d'une arme maîtrisée par des centaines d'entraînements ; transmission et compréhension d'ordres formulés sans ambiguïtés… Mais la combinaison de tous ces éléments peut atteindre une extraordinaire complexité, face à un ennemi réel qui s'évertue à saper la moindre initiative en utilisation sa réflexion stratégique et ses forces. » (Luttwak, 1985, p.26). Une intelligence artificielle pourrait mener des opérations militaires ou même diriger un système d'armes dans un environnement complexe si elle « comprenait » l'art de la guerre et développait ses propres ruses, dans un contexte où la « règle » n'existe pas. « Il est extraordinairement difficile de prédire le déroulement d'une guerre. Chaque guerre suppose la redéfinition d'une nouvelle doctrine stratégique. Chaque guerre est unique, et appelle des choix quant à sa logique propre plutôt que la mise en œuvre de modèles pré-définis », expliquait, dès avant le second conflit mondial, le théoricien russe Aleksandr Svechin (Gerasimov, 2016). En effet, dans le contexte militaire, la stratégie va consister à privilégier des méthodes d'action parfois en apparence contre-productives où prédominent la ruse et la « tactique » : « (…) des préparatifs manifestement bâclés, (…) des approches en apparence trop dangereuses ; (…) le combat de nuit ou par mauvais temps… Voilà autant de manifestions courantes de l'ingéniosité tactique, conformes à l'essence même de la guerre » (Luttwak, 1985, p.25).

CONCLUSION : BIG DATA, ALGORITHMES,

INTELLIGENCE ARTIFICIELLE, ET NOUVELLES DOCTRINES D'EMPLOI DE LA FORCE

À titre d'illustration des faiblesses et vulnérabilités des outils big data et de l'intelligence artificielle appliquée à la « chose » militaire, l'exemple russe est particulièrement instructif. La doctrine stratégique Gerasimov, du nom du Chef d'État-major des forces de la Fédération de Russie, est en effet particulièrement illustrative des effets de rupture des doctrines, plaidant pour une vision réflexive, pilotée et intégrative, des stratégies militaires.

Cette doctrine plaide pour le déploiement conjoint et intégré par des systèmes de communication et de commandement d'actions politiques, diplomatiques, médiatiques, cyber et militaires, au service d'une guerre non pas totale, mais globale, contre un adversaire donné. La doctrine d'emploi des cyberforces russes vise ainsi non pas à réaliser des actions ciblées en complément des opérations militaires, mais à mener de vastes opérations simultanées et conjointes à visées multiples (guerre électronique, guerre d'influence, paralysie des moyens, médias et infrastructures adverses). On parle alors de conflit « non-linéaire » (Bartles 2016) dans lequel un adversaire plus faible technologiquement compense son désavantage en termes informationnel en leurrant son adversaire par des opérations coordonnées de désinformation, de déstabilisation et de leurres visant particulièrement le système de décision adverse et les algorithmes qui l'alimentent (Chin Hui Han, 2016).

Aujourd'hui, cette guerre nouvelle se traduit par des doctrines d'emploi très offensives, mixant les opérations conventionnelles, celles menées par des irréguliers (rebelles, indépendantistes par exemple) et les opérations ciblant justement les big data et les algorithmes décisionnels des adversaires, devenus des cibles à part entière. Il va s'agir en effet de leurrer, tromper les moyens logiciels de l'ennemi. Ces doctrines se traduisent, par exemple, par la mise en place de flottes de robots sur les médias sociaux notamment, afin de générer du bruit et simuler des mouvements d'opinion, des campagnes de désinformation ou encore de fausses contestations potentiellement violentes. Il va s'agir d'interpréter le mode opératoire de l'intelligence artificielle de l'adversaire pour générer des signaux visant à l'induire en erreur : pollution de données, actions visant à tromper (ce que l'on appelle la « déception ») pour générer de multiples « opérations Fortitude » digitales comme physiques. Cette appellation s'inspire du nom de l'opération de leurrage de l'État-Major allemand au moment du débarquement en Normandie, simulant une action d'envergure sur le Pas de Calais. Les « big data » offrent alors paradoxalement des moyens pour agir contre le camp qui les possède et les exploite, et l'intelligence artificielle devient une cible comme les autres, et potentiellement une vulnérabilité majeure. Du côté russe, le pragmatisme domine et les data sont considérées comme des ressource clefs sur des thématiques précises et comme une dimension à part entière du fonctionnement et de l'efficience du système de forces, mais non comme une solution globale et miraculeuse de production rapide de décisions optimales.

Big, thick, integrated, autonomous… Chacun des adjectifs auxquels le mot data a été accolé est porteur d'utopies positivistes, qu'il s'agisse de gagner des marchés ou des conflits. La manière dont l'information et les data ont été pensées par les stratèges militaires peut apporter un éclairage aux débats sur les data, pétrole du XXIe siècle… Comme l'exprimait l'Amiral Owens devant le Congrès américain en 2001 de manière prémonitoire : « Ce n'est pas la masse des données accumulées qui va conditionner nos succès, c'est la force de nos connaissances, qu'il s'agisse de la guerre en Somalie ou de la lutte anti-terroriste dans nos frontières ou à l'étranger. Ce qui compte, c'est le savoir » (Shimko, 2010). Et, par essence, la connaissance et le savoir sont incarnés.

RÉFÉRENCES BIBLIOGRAPHIQUES

Alloing, C. & Moinet, N. (2016). Les signaux faibles : du mythe à la mystification. *Hermès*, La Revue, 76,(3), 86-92.

Bartles, Charles K. (2016). Getting Gerasomov Right. USACAC *Military Review*. 30-38 - Fort Leavenworth (USA/KS).

Cansell, Patrick. (2003). *Management de l'information et connaissance du marché : développement des pratiques collectives d'intelligence économique et de management de l'information (…)* ». Thèse de Doctorat : Sciences de l'Information et de la Communication. CESD : Université Paris-Est Marne-la-Vallée.

Chin, Hui Han. (2016). Mskirovka in the Information Age. *Pointer, Journal of the Singapore Armed Forces* (vol. 42, n°1 - 2016), 39-50.

Clausewitz, C. von. (1832). *De la Guerre*. Paris: Payot & Rivages, impr. 2014.

Cohen, C. (2013). *Business intelligence: the effectiveness of strategic intelligence and its impact on the performance of organizations*. Hoboken, NJ : Wiley-ISTE.

David, A. (dir.). (2005), Organisation des connaissances dans les systèmes d'information orientés utilisation. *Actes du colloque international de ISKO-France*, 28-29 avril 2005, Presses Universitaires de Nancy.

David, C. P. (2016). *Repenser la sécurité, nouvelles menaces nouvelles politiques*. Montréal : Fides, Collection Points Chauds.

De Neve, A. (2011). Mutations technologiques et transformations militaires : que reste-t-il du discours de la RMA ?. *Pyramide. Centre d'Etudes et de Recherche en Administration Publique*, 27-52.

Gerasimov, V. (2016). *The Value of Science is in the Foresight - New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations.* USCAC *Military Review,* Fort Leavenworth (USA/KS), *23-29.*

Gray, C. (2004). Strategy for Chaos: Revolutions in Military Affairs and the Evidence of

History (Strategy and History). Oxford: Routledge.

Gros, P. et al. (2010). *Du Network-Centric à la stabilisation : émergence des « nouveaux » concepts et innovation militaire*. 91-128. Paris : IRSEM.

Grossman E. M. (2005). Does the modular brigade need armed recon facilitators? Army Cavalry regiment may be last bastion. "*Fight for information". Inside The Pentagon*, February 10, 2005. INSIDER, http://defense.iwpnewsstand.com/insider.asp, Inside Washington Publishers.]

Haridas, M. (2015). Redefining Military Intelligence Using Big Data Analytics. *Scholar Warrior*. CLAWS - Centre for Landwarfare Studies. Automne 2015, 72-78.

Hoppe, M. (2015). Intelligence as a discipline, not just as a practice. *Journal of Intelligence Studies in Business*, 5(3), 47-56.

Husson, S.. (2017). La transformation digitale en entreprise, quels enjeux pour les veilleurs. *Mémoire professionnel*. Master 2 IE-ISART, sous la direction de Patrick Cansell. UPEM/IFIS.

Ibügger, L. (1998). *The Revolution in Military Affairs*. Nato Parliamentary Assembly, Science and Technology Committee. NATO.

Jouet, J. (1992). *Pratiques de communication et changement social*. Habilitation à diriger des recherches : Sci. de la comm : Grenoble 3.

Lacoste, P. (1995). *Culture française du Renseignement*. Actes du colloque. CESD.

Luttwack, E. N. (2002). *Le grand livre de la stratégie*. Paris : Éditions Odile Jacob.

Mesguich, V., Diallo, A., Jdey, A., Bergeret, C., Dumas, S., Séménéri, M .. & Remize, M. (2008). Où va la veille ?. *Documentaliste-Sciences de l'Information*, vol. 45,(4), 58-69.

Moinet, N. (2009). Du « savoir pour agir » au « connaître est agir »: L'intelligence économique face au défi de la communication. *Les Cahiers du numérique*, vol. 5,(4), 53-77.

Rouach, D. (2010). *La veille technologique et l'intelligence économique*. Collection : Que sais-je ?, Paris : PUF.

Rosa, H. (2010). *Accélération. Une critique sociale du temps*. Paris : La Découverte, coll. Théorie critique.

Saleh, I., Zacklad, M., Leleu-Merviel, S., Jeanneret, Y., Massou, L., Roxin, I., Soulages, F., Bouhaï, N. (coord. par) (2013). *Pratiques et usages numériques*. H2PTM'13, Hermes Science publications, Lavoisier.

Shimoko, K. L. (2010). *The Iraq Wars and America's Military Revolution*. London (UK) :

Cambridge University Press.

Vandomme, R. (2010). Du renseignement à l'influence : le rôle des opérations d'information. *Cahiers Strathrobyn* n°6. Toronto (Canada) : Centre des Etudes sur la Sécurité nationale. 9-87.

Welsch, T. J. (1999). Revolution in military affairs: One perspective. In Omory Frances, Sommerville M. A. (eds.), *Strenght through cooperation: Military Forces in the Asia-Pacific Region*. Washington DC: National Defense University press.

Zacklad, M. (2012). Vers une informatique au service de l'homme. *Personnel*, 527, 63-64.